

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

BENEFITALIGN, LLC, et al.,

Plaintiffs,

v.

CENTERS FOR MEDICARE & MEDICAID  
SERVICES, et al.,

Defendants.

Civil Action No. 24-2494 (JEB)

**DEFENDANTS' COMBINED MOTION TO DISMISS AND OPPOSITION TO  
PLAINTIFFS' AMENDED MOTION FOR TEMPORARY RESTRAINING ORDER  
AND PRELIMINARY INJUNCTION, AND REQUEST FOR EXPEDITED HEARING  
AND MEMORANDUM IN SUPPORT THEREOF**

**TABLE OF CONTENTS**

Table of Contents ..... i

Table of Authorities ..... ii

Introduction..... 1

Statutory and Reguatory Background..... 3

    I.    Web-Brokers, Enhanced Direct Enrollment Entities, Direct Enrollment Entities,  
          and Their Participation in the Exchanges Under the Affordable Care Act..... 3

    II.   Oversight, Enforcement, and Rebuttal Opportunity ..... 8

Factual and Procedural Background ..... 11

Legal Standards..... 14

    I.    Rule 12(b)(1)..... 14

    II.   Rule 12(b)(6)..... 14

    III.  Preliminary Injunction ..... 15

Argument ..... 16

    I.    This Action Should Be Dismissed for Lack of Jurisdiction. .... 16

        A.    Any Claims Related to the August 8 Email Are Moot. .... 16

        B.    Plaintiffs’ Claims Are Not Ripe..... 18

        C.    Plaintiffs’ Other Assertions of Jurisdiction Also Fail..... 21

    II.   This Action Should Also Be Dismissed for Failure to State a Claim. .... 22

        A.    Plaintiffs Do Not Have a Viable APA Claim. .... 22

        B.    Plaintiff’s Fifth Amendment Due Process Claim is Legally Deficient..... 30

    III.  Even If the Court Does Not Dismiss This Lawsuit, Plaintiffs Are Not Entitled to a  
          Temporary Restraining Order or Preliminary Injunction. .... 33

        A.    Plaintiffs Have Not Established Irreparable Injury..... 33

        B.    Plaintiffs Are Unlikely to Succeed on the Merits. .... 39

        C.    The Remaining Factors Weigh Against Mandatory Injunction..... 39

Conclusion ..... 41

## TABLE OF AUTHORITIES

<u>Cases</u>	<u>Page</u>
<i>13th Reg'l Corp., v. Dep't of Interior,</i> 654 F.2d 758 (D.C. Cir. 1980) .....	21
<i>Already, LLC v. Nike, Inc.,</i> 568 U.S. 85 (2013) .....	17
<i>Am. Bankers Ass'n v. Nat'l Credit Union Admin.,</i> 271 F.3d 262 (D.C. Cir. 2001) .....	22
<i>Am. Nat'l Ins. Co. v. FDIC,</i> 642 F.3d 1137 (D.C. Cir. 2011) .....	14
<i>Apex, Inc. v. FDA,</i> 449 F.3d 1249 (D.C. Cir. 2006) .....	39
<i>Arpaio v. Obama,</i> 797 F.3d 11 (D.C. Cir. 2015) .....	38
<i>Asante v. Azar,</i> 436 F. Supp. 3d 215 (D.D.C. 2020) .....	18
<i>Ashcroft v. Iqbal,</i> 556 U.S. 662 (2009) .....	14, 15, 31
<i>Atherton v. D.C. Off. of the Mayor,</i> 567 F.3d 672 (D.C. Cir. 2009) .....	31
<i>Belmont Abbey Coll. v. Sebelius,</i> 878 F. Supp. 2d 25 (D.D.C. 2012) .....	20
<i>Biovail Corp. v. FDA,</i> 448 F. Supp. 2d 154, (D.D.C. 2006) .....	39
<i>Blue Water Balt. v. Pruitt,</i> 266 F. Supp. 3d 174 (D.D.C. 2017) .....	18
<i>Burke v. Barnes,</i> 479 U.S. 361 (1987) .....	16-17
<i>C&amp;E Servs., Inc. v. D.C. Water &amp; Sewer Auth.,</i> 310 F.3d 197 (D.C. Cir. 2002) .....	21
<i>California v. Texas,</i> 593 U.S. 659 (2021) .....	21
<i>Chaplaincy of Full Gospel Churches v. England,</i>	

454 F.3d 290 (D.C. Cir. 2006) ..... 15

*Cheney v. U.S. Dist. Ct. for Dist. Of Columbia*,  
542 U.S. 367 (2004) ..... 21

*City of Columbus v. Trump*,  
453 F. Supp. 3d 770 (D. Md. 2020) ..... 3

*Clapper v. Amnesty Int’l USA*,  
568 U.S. 398 (2013) ..... 38

*Colo. Wild Horse v. Jewell*,  
130 F. Supp. 3d 205 (D.D.C. 2015) ..... 39

*D&G Holdings, LLC v. Burwell*,  
156 F. Supp. 3d 798 (W.D. La. 2016) ..... 25

*Damus v. Nielsen*,  
Civ. A. No. 18-0578 (JEB), 2018 WL 3232515 (D.D.C. July 2, 2018) ..... 15

*Davis v. Pension Ben. Guar. Corp.*,  
571 F.3d 1288–92 (D.C. Cir. 2009) ..... 15

*Decatur Liquors v. Dist. of Columbia*,  
478 F.3d 360 (D.C. Cir. 2007) ..... 32

*Elec. Privacy Info. Ctr. v. Dep’t of Just.*  
15 F. Supp. 3d 32 (D.D.C. 2014) ..... 34

*Elkins v. Dist. of Columbia*,  
690 F.3d 554 (D.C. Cir. 2012) ..... 31

*Emily’s List v. FEC*,  
362 F. Supp. 2d 43 (D.D.C. 2005) ..... 33

*Farris v. Rice*,  
453 F. Supp. 2d 76 (D.D.C. 2006) ..... 16

*Federal Deposit Insurance Corp. v. Mallen*,  
486 U.S. 230 (1988) ..... 29

*Finca Santa Elena, Inc. v. Army Corps of Eng’rs*,  
873 F. Supp. 2d 363–71 (D.D.C. 2012) ..... 20-21

*Fla. Power & Light Co. v. Lorion*,  
470 U.S. 729 (1985) ..... 20

*Food and Water Watch v. EPA*,  
5 F. Supp. 3d 62–81 (D.D.C. 2013) ..... 20

*Fox Ins. Co. v. Sebelius*,

381 Fed. Appx. 93 (2d Cir. 2010) ..... 25

*Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.*,  
460 F.3d 13 (D.C. Cir. 2006) ..... 23

*General Electric Co. v. Jackson*,  
610 F.3d 110 (D.C. Cir. 2010) ..... 30

*Gonzalez Boisson v. Pompeo*,  
459 F. Supp. 3d 7 (D.D.C. 2020) ..... 31-32

*Greenwald v. Becerra*,  
Civ. A. No. 17-797 (LLA), 2024 WL 3617466 (D.D.C. Aug. 1, 2024) ..... 18

*Health Care Auth. v. Shalala*,  
988 F.2d 1221 (D.C. Cir. 1993) ..... 22

*Herbert v. Nat’l Acad. of Scis.*,  
974 F.2d 192 (D.C. Cir. 1992) ..... 14

*Hospitality Staffing Sols., LLC v. Reyes*,  
736 F. Supp. 2d 192 (D.D.C. 2010) ..... 15

*Katz v. Georgetown Uni.*,  
246 F.3d 685 (D.C. Cir. 2001) ..... 39

*King v. Burwell*,  
576 U.S. 473 (2015) ..... 3

*Kowal v. MCI Comm. Corp.*,  
16 F.3d 1271 (D.C. Cir. 1994) ..... 31

*Larsen v. U.S. Navy*,  
525 F.3d 1 (D.C. Cir. 2008) ..... 17

*League of Women Voters of the U.S. v. Newby*,  
838 F.3d 1 (D.C. Cir. 2016) ..... 15

*Lemon v. Geren*,  
514 F.3d 1312 (D.C. Cir. 2008) ..... 17

*Lewis v. Gov’t of the D.C.*,  
161 F. Supp. 3d 15–31 (D.D.C. 2015) ..... 32

*Lovitky v. Trump*,  
918 F.3d 160 (D.C. Cir. 2019) ..... 21

*Lujan v. Defenders of Wildlife*,  
504 U.S. 555 (1992) ..... 14

*Medina v. Dist. of Columbia*,

517 F. Supp. 2d 272 (D.D.C. 2007) ..... 31

*Nat’l Fed’n of Indep. Bus. v. Sebelius*,  
567 U.S. 519 (2012) ..... 3

*Nat’l Min. Ass’n v. McCarthy*,  
758 F.3d 243 (D.C. Cir. 2014) ..... 23

*Nat’l Park Hosp. Ass’n*,  
538 U.S. .... 19

*Nevada v. Dep’t of Energy*,  
457 F.3d 78 (D.C. Cir. 2006) ..... 19

*Nken v. Holder*,  
556 U.S. 418 (2009) ..... 39

*Norton v. S. Utah Wilderness Alliance*,  
542 U.S. 55 (2004) ..... 22

*Oregonians for Floodplain Prot.*,  
334 F. Supp. 3d at 73–74 ..... 19-20, 20

*Papasan v. Allain*,  
478 U.S. 265 (1986) ..... 15

*Power Mobility Coal. v. Leavitt*,  
404 F. Supp. 2d 190 (D.D.C. 2005) ..... 33

*Pursuing Am.’s Greatness v. FEC*,  
831 F.3d 500 (D.C. Cir. 2016) ..... 15

*Save Jobs USA v. Dep’t of Homeland Sec.*,  
105 F. Supp. 3d 108 (D.D.C. 2015) ..... 33

*Shalala v. Illinois Council*,  
529 U.S. 1–20 (2000) ..... 25-26, 26

*Sherley v. Sebelius*,  
644 F.3d 388–93 (D.C. Cir. 2011) ..... 15

*Small v. Avanti Health Sys, LLC*,  
661 F.3d 1180 (9th Cir. 2011) ..... 40

*Solomon v. Off. of the Architect of the Capitol*,  
539 F. Supp. 2d 347 (D.D.C. 2008) ..... 32

*Texas v. United States*,  
86 F. Supp. 3d 591 (S.D. Tex.) ..... 41

*Theodore Roosevelt Conservation P’ship v. Salazar*,

661 F.3d 66 (D.C. Cir. 2011) ..... 17

*Thomas v. Principi*,  
394 F.3d 970 (D.C. Cir. 2005) ..... 14

*Toms v. Off. of the Architect of the Capitol*,  
650 F. Supp. 2d 11–27 (D.D.C. 2009) ..... 32

*Trudeau v. FTC*,  
456 F.3d 178–85 (D.C. Cir. 2006) ..... 23, 39

*Wash. Metro. Area Transit Comm’n v. Holiday Tours, Inc.*,  
559 F.2d 841 (D.C. Cir. 1977) ..... 34

*Weinberger v. Romero-Barcelo*,  
456 U.S. 305 (1982) ..... 40, 41

*Winter v. Nat. Res. Def. Council*,  
555 U.S. 7 (2008) ..... 15, 34, 41

**Statutes, Regulations, Rules, and Other Authorities**

28 U.S.C. § 1346 ..... 22

28 U.S.C. § 1361 ..... 21

28 U.S.C. § 2201 ..... 21

28 U.S.C. §§ 2201, 1361 ..... 21

42 C.F.R. 155.220 ..... 10

42 U.S.C. § 18031 ..... 3

42 U.S.C. § 18032 ..... 5

42 U.S.C. § 18033 ..... 5

42 U.S.C. § 18041 ..... 3, 5

42 U.S.C. § 18083 ..... 5

45 C.F.R. § 155.220 ..... 5

45 C.F.R. §§ 155.220 ..... 23

45 C.F.R. at § 155.220 ..... 24

45 C.F.R. at § 155.221 ..... 24-25

45 C.F.R. § 155.20 ..... 11, 12, 13

45 C.F.R. § 155.200 ..... 5

45 C.F.R. § 155.220 ..... 5, 6, 2, 5, 7, 10, 11, 13, 23, 26

45 C.F.R. § 155.221 ..... 6, 7, 8, 9, 10

45 C.F.R. §§ 155.220 ..... 5, 7, 8, 13, 24

77 Fed. Reg. 18310 (Mar. 27, 2012) ..... 4

77 Fed. Reg. at 18334–36 ..... 5

78 Fed. Reg. 54070 (Aug. 30, 2013) ..... 4

78 Fed. Reg. 65046 ..... 4

78 Fed. Reg. at 54079–80 ..... 10

79 Fed. Reg. 30240 (May 27, 2014) ..... 4

81 Fed. Reg. at 12262, 12339 ..... 6

81 Fed. Reg. at 94122 ..... 6, 7

82 Fed. Reg. 18346 (Apr. 18, 2017) ..... 4

83 Fed. Reg. at 16933-34 (Apr. 17, 2018) ..... 4

83 Fed. Reg. at 16981 ..... 8

84 Fed. Reg. 17454-01, 17515 ..... 6

85 Fed. Reg. at 78618–19 ..... 7

86 Fed. Reg. at 24208–09 ..... 7

5 U.S.C. § 704 ..... 23

5 U.S.C. § 706 ..... 20

5 U.S.C. §§ 551–559, 701–706 ..... 22

8 U.S.C. §§ 2201, 1361 ..... 16, 39

Fed. R. Civ. P. 12 ..... 14, 22



Defendants—certain agencies and officials of the United States responsible for the operation and oversight of the Federally-Facilitated Exchanges and State-based Exchanges on the Federal Platform (“Exchange” or “Exchanges”)<sup>1</sup>—respectfully move to dismiss this action pursuant to Federal Rules of Civil Procedure (“Rules”) 12(b)(1) and 12(b)(6) and oppose the amended motion for a temporary restraining order and preliminary injunction and request for expedited hearing (“Pls.’ Mot.” (ECF No. 9)) filed by Plaintiffs Benefitalign, LLC and TrueCoverage, LLC (collectively “Plaintiffs”).

### INTRODUCTION

Plaintiffs bring this action under the Administrative Procedure Act (“APA”), alleging that Defendants’ suspension was not in accordance with law or with procedure required by law, and was arbitrary and capricious. *See generally* Am. Compl. (ECF No. 8) ¶¶ 34–47. Plaintiffs also claim that the suspension violated the Due Process Clause of the Constitution. *Id.* ¶¶ 48–55.

Centers for Medicare & Medicaid Services (“CMS”) suspended Plaintiffs, each of whom are enhanced direct enrollment entities and private health insurance web-brokers, from accessing the Exchanges’ information technology systems, which prevents Plaintiffs from assisting consumers with submitting applications for and enrollments in health insurance plans and insurance affordability programs offered on the Exchanges through their direct enrollment platforms. CMS also suspended Plaintiffs’ ability to make their direct enrollment platforms available to other agents and brokers to assist consumers with submitting applications for and

---

<sup>1</sup> “Exchange” or “Exchanges” refer to both the Federally-facilitated Exchanges and the State-based Exchanges on the Federal Platform. In this brief and the annexed exhibits, these “Exchanges” are sometimes referred to as “Federally-facilitated Marketplaces,” “State-based Marketplaces on the Federal Platform” “Marketplaces,” “FFM,” “FFE,” “SBM-FP,” and “SBE-FP”. The terms are all interchangeable and hereinafter refer to simply as “Exchange or “Exchanges.”

enrollments in health insurance plans and insurance affordability programs offered on the Exchanges.

The suspension was implemented because CMS learned that Plaintiffs were engaging in potentially dangerous behavior and received reports of concerning behavior and serious breaches of Plaintiffs' and CMS's agreements. CMS determined Plaintiffs' behavior and the serious breaches compromised and placed consumers' personally identifiable information ("PII") and the integrity of the Exchanges at risk. CMS concluded that it needed to immediately suspend the Plaintiffs' connection to CMS systems Exchanges and their ability to operate as web brokers to prevent any further damage.

During the suspension, however, CMS-registered agents and brokers affiliated with Plaintiffs can continue to assist Exchange consumers with submitting applications and enrolling in Exchange coverage using another approved entity's Classic direct enrollment platform or Enhanced direct enrollment platform, using the Exchanges' Call Center on a three-way call with the enrollees or applicants, or by assisting an enrollee or applicant side-by-side on HealthCare.gov (also referred to as the Exchange Pathway). This will remain the case unless and until the Plaintiffs' Exchange Agreements are suspended or terminated under 45 C.F.R. § 155.220(f)(4) or (g)(4).

Nevertheless, Plaintiffs' motion minimizes the serious risk and their breaches of their contractual obligations and applicable CMS regulations. As mentioned, Plaintiffs' conduct compromised consumers' PII and the integrity of, and confidence in, the Exchanges, and exposed consumers' PII, the Exchanges, and CMS systems to foreign actors, such as users from overseas locations including India and Pakistan and potentially Saudi Arabia and Singapore. This is not the first time CMS had to take enforcement action to address Plaintiffs' non-compliance with CMS's

rules and regulations. Plaintiffs feigned concern that their suspension will harm consumers does not outweigh the harms that Plaintiffs expose consumers and the Exchanges to. The government had to take immediate action and the government, not Plaintiffs, is acting to protect consumers from any further harm.

## STATUTORY AND REGULATORY BACKGROUND

### I. **Web-Brokers, Enhanced Direct Enrollment Entities, Direct Enrollment Entities, and Their Participation in the Exchanges Under the Affordable Care Act.**

In 2010, Congress enacted the Patient Protection and Affordable Care Act (the “Act”)<sup>2</sup> with the aim of “increas[ing] the number of Americans covered by health insurance and decreas[ing] the cost of health care.” *Nat’l Fed’n of Indep. Bus. v. Sebelius*, 567 U.S. 519, 538 (2012). The Act established, among other things, a series of new insurance market reforms in the individual and small group markets and also imposed a number of other requirements for health insurance plans in those markets. *See City of Columbus v. Trump*, 453 F. Supp. 3d 770, 778–79 (D. Md. 2020) (describing the Act’s reforms).

To facilitate a market for health insurance products that conform to its market reforms, the Act established “Health Benefit Exchanges” or State-based virtual marketplaces where consumers can purchase qualified health plans. *See* 42 U.S.C. § 18031. The Act “requires the creation of an ‘Exchange’ in each State—basically, a marketplace that allows people to compare and purchase insurance plans [and] gives each State the opportunity to establish its own Exchange, but provides that the Federal Government will establish the Exchange if the State does not.” *King v. Burwell*, 576 U.S. 473, 479 (2015). The Act thus provides for the establishment of Federal-facilitated Exchanges in States that chose not to establish their own Exchanges. 42 U.S.C. § 18041(c)(1).

---

<sup>2</sup> Pub. L. No. 111-148, 124 Stat. 119 (2010), as amended by the Health Care and Education Reconciliation Act, Pub. L. No. 111-152, 124 Stat. 1029 (2010).

Some States operate a State-based Exchange on the Federal Platform, which is a type of State Exchange that relies on the Department of Health and Human Services (“HHS”) services for performing certain Exchange functions, particularly eligibility and enrollment functions, while still retaining responsibility for performing certain other Exchange functions, such as qualified health plan certification and consumer outreach and assistance functions. *See* State-based Exchanges | CMS, <https://www.cms.gov/ccio/resources/fact-sheets-and-faqs/state-marketplaces> (last accessed Sept. 20, 2024) . In addition, HealthCare.gov, the Exchange website administered by HHS, is the Exchange website available to consumers in states with a State-based Exchange on the Federal Platform as well as consumers in states served by a Federal Exchange. *See* State Health Insurance Marketplace Types, 2024 | KFF, <https://www.kff.org/affordable-care-act/state-indicator/state-health-insurance-marketplace-types/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D> (last accessed Sept. 20, 2024). Since the Act’s enactment, HHS has engaged in numerous rulemakings to implement various aspects of the law. *See* 83 Fed. Reg. at 16933-34 (Apr. 17, 2018) (Patient Protection and Affordable Care Act; HHS Notice of Benefit and Payment Parameters for 2019) (describing prior rulemakings).<sup>3</sup>

The Act directed the Secretary to establish procedures under which a State may permit agents or brokers to enroll individuals and employers in qualified health plans offered through an Exchange in the individual or small group market and to assist individuals in applying for financial

---

<sup>3</sup> These rulemakings have addressed the frameworks for Exchanges, *see, e.g.* 77 Fed. Reg. 18310 (Mar. 27, 2012) (“Exchange Establishment Rule”); 82 Fed. Reg. 18346 (Apr. 18, 2017) (“Market Stabilization Rule”); health insurance market standards, *see, e.g.*, 79 Fed. Reg. 30240 (May 27, 2014) (“2015 Market Standards Rule”); as well as program integrity standards, *see, e.g.*, 78 Fed. Reg. 54070 (Aug. 30, 2013) (“first Program Integrity Rule”), 78 Fed. Reg. 65046 Oct. 30, 2013) (“second Program Integrity Rule”).

assistance for qualified health plans sold through an Exchange. 42 U.S.C. § 18032(e). The Act also directed the Secretary to establish, subject to certain minimum requirements, a streamlined process for enrollment in qualified health plans and all insurance affordability programs. *Id.* § 18083(a), (b). The Act delegates to the Secretary authority to implement any measure or procedure the Secretary determines is appropriate to reduce fraud and abuse. *Id.* § 18033(a)(5)(A). The Act also grants the Secretary broad authority to establish standards and issue regulations to implement the statutory requirements related to Exchanges, qualified health plans, and other components of title I of the Act and broadly authorizes the Secretary to implement “other requirements as the Secretary determines appropriate.” 42 U.S.C. 18041(a).

Pursuant to the authority granted under the Act, the Secretary adopted 45 C.F.R. § 155.220, establishing standards and requirements applicable to web-brokers<sup>4</sup> assisting individuals, employers, or employees with enrollment in qualified health plans and insurance affordability programs offered through an Exchange. *See* 77 Fed. Reg. at 18334–36. For example, web-brokers must take annual training on Exchange coverage options and insurance affordability programs, comply with Exchange privacy and security standards, and complete registration with the Exchange in advance of assisting with enrollments through a Federal Exchange or State-based Exchange on the Federal Platform. 45 C.F.R. § 155.220(d), (l). HHS “or its designee” is

---

<sup>4</sup> The regulatory definition of a “web-broker” includes an individual agent or broker, group of agents or brokers, or business entity registered with an Exchange under 45 C.F.R. § 155.220(d)(1) that develops and hosts a non-Exchange website that interfaces with an Exchange to assist consumers with direct enrollment in qualified health plans offered through the Exchange as described in 45 C.F.R. §§ 155.220(c)(3) or 155.221. The term also includes an agent or broker direct enrollment technology provider. *Id.* Agent or broker direct enrollment technology provider means a type of web-broker business entity that is not a licensed agent or broker under State law and has been engaged or created by, or is owned by an agent or broker, to provide technology services to facilitate participation in direct enrollment under 45 C.F.R. §§ 155.220(c)(3) and 155.221. *See* 45 C.F.R. § 155.200 (definition of “agent or broker direct enrollment technology provider”).

authorized to “periodically monitor and audit” web-brokers.<sup>5</sup> 2017 Payment Notice, 81 Fed. Reg. at 12262, 12339 (adding 45 C.F.R. § 155.220(c)(5)). Using these same statutory authorities, the Secretary also adopted 45 C.F.R. § 155.221, establishing standards for direct enrollment entities, and enabling third-parties to perform audits of these direct enrollment entities. *See* 81 Fed. Reg. at 94122.

There are two forms of direct enrollment available in states with a Federal Exchange or State-based Exchange on the Federal Platform: (1) Classic direct enrollment, and (2) Enhanced direct enrollment. *See* Grant Decl., submitted herewith. In Classic direct enrollment, consumers start on a direct enrollment entity’s website by indicating they are interested in Exchange coverage. *See* Direct Enrollment and Enhanced Direct Enrollment | CMS, <https://www.cms.gov/marketplace/agents-brokers/direct-enrollment-partners> (last accessed Sept. 20, 2024). The direct enrollment entity’s website redirects users to HealthCare.gov to complete the Exchange eligibility application. *Id.* After completing their application, HealthCare.gov redirects the consumer back to the direct enrollment entity’s website to shop for, and potentially enroll in, a qualified health plan and insurance affordability programs offered through the Exchange. Enhanced direct enrollment, on the other hand, is a service that allows approved enhanced direct enrollment entities to provide a comprehensive consumer experience. *See id.* This experience includes the eligibility application, Exchange enrollment, and post-enrollment year-round customer service capabilities for consumers and agents or brokers working on behalf of consumers. *Id.* All of this activity happens directly on issuer and web-broker websites. Through enhanced direct enrollment, approved direct enrollment entities build and host a version of the

---

<sup>5</sup> The reference to web-brokers was added to 45 C.F.R. § 155.220(c) in the 2020 Payment Notice. *See* 84 Fed. Reg. 17454-01, 17515 and 17564 (Apr. 25, 2019).

HealthCare.gov eligibility application directly on their websites. *Id.* These websites are designed to securely integrate with a back-end suite of Exchange application programming interfaces to support application, enrollment, and more. *See id.* This experience includes the eligibility application, Exchange enrollment, and post-enrollment year-round customer service capabilities for consumers and agents or brokers working on behalf of consumers. *Id.* All of this activity happens directly on issuer and web-broker websites. *Id.* Through enhanced direct enrollment, approved direct enrollment entities build and host a version of the HealthCare.gov eligibility application directly on their websites. *Id.* These websites are designed to securely integrate with a back-end suite of Exchange application programming interfaces to support application, enrollment, and more.

Web-brokers who want to assist consumers with direct enrollment in qualified health plans offered through Exchanges must first demonstrate operational readiness to HHS on an annual basis before the web-broker's non-Exchange internet website can be used to assist consumers with eligibility determinations or plan selection. *See* 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4); *see also* 85 Fed. Reg. at 78618–19. Web-brokers who only participate in Classic direct enrollment are only required to comply with the operational readiness review requirements in 45 C.F.R. § 155.220(c)(6). *See* 85 Fed. Reg. at 78618–19; *see also* 86 Fed. Reg. at 24208–09. A direct enrollment entity must also engage an independent third-party entity to conduct an initial readiness review as well as an annual readiness review. *See* 45 C.F.R. § 155.221(f). This third-party review is intended to demonstrate the direct enrollment entity's operational readiness and compliance with applicable requirements before the entity may use its non-Exchange website to complete an Exchange eligibility application or a qualified health plan selection. *See* 45 C.F.R. §§ 155.220(c)(6), 155.221(f).

These third-party auditors must comply with the Secretary's standards. *See* 83 Fed. Reg. at 16981; 45 C.F.R. § 155.221(g). The third-party auditors are "subject to HHS oversight," 83 Fed. Reg. at 16981; 45 C.F.R. § 155.221(f). The auditors must cooperate with HHS or its designee when HHS conducts an audit, inspection, or other evaluation, and provide access to the third-party entities' records and systems relating to their audits of a direct enrollment entity. *Id.* § 155.221(g)(7). In addition, "the agent, broker, or issuer will remain responsible for compliance with all applicable direct enrollment requirements." 83 Fed. Reg. at 16981. Web-brokers who are direct enrollment entities must enter into Exchange Agreements with CMS as part of demonstrating operational readiness on an annual basis. 45 C.F.R. §§ 155.220(c)(6)(v), 155.221(b)(4)(ii)(A), (v).

## **II. Oversight, Enforcement, and Rebuttal Opportunity**

When CMS receives credible information about a direct enrollment entity's potential non-compliance with applicable requirements that requires further investigation, or discovers circumstances that pose unacceptable risk to Exchange operations or Exchange information technology systems, it may immediately suspend a direct enrollment entity or web-broker's access to CMS systems and their ability to transact information with the Exchanges to protect consumers and the integrity of the Exchanges while it conducts an investigation. *See* 45 C.F.R. §§ 155.220(c)(4)(ii), 155.221(e); *see also* Busby Dec., submitted herewith, Ex. I, Interconnection Security Agreement ("Interconnection Agreement"), Section 15. Compliance and Section 16. Termination, at 20, Busby Dec. Ex. F, Enhanced Direct Enrollment Business Agreement ("Enhanced Direct Enrollment Agreement"), Section V. Termination, at 8-10. Under the plain terms of the agreement entered into by the direct enrollment entity, the entity must cooperate with the resulting investigation.



The Interconnection Agreement allows CMS to terminate an entity's access to the Exchanges for non-compliance with the terms of the agreement or unmitigated security risks. This Agreement requires entities to maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system with the highest sensitivity levels. The Interconnection Agreement prohibits an entity from releasing, publishing, or disclosing information to unauthorized personnel.

Non-compliance with the privacy and security standards and operational requirements under the Enhanced Direct Agreement by the Entity, regardless of whether it rises to the level of a material breach of that agreement, may lead to termination of the interconnection between the Parties. CMS may block the entity's access to the Exchanges based on the existence of unmitigated privacy or security risks, or the misuse of the personally identifiable information of consumers. CMS may immediately suspend the entity's ability to access Exchange systems if CMS discovers circumstances that pose unacceptable or unmitigated risk to the Exchanges. If the CMS imposes a suspension, CMS will provide written notice within two business days of imposing a suspension.

CMS may immediately suspend a direct enrollment entity's connection to CMS Exchange information technology systems "if HHS discovers circumstances that pose unacceptable risk to the accuracy of the Exchange's eligibility determinations, Exchange operations, or Exchange information technology systems." 45 C.F.R. § 155.221(e). The Secretary will notify the direct enrollment entity of the suspension and provide an opportunity to submit rebuttal evidence and information, or otherwise demonstrate that the circumstances of the incident or breach are sufficiently remedied or mitigated to HHS's satisfaction before the suspension may be lifted. *Id.* CMS, on behalf of HHS, reviews the evidence and information submitted by the direct enrollment

entity to determine if the circumstances of the incident or breach are sufficiently remedied or mitigated to warrant reinstating their system access. *Id.* CMS also has authority to immediately suspend a web-broker's ability to make its non-Exchange website available to other agents and brokers who assist consumers with Exchange applications and enrollments if HHS discovers a security and privacy incident or breach. 45 C.F.R. § 155.220(c)(4)(ii). In such a case HHS must follow its incident response plan to address privacy and security incidents and breaches. 78 Fed. Reg. at 54079–80. Under the incident response plan, HHS may need to temporarily suspend a web-broker's connection to CMS systems and the web-broker's ability to make its non-Exchange website available to other agents and brokers to prevent further damage from the incident or breach. *Id.* The temporary suspension is intended to allow HHS to conduct an investigation and otherwise work with the web-broker to remedy the breach or incident to HHS's satisfaction. *Id.*

In situations where the suspended entity does not provide rebuttal evidence and information, or the evidence and information submitted does not sufficiently remedy or mitigate the circumstances of the incident or breach to HHS' satisfaction, CMS will not lift the suspension to reinstate the entity's system access. 42 C.F.R. 155.220(c)(4)(ii). In that case—where rebuttal evidence or information is not submitted, or where it is insufficient to mitigate the potential security breach—CMS will pursue a suspension or termination of the entity's Exchange Agreements. *See, e.g.*, 45 C.F.R. § 155.220(g). An enforcement action under § 155.220(g) to suspend or terminate a web-broker's Exchange Agreements results in the web-broker no longer being registered with the Exchanges. 45 C.F.R. § 155.220(g)(4) and (5)(iii). When CMS suspends or terminates a web-broker's Exchange Agreements, the web-broker can no longer assist with or facilitate enrollment of individual consumers or employers and their employees in coverage through a Federal Exchange or State-based Exchange on the Federal Platform or assist individuals

in applying for financial assistance for Exchange coverage. *Id.* These web-brokers cannot submit Exchange applications and enrollments through any of the available pathways—i.e., through Classic direct enrollment, Enhanced direct enrollment, the Exchange Call Center, and/or through HealthCare.gov. A web-broker whose Exchange Agreements are terminated can request reconsideration of such action. *See* 45 C.F.R. § 155.220(h)(1). HHS is required to provide written notice of its reconsideration decision within 60 calendar days of receipt of the reconsideration request. 45 C.F.R. § 155.220(h)(3). The agency’s decision on reconsideration then becomes the agency’s final decision. *Id.*

### **FACTUAL AND PROCEDURAL BACKGROUND**

Plaintiff BenefitAlign is an enhanced direct enrollment entity and Plaintiff TrueCoverage, is a private health insurance agency and, is a private health insurance web-broker. Am. Compl. (ECF No. 8) ¶¶ 6–7; *see* 45 C.F.R. § 155.20 (definition “web-broker”); *see* Grant Decl. In order to participate in the Exchange as approved web-brokers and Enhanced direct enrollment partners in the Exchange, both Plaintiffs entered into Enhanced Direct Agreements and Web-Broker Agreements with CMS. *See* Busby Dec. Exs. E, F, G, and H. Plaintiffs enter into the Enhanced Direct Enrollment and Web-Broker Agreements with CMS annually. In addition, Plaintiff Benefitalign also participates as direct enrollment partner in the Exchange and entered into an Interconnection Agreement with CMS. Busby Dec. Ex. I.

On July 23, 2024, CMS’s Information Technology Service Desk received an email from an agent/broker, stating that a company had fraudulently used his credentials that led to the suspension of his access to the Exchange systems. Busby Decl. Ex. B. Also, attached to the email was a complaint filed in the U.S. District Court for the Southern District of Florida against Plaintiff TrueCoverage, LLC and the parent corporation of both Plaintiffs in this lawsuit, Speridian Technologies, LLC. Ex. A; *see also* *Turner v. Enhance Health, LLC*, Civ. A. No. 24-60591 (S.D.

Fla. Apr. 12, 2024), ECF No. 1. In addition, attached to the email were declarations raising concerning allegations against both Plaintiffs and their parent company Speridian.

On July 29, 2024, CMS's Security Operations Center received a report that the Speridian Companies' Customer Relationship Management system may be based overseas, which would violate its Agreements with CMS. CMS became concerned that the privacy and security of Exchange data, including consumer PII, was processed or stored outside of the United States, which is a violation of the Exchange agreements. Accordingly, CMS performed a supply chain risk assessment and on August 6, 2024, "[t]he assessment concluded that the overall risk to CMS data and information systems was critical, meaning that the product, service or supplier contains vulnerabilities or weaknesses that are wholly exposed and easily exploitable." *See* Busby Decl. The next day, CMS initiated a "privacy risk assessment...to assess whether there was a high likelihood that the Speridian Companies were transmitting or storing [Exchange] data outside their approved environment and/or outside of the United States." *Id.* ¶ 7.

On August 8, 2024, CMS concluded that there was sufficient evidence that the Speridian Companies' platforms could be accessed by systems that were not authorized by the agreements between CMS and the Speridian Companies,' both inside and outside of the United States and immediately suspended Plaintiffs' access to the Exchange. *Id.* ¶ 11. The suspension "is a temporary situation" to allow "CMS [to] continue[] its review of apparent breaches...[and] to protect the public until CMS can [complete its assessment]." *See id.* ¶ 12.

On August 13, 2024, CMS met with Plaintiffs again and "discussed reports of improper access to CMS systems from outside of the United States, in addition to reports that [Exchange] data were being transmitted and stored in non-CMS approved systems in foreign countries." *Id.* ¶ 13. Plaintiffs disputed CMS's assessment. *Id.* CMS requested that Plaintiffs produce information.

After reviewing the information Plaintiffs provided, CMS had concerns that “three [internet protocol] addresses belong to companies known for providing [virtual private network] services, [that could be] used...to mask locations or encrypt internet traffic...[that] might [be used to] bypass geoblocking and reach destinations outside the [United States].” *Id.*

On August 15, 2024, CMS met again with Plaintiffs and requested additional information including “system logs . . . to verify the reported location of the internet protocol (IP) addresses connecting to [Plaintiffs’] information systems and the data accessed in those information systems.” *Id.* ¶ 17. CMS sought information about measures Plaintiffs “have put in place to prevent overseas users from using [virtual private networks] to connect to the information systems that contained CMS data and transmit the data to other locations.” *Id.*

CMS continued reviewing information that Plaintiffs produced, and new concerns developed. For example, “data analysis revealed multiple other anomalies, including access to the [Plaintiffs’] [electronic data exchange] platforms by at least eleven unique users from overseas locations, including in India and Pakistan.” *Id.* ¶ 17.

On August 29, 2024, Plaintiffs filed this action bringing claims under the APA and alleging a violation of the Due Process Clause. *See generally* Compl. (ECF No. 1).

On September 2, 2024, CMS sent its suspension and audit notice, pursuant to 45 C.F.R. §§ 155.220(c)(4)(ii) and 155.221(e), and attributable to credible allegations of misconduct, CMS had suspended Plaintiffs’ ability to transact with the Exchanges and their ability to make their platforms available to other agents and brokers to transact with the Exchanges. *See id.* ¶ 24. In addition, pursuant to 45 C.F.R. § 155.220(c)(5), the Enhanced Direct Agreement, the Web-Broker Agreement, and the Interconnection Agreement, CMS notified Plaintiffs of its intent to conduct a compliance review and audit. *Id.* Subsequently thereafter, Plaintiffs amended their complaint and

their motion for a temporary restraining order, preliminary injunction, and hearing, *see generally* ECF Nos. 8 and 9.

Defendants now move to dismiss Plaintiffs' amended complaint pursuant to Rule 12(b)(1) and 12(b)(6) and opposes Plaintiffs' motion.

## LEGAL STANDARDS

### I. Rule 12(b)(1)

Under Rule 12(b)(1), a plaintiff bears the burden of establishing jurisdiction by a preponderance of the evidence. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). A court considering a Rule 12(b)(1) motion must “assume the truth of all material factual allegations in the complaint and ‘construe the complaint liberally, granting plaintiff the benefit of all inferences that can be derived from the facts alleged.’” *Am. Nat’l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011) (quoting *Thomas v. Principi*, 394 F.3d 970, 972 (D.C. Cir. 2005)). A court may examine materials outside the pleadings as it deems appropriate to resolve the question of its jurisdiction. *See Herbert v. Nat’l Acad. of Scis.*, 974 F.2d 192, 197 (D.C. Cir. 1992).

### II. Rule 12(b)(6)

Under Rule 12(b)(6), the Court may dismiss a Complaint where a plaintiff fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion to dismiss, “a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). When resolving a motion to dismiss pursuant to Rule 12(b)(6), the pleadings are construed broadly so that all facts pleaded therein are accepted as true, and all inferences are viewed in a light most favorable to the plaintiff. *See Iqbal*, 556 U.S. at 678. However, a court is not required to accept conclusory allegations or unwarranted factual

deductions as true. *Id.* “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* Likewise, a court need not “accept as true a legal conclusion couched as a factual allegation.” *Papasan v. Allain*, 478 U.S. 265, 286 (1986). Ultimately, the focus is on the language in the complaint and whether that sets forth sufficient factual allegations to support a plaintiff’s claims for relief.

### **III. Preliminary Injunction**

“A preliminary injunction is an extraordinary remedy never awarded as of right.” *Winter v. Nat. Res. Def. Council*, 555 U.S. 7, 24 (2008). A party seeking preliminary relief must make a “clear showing that four factors, taken together, warrant relief: likely success on the merits, likely irreparable harm in the absence of preliminary relief, a balance of the equities in its favor, and accord with the public interest.” *League of Women Voters of the U.S. v. Newby*, 838 F.3d 1, 6 (D.C. Cir. 2016) (quoting *Pursuing Am.’s Greatness v. FEC*, 831 F.3d 500, 505 (D.C. Cir. 2016)). The moving party bears the burden of persuasion and must demonstrate, “by a clear showing,” that the requested relief is warranted. *Hospitality Staffing Sols., LLC v. Reyes*, 736 F. Supp. 2d 192, 197 (D.D.C. 2010) (quoting *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006)).

Before the Supreme Court’s decision in *Winter*, courts weighed these factors on a “sliding scale,” allowing “an unusually strong showing on one of the factors” to overcome a weaker showing on another. *Damus v. Nielsen*, Civ. A. No. 18-0578 (JEB), 2018 WL 3232515, at \*4 (D.D.C. July 2, 2018) (quoting *Davis v. Pension Ben. Guar. Corp.*, 571 F.3d 1288, 1291–92 (D.C. Cir. 2009)). This Circuit has hinted, though not held, that *Winter*—which overturned the Ninth Circuit’s “possibility of irreparable harm” standard—establishes that “likelihood of irreparable harm” and “likelihood of success” are “independent, free-standing requirement[s].” *Sherley v. Sebelius*, 644 F.3d 388, 392–93 (D.C. Cir. 2011); *see also League of Women Voters*, 838 F.3d at

7 (declining to address whether “sliding scale” approach is valid after *Winter*). And where, as here, a party “seeks a mandatory injunction—to change the status quo through action rather than merely to preserve the status quo—typically the moving party must meet a higher standard than in the ordinary case: the movant must show ‘clearly’ that [it] is entitled to relief or that extreme or very serious damage will result.” *Farris v. Rice*, 453 F. Supp. 2d 76, 78 (D.D.C. 2006).

## ARGUMENT

The Court should dismiss Plaintiffs’ Amended Complaint because it lacks jurisdiction over Plaintiffs’ claims and Plaintiffs fail to state a claim upon which relief may be granted. Should this Court however find that jurisdiction resides within this Court and Plaintiffs have stated a claim upon which relief can be granted, Plaintiffs’ request for temporary restraining order, preliminary injunction motion, and request for a hearing should be denied. Plaintiffs simply have not established that they are entitled to this extraordinary remedy. For the reasons discussed further below, the Court should dismiss this matter in its entirety and deny Plaintiffs’ Motion.

### **I. This Action Should Be Dismissed for Lack of Jurisdiction.**

The Court should find that its lacks jurisdiction over Plaintiffs’ claims because any challenges relating to the August 8, 2024, Suspension Email (“August 8 Email”) are moot, any challenges relating to the suspension are not ripe, and there are no allegations to establish subject matter jurisdiction under 8 U.S.C. §§ 2201, 1361, and 1346.

#### **A. Any Claims Related to the August 8 Email Are Moot.**

To the extent Plaintiffs claim that the August 8 Email was not in accordance with law or with procedure required by law and was arbitrary and capricious and violated the Due Process Clause, these claims are moot.

Federal courts lack subject matter jurisdiction to decide moot questions. *Burke v. Barnes*, 479 U.S. 361, 363 (1987) (“Article III of the Constitution requires that there be a live case or



controversy at the time that a federal court decides the case”). A case or claim becomes moot “when the issues presented are no longer live or the parties lack a legally cognizable interest in the outcome.” *Larsen v. U.S. Navy*, 525 F.3d 1, 3-4 (D.C. Cir. 2008) (quoting *County of Los Angeles v. Davis*, 440 U.S. 625, 631 (1979)). Thus, mootness deprives the court of jurisdiction and requires dismissal “when intervening events make it impossible to grant the prevailing party effective relief.” *Lemon v. Geren*, 514 F.3d 1312, 1315 (D.C. Cir. 2008). “If it becomes impossible for the court to grant any effectual relief *whatever* to a prevailing party on a particular claim, that claim must be dismissed,” *Theodore Roosevelt Conservation P’ship v. Salazar*, 661 F.3d 66, 79 (D.C. Cir. 2011) (emphasis added and internal quotations omitted), “[n]o matter how vehemently the parties continue to dispute the lawfulness of the conduct that precipitated the lawsuit.” *Already, LLC v. Nike, Inc.*, 568 U.S. 85, 91 (2013).

Here, the August 8 Email, and any purported deficiencies, has been superseded by the September 2, 2024 “Suspensions of Web-broker and Enhanced Direct Enrollment Entity Activities and Notice of Compliance Audit” notice (the “September 2 Notice”), which provides a detailed explanation and additional grounds for suspending Plaintiffs’ access to the Exchanges’ information technology systems and their ability to make their direct enrollment platforms available to other agents and brokers to transact information with the Exchanges. *See* Busby Dec. ¶ 24. The September 2 Notice not only incorporates the August 8 Email but also supplements the basis for the suspension with additional information gathered between August 8 and September 2 and leverages additional regulatory authority for suspending Plaintiffs’ Exchange system access. *Compare id. with* Busby Dec. ¶ 11. Indeed, courts in this district regularly find that actions challenging superseded agency policies or decision documents are moot because they no longer present a live controversy. *See, e.g., Theodore Roosevelt Conservation P’ship*, 661 F.3d at 79

(finding that a superseded agency policy document “no longer exists” and any action brought to challenge it is moot); *Greenwald v. Becerra*, Civ. A. No. 17-797 (LLA), 2024 WL 3617466, at \*7 (D.D.C. Aug. 1, 2024) (Medicare contractor issuing new local coverage determination rendered the lawsuit challenging the original local coverage determination moot); *Blue Water Balt. v. Pruitt*, 266 F. Supp. 3d 174, 180–81 (D.D.C. 2017) (determining that where a newly issued EPA report superseded the previous iteration of the report, it “thus moot[ed] the plaintiffs’ challenge to the reclassifications in the [original report]”).

Thus, the September 2 Notice renders any challenges or claims Plaintiffs may have relating to the August 8 Email moot and the Court should dismiss any such claims for lack of jurisdiction.

**B. Plaintiffs’ Claims Are Not Ripe.**

This Court lacks subject matter jurisdiction over Plaintiffs’ claims because Plaintiffs’ claims are not ripe. The ripeness doctrine requires that a litigant’s claims be “constitutionally and prudentially ripe,” so as to protect: (1) “the agency’s interest in crystallizing its policy before that policy is subjected to judicial review,” (2) “the court’s interests in avoiding unnecessary adjudication and in deciding issues in a concrete setting,” and (3) “the petitioner’s interest in prompt consideration of allegedly unlawful agency action.” *Asante v. Azar*, 436 F. Supp. 3d 215, 224 (D.D.C. 2020) (quoting *Nevada v. Dep’t of Energy*, 457 F.3d 78, 83–84 (D.C. Cir. 2006)). “Ripeness is a justiciability doctrine designed to prevent the courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements over administrative policies, and also to protect the agencies from judicial interference until an administrative decision has been formalized and its effects felt in a concrete way by the challenging parties.” *Nat’l Park Hosp. Ass’n v. Dep’t of the Interior*, 538 U.S. 803, 807–08 (2003) (quoting *Abbott Labs. v. Gardner*, 387 U.S. 136, 148–49 (1967)). Here, Plaintiffs fail to demonstrate that their claims are prudentially ripe.

Here, Plaintiffs can not demonstrate that their claims are prudentially ripe. In order to satisfy the prudential elements of ripeness courts consider “(1) the fitness of the issues for judicial decision and (2) the hardship to the parties of withholding court consideration.” *Nat’l Park Hosp. Ass’n*, 538 U.S. at 808. In actions against agencies, the inquiry focuses on: “(1) whether delayed review would cause hardship to the plaintiffs; (2) whether judicial intervention would inappropriately interfere with further administrative action; and (3) whether the courts would benefit from further factual development of the issues presented.” *Nevada v. Dep’t of Energy*, 457 F.3d 78, 84 (D.C. Cir. 2006) (quoting *Ohio Forestry Ass’n v. Sierra Club*, 523 U.S. 726, 733 (1998)).

Here, Plaintiffs attempt to challenge the suspension, *see generally* Am. Compl. (ECF No. 8), however, as elaborated further below, Plaintiffs do not challenge any final agency action. The suspension and the September 2 Notice is merely the first stage of a process, which is underway. As the September 2 Notice advised Plaintiffs, there is a need for the Defendants to conduct an audit because of reports and information showing potential, credible, and serious lapses and security breaches by Plaintiffs. *See* Busby Dec. ¶ 24; *see also* Wu Decl. Ex. A. Defendants have issued no formal findings at this time and the September 2 Notice is not the consummation of Defendants’ fact finding. During the audit, Plaintiffs will be able to produce evidence, explain any discrepancies found during such review, and challenge any findings from the audit, and reopening Plaintiffs’ access to the Exchanges and permitting other agents and brokers to use Plaintiffs’ direct enrollment platforms to transact information with the Exchanges at this time would circumvent the administrative process. The outcome of process is unknown at this time, and judicial intervention would impede this administrative process and inappropriately interfere with further administrative action. Therefore, dismissal is warranted. *See Oregonians for*

*Floodplain Prot.*, 334 F. Supp. 3d at 73–74 (dismissing on ripeness grounds in part to not interfere with the administrative process); *Food and Water Watch v. EPA*, 5 F. Supp. 3d 62, 80–81 (D.D.C. 2013) (same). And any “theoretical possibility of future hardship arising from the Court’s decision to withhold review until the agency’s position is settled does not overcome the finding that the case is not yet ‘fit’ for judicial resolution.” *Belmont Abbey Coll. v. Sebelius*, 878 F. Supp. 2d 25, 41 (D.D.C. 2012).

Also, “[t]his Circuit has previously held that courts should refrain from ‘intervening into matters that may best be reviewed at another time or in another setting, even if the issue presented is purely legal and otherwise fit for review.’” *Id.* at 41. (internal quotations and citations omitted). The Court would benefit from further factual development of the issues presented in this case. If Plaintiffs eventually challenge Defendants’ final agency action under the APA, the Court will have the benefit of an administrative record, compiled by the agency, reflecting what the agency considered in making its decision and the agency’s explanation for its final agency action. *See Fla. Power & Light Co. v. Lorion*, 470 U.S. 729, 744 (1985) (“[T]he task of the reviewing court is to apply the appropriate APA standard of review, 5 U.S.C. § 706, to the agency decision based on the record the agency presents to the reviewing court.”); *see also* 5 U.S.C. § 706 ([T]he court shall review the whole record...). This factor also militates against review at this time. *See Oregonians for Floodplain Prot.*, 334 F. Supp. 3d at 73–74 (dismissing on ripeness grounds in part to allow for further factual development); *Food and Water Watch*, 5 F. Supp. 3d at 80–81 (same).

“Because of the prudential considerations which innervate the ripeness doctrine,” courts will dismiss claims “‘even if there is not a constitutional bar to the exercise of [ ] jurisdiction’” *Full Value Advisors*, 633 F. 3d at 1106 (internal quotation marks and citation omitted), and thus

dismissal is warranted in this matter. *See, e.g., Finca Santa Elena, Inc. v. Army Corps of Eng'rs*, 873 F. Supp. 2d 363, 370–71 (D.D.C. 2012) (granting motion to dismiss based on lack of prudential ripeness).

**C. Plaintiffs' Other Assertions of Jurisdiction Also Fail.**

Plaintiffs assert jurisdiction under a host of other statutes, including 28 U.S.C. §§ 2201, 1361, and 1346; however, Plaintiffs have failed to meet their burden and establish that the Court has jurisdiction under any of these statutes.

First, Plaintiffs assert jurisdiction under the Declaratory Judgment Act (28 U.S.C. § 2201). *See* Am. Compl. ¶ 13. But that statute does not provide this Court with an independent source of federal subject matter jurisdiction. *California v. Texas*, 593 U.S. 659, 672 (2021) (“The Declaratory Judgment Act, 28 U.S.C. § 2201, alone does not provide a court with jurisdiction.”); *Lovitky v. Trump*, 918 F.3d 160, 161 (D.C. Cir. 2019) (“But § 2201 (declaratory judgment) is not an independent source of federal jurisdiction.” (citations and internal quotations omitted)); *see also C&E Servs., Inc. v. D.C. Water & Sewer Auth.*, 310 F.3d 197, 201 (D.C. Cir. 2002) (“[W]e begin with the well-established rule that the Declaratory Judgment Act is not an independent source of federal jurisdiction.” (internal quotation omitted)). Accordingly, Plaintiffs are not entitled to any relief under 28 U.S.C. § 2201.

Plaintiffs also assert mandamus jurisdiction. Am. Compl. (ECF No. 8) ¶ 13 (citing 28 U.S.C. § 1361). Similar to their declaratory judgment claim, Plaintiffs cannot establish jurisdiction under this statute. Separate from the failure to establish jurisdiction, the remedy of mandamus is “one of ‘the most potent weapons in the judicial arsenal.’” *Cheney v. U.S. Dist. Ct. for Dist. Of Columbia*, 542 U.S. 367, 380 (2004). Due to the potential conflict between the branches of government engendered by use of this remedy, courts have limited its application to “only . . . the clearest and most compelling cases.” *13th Reg'l Corp., v. Dep't of Interior*, 654 F.2d 758, 760

(D.C. Cir. 1980). The Amended Complaint is devoid of any facts that meet the requirements for mandamus relief. Mandamus requires a clear and certain claim, a non-discretionary duty of the Defendants, and the absence of any other remedy. *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64, 66 (2004) (mandamus only available to compel acts that are ministerial and nondiscretionary). Plaintiffs have not – nor can they - attempted to demonstrate how or why they are entitled to this extraordinary relief, which warrants dismissal under both Rule 12(b)(1) and 12(b)(6).

Finally, Plaintiffs assert jurisdiction under 28 U.S.C. § 1346. Am. Compl. (ECF No. 8 ¶ 13). This basis is inapposite, however, as it applies to taxes and monetary damages against the United States, which are not at issue here and thus the Court lacks jurisdiction under this statute.

## **II. This Action Should Also Be Dismissed for Failure to State a Claim.**

The Court should dismiss Plaintiffs’ claims because Plaintiffs have not identified any final agency action, which is necessary to sustain a claim under the APA and Plaintiffs’ statutory and constitutional claims fail as a matter of law.

### **A. Plaintiffs Do Not Have a Viable APA Claim.**

In a suit seeking judicial review of agency action under the standards of the APA, 5 U.S.C. §§ 551–559, 701–706, the “entire case on review is a question of law, and only a question of law.” *Marshall Cnty. Health Care Auth. v. Shalala*, 988 F.2d 1221, 1226 (D.C. Cir. 1993). And an APA suit can be resolved on a motion to dismiss, without examination of the administrative record, where the dispute involves competing interpretations of statutes and regulations. *See Am. Bankers Ass’n v. Nat’l Credit Union Admin.*, 271 F.3d 262, 266–67 (D.C. Cir. 2001) (noting that a claim that agency action is contrary to statute can be resolved without examining an administrative record). Plaintiffs’ APA claim is ripe for dismissal for three reasons: (1) there is no final agency

action; (2) the suspension was authorized under Defendants’ regulations; and (3) the suspension is authorized under the agreements between the parties.

1. There is No Final Agency Action.

Plaintiffs’ claims have been brought under the APA, *see* Am. Compl. (ECF No. 8) ¶¶ 34–47, which limits review to “final agency action for which there is no other adequate remedy in a court.” 5 U.S.C. § 704 (emphasis added). Finality is a “threshold question” that determines whether judicial review is available under the APA. *See Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.*, 460 F.3d 13, 18 (D.C. Cir. 2006). “An agency action is final only if it is *both* ‘the consummation of the agency’s decisionmaking process’ and a decision by which ‘rights or obligations have been determined’ or from which ‘legal consequences will flow.’” *Nat’l Min. Ass’n v. McCarthy*, 758 F.3d 243, 250 (D.C. Cir. 2014) (quoting *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997)) (emphasis in original).

Here, Plaintiffs have not identified any final agency action, which is necessary to sustain any claims under the APA and if the challenged agency action is not “final,” the claims must be dismissed.<sup>6</sup> In addition to the reasons discussed above (*supra* at 18–20), the September 2 Notice can hardly be considered “final agency action.” Under CMS’s regulations and the agreements entered into by Plaintiffs and the agency, the suspension is a temporary measure that can be invoked by the agency when it discovers circumstances that pose unacceptable risk to consumers and the Exchanges. *See* 45 C.F.R §§ 155.220(c)(4)(ii) and 155.221(e). As detailed in the September 2 Notice, the agency has determined that there is a need for the Defendants to conduct an audit to further investigate the matter and confirm the Plaintiffs’ compliance with applicable

---

<sup>6</sup> In *Trudeau v. FTC*, 456 F.3d 178, 184–85 (D.C. Cir. 2006), the D.C. Circuit made clear that, even though the APA’s final agency action requirement was not jurisdictional, it was a necessary requirement in order for the plaintiff to state a cause of action under the APA.

requirements in CMS regulations, and the terms and conditions of their Exchange Agreements. *See* 45 C.F.R. § 155.220(c)(5); *see also* Enhanced Direct Enrollment Agreement, section X.m. at; Web-Broker Agreement, section X.l; Executed Interconnection Agreement, Section 15. The audit process is an interactive process that will include, and has already included, a series of back-and-forth communications between Plaintiffs and CMS, requests for data and information from CMS, the transmission of data and information from Plaintiffs to CMS, and an opportunity for Plaintiffs to challenge the findings of the audit, and it will conclude with a final decision issued by CMS. At any point during this audit, CMS could lift the suspension if it is determined that the privacy and security concerns that led to the audit have been sufficiently remedied or mitigated. The September 2 Notice thus signals the beginning of the agency auditing work; it does not “mark the consummation of the agency’s decisionmaking process.” *See Bennett*, 520 U.S. at 177–178.

Thus, Plaintiffs have failed to identify any action, including the September 2 Notice, that constitutes a final agency action under *Bennett v. Spear*, 520 U.S. at 177–78, and the Complaint therefore fails to state a claim on this ground alone.

## 2. Temporary Suspension Is Permitted Under CMS’s Regulations

CMS’s September 2 Notice also makes plain that the agency’s suspension is authorized under its regulations. *See* 45 C.F.R. §§ 155.220(c)(4)(ii), 155.221(e). Those authorities specifically advise companies like Plaintiffs that “HHS retains the right to temporarily suspend the ability of a web-broker making its website available to transact information with HHS, if HHS discovers a security and privacy incident or breach, for the period in which HHS begins to conduct an investigation and until the incident or breach is remedied to HHS’ satisfaction.” *Id.* at § 155.220(c)(4)(ii). Similarly, the regulations grant very broad discretion for the Secretary to “immediately suspend the direct enrollment entity's ability to transact information with the Exchange if HHS discovers circumstances that pose unacceptable risk to the accuracy of the



Exchange's eligibility determinations, Exchange operations, or Exchange information technology systems until the incident or breach is remedied or sufficiently mitigated to HHS' satisfaction.” *Id.* at § 155.221(e). As explained above and in the attached Busby Declaration, CMS received credible reports about Plaintiffs’ security lapses that placed the Exchanges and consumers at great risk. CMS immediately began its own assessment to determine the extent of the risk and confirm the reports of lapses in data security. Even after the agency initiated the suspension on August 8, 2024, CMS continued to work with Plaintiffs, providing them the opportunity to address the information CMS had received.

In a variety of contexts, Courts defer to an agency when it needs to take emergency action that requires immediate response. In the Medicare context, for example, courts have required an administrative process to conclude before it will intervene, even when the potential harm to a Plaintiff is great. In *D&G Holdings, LLC v. Burwell*, 156 F. Supp. 3d 798 (W.D. La. 2016), a laboratory sued the Secretary for withholding Medicare payments pursuant to a Medicare overpayment dispute. *See id.* at 803. The district court dismissed the plaintiff’s substantive due process claim even though the Plaintiff had described a “dire situation, one where a government contract erroneously claims overpayment in an unreasonable amount, binds the provider in a seemingly endless administrative process, withholds 95% of the provider’s income, and forces the provider out of business before it can receive its day in court.” *Id.* at 809, 817.

Similarly, in *Fox Ins. Co. v. Sebelius*, 381 Fed. Appx. 93 (2d Cir. 2010), CMS terminated its contract with a Medicare Part D plan because CMS determined the plan failed to provide drug benefits “in accordance with CMS requirements...and professionally recognized standards of care,” putting enrollees at risk of serious harm. *Id.* The Plaintiff claimed that CMS’s termination put the company at risk of severe financial hardship and at the brink of bankruptcy. *Id.* at 96. The

Second Circuit held that Plaintiff's threat of financial harm did not fall under any narrow exception contemplated by *Shalala v. Illinois Council*, 529 U.S. 1, 19–20 (2000) (the Medicare exhaustion requirement), and that the Plaintiff first had to pursue administrative remedies before seeking judicial review. *Id.* at 97. Although the case before this Court does not involve the Medicare program, exhaustion principles still apply—Plaintiffs will have opportunities to challenge audit findings and any ultimate final agency action that may result after conclusion of the audit. *See* 45 C.F.R. § 155.220(g)(5)(i)(B) and (h). Plaintiffs also have the opportunity to resolve, remediate, or otherwise mitigate the privacy and security concerns at various stages of the process, but there is no reason for judicial intervention before the agency issues a final decision.

Because the regulations here authorize CMS to impose a suspension to protect the privacy and security of Exchange consumers' PII or data and CMS information technology systems, this Court, like the other courts, must wait until the agency's administrative process concludes and there is a final agency decision before reviewing the agency action. For these reasons, this Court should dismiss Plaintiffs' action.

3. Temporary Suspension Is Permitted Under the Plain Terms of the Agreements with Plaintiffs.

CMS received complaints and reports about Plaintiffs' compliance with CMS Exchange requirements, including concerns related to the privacy and security of Exchange consumer data, including but not limited to consumer PII, and CMS information technology systems. As a result, on August 8, 2024, CMS preliminarily suspended Plaintiffs' access to the Exchanges while CMS continued its review of the alarming reports it received and further engaged with Plaintiffs. On September 2, 2024, CMS sent a letter to Plaintiffs explaining that the agency had suspended Plaintiffs' access to the CMS Exchanges pursuant to the agency's obligations under the parties'

Exchange Agreements and in accordance with its regulatory authority.<sup>7</sup> This action is reasonable and complies with the terms of the parties' agreements.

Specifically, Section X.m of the Enhanced Direct Enrollment Agreement, Section X.1 of the Web-Broker Agreement, and Section 15 of the Interconnection Agreement authorizes CMS's action here. For example, Section 15 of the Interconnection Agreement provides:

*Non-compliance with the terms of this ISA by either party or unmitigated security risks in violation of this ISA may lead to termination of the interconnection. CMS may block network access for the Non-CMS Organization if the Non-CMS Organization does not implement reasonable precautions to prevent the risk of security incidents spreading to CMS's network. CMS is authorized to audit the security of Non-CMS Organization's Network periodically by requesting that Non-CMS Organization provide documentation of compliance with the security requirements in this ISA (please refer to Section 22, Records). The Non-CMS Organization shall provide CMS reasonable access to its IT resources impacted by this ISA for the purposes of audits, subject to applicable legal requirements and policies.*

The Enhanced Direct Enrollment Agreement likewise grants CMS extensive authority to conduct thorough audits and provides, in pertinent part, that the agency has "the right to audit [Plaintiffs'] compliance with and implementation of the privacy and security requirements under this Agreement [and other agreements with CMS] and applicable program requirements." The Web-Broker Agreement provides for essentially the same audit authority as the Enhanced Direct Enrollment agreement.

Plaintiffs ignore the fact that their agreements with CMS permit the precise action that the agency has undertaken here, and in particular the authorization pursuant to the Interconnection Agreement for the August 8 immediate suspension. CMS received credible reports of serious

---

<sup>7</sup> As explained in the September 2 Notice, "...CMS has determined that continuing the August 8, 2024, suspension of the Speridian Companies is necessary and appropriate." The immediate suspension initiated on August 8 was pursued under Section 15 of the Interconnection Agreement.

privacy and security lapses that placed the Exchanges and consumers at risk, and CMS's initial review as well as its discussions with Plaintiffs did not resolve CMS's concerns or sufficiently remediate or mitigate the identified risks. For example, CMS received information from an agent/broker stating that a company had fraudulently used his credentials that resulted in his suspension from accessing the Exchanges. *See* Busby Decl. CMS also learned of a lawsuit filed against Plaintiff TrueCoverage, which included signed declarations. *See Turner*, Civ. A. No. 24-60591, ECF No. 1. Then on July 29, 2024, CMS received a report that the Plaintiffs' Customer Relationship Management system may be based overseas in violation of its Agreements with CMS. *See* Busby Dec.

On August 6, 2024, CMS received the results of an assessment that concluded "that the overall risk to CMS data and information systems was critical, meaning that the product, service or supplier contains vulnerabilities or weaknesses that are wholly exposed and easily exploitable." *See id.* "On August 8, 2024, CMS concluded that there was sufficient evidence that [Plaintiffs'] platforms could be accessed by systems that were not included within the agreements between CMS and [Plaintiffs] both inside and outside of the United States to warrant immediately suspending their ability to transact information with the [Exchanges]." *See id.* This violated Section X.n of the Enhanced Direct Enrollment Agreement, which prohibits an entity to "remotely connect or transmit data to the [Exchange or] remotely connect or transmit data to [Plaintiffs'] systems that maintain connections to the [Exchange] or its testing environments, from locations outside of the United States of America. [including] any such connection through virtual private networks (VPNs)." *Id.* CMS continued to review this matter over the next several weeks, but the review led to more concerns. *Id.* ¶¶ 14–23.

CMS clearly has authority under its agreements with Plaintiffs to suspend their access to the Exchanges. As set forth above, and in the attached Declarations, CMS's decision to continue the suspension pending an audit is reasonable under the circumstances. Furthermore, Plaintiffs voluntarily entered into these agreements and agreed to comply with CMS requirements and allow CMS to suspend their access to the Exchanges, as well as to conduct the ensuing audit.

In addition to the Plaintiffs' voluntarily agreeing to comply with the requirements to participate in the Exchanges, the agency has its own obligations and duty to ensure the privacy and security of Exchange data and CMS information technology systems. In emergency situations, such those presented here, where Plaintiffs' access to consumers' private information and the Exchanges can result in great harm to the public and CMS information technology systems, it is prudent that CMS has the authority to suspend Plaintiffs' access to the Exchanges – particularly when it receives credible information, confirmed by initial review, that entities like Plaintiffs engaged in improper behavior. In *Federal Deposit Insurance Corp. v. Mallen*, 486 U.S. 230, 244 (1988), the Supreme Court held that an agency may issue a suspension and hold a post-suspension hearing if the public interests weigh in the agency's favor. In that case, a bank president was suspended from his role after being indicted. *Id.* at 237–38. The court did not require that the agency wait for the conclusion of the court proceedings. The Plaintiff there likewise moved for a preliminary injunction before an administrative hearing could be held. *Id.* at 239. Although the Plaintiff had an interest in the right to continue in his role as bank president, the Court found a post-suspension procedure was not unconstitutional because of the government's recognized interest in maintaining confidence in the banks, and due process did not require providing Plaintiff a pre-suspension hearing. *See id.* at 245, 248.

Here, the protection of consumers' PII and confidence in, along with the protection of the security of CMS information technology systems, is likewise a substantial, legitimate government interest. And in the same manner, the need to implement a suspension to provide protection while CMS conducts an audit is reasonable, even if it is disruptive to Plaintiffs' current lines of business.

Similarly, in *General Electric Co. v. Jackson*, 610 F.3d 110 (D.C. Cir. 2010), the D.C. Circuit upheld a unilateral administrative order process issued by the EPA. The Court acknowledged the Plaintiff company faced financial consequences and recognized that other administrative enforcement schemes addressing similar matters may offer more process than the one at issue. *Id.* at 129. But the court nevertheless held that the process offered by the EPA did not deprive Plaintiff of due process. *Id.*

In this case, Plaintiffs have access to highly private consumer information and CMS information technology systems—and knowingly agreed that CMS has the authority to issue Exchange system suspensions when necessary to protect the public and CMS information technology systems from irreparable harm due to Plaintiffs' behavior. This framework adopted by CMS in its agreements do not violate due process nor support a claim under the APA. Thus, this matter should be dismissed.

**B. Plaintiff's Fifth Amendment Due Process Claim is Legally Deficient.**

Plaintiff's due process claim does not rise above the speculative level to the realm of plausibility and thus, should be dismissed.

As an initial matter, Plaintiffs' due process claim fails to meet the applicable pleading standard described in *Twombly* and *Iqbal*. Here, the same allegations that support Plaintiffs' APA claims are the same allegations that support their due process claim and Plaintiff neither identifies whether their procedural or substantive due process rights were violated nor plead sufficient facts that could give rise to an inference of a violation. *See* Am Compl. (ECF No 8) ¶¶ 48–55. This is

insufficient to substantiate a claim for a due process violation. *See Iqbal*, 556 U.S. at 678 (“A pleading that offers labels and conclusions or a formulaic recitation of the elements of a cause of action will not do.”); *Kowal v. MCI Comm. Corp.*, 16 F.3d 1271, 1276 (D.C. Cir. 1994) (“[T]he court need not accept inferences drawn by plaintiffs if such inferences are unsupported by the facts set out in the complaint . . . [n]or must the court accept legal conclusions cast in the form of factual allegations.”).

In any event, any procedural due process claim fails. A “procedural due process violation occurs when an official deprives an individual of a liberty or property interest without providing appropriate procedural protections.” *Atherton v. D.C. Off. of the Mayor*, 567 F.3d 672, 689 (D.C. Cir. 2009). “At a minimum, a procedural due process claim ‘requires the plaintiff to identify the process that is due.’” *Medina v. Dist. of Columbia*, 517 F. Supp. 2d 272, 281 (D.D.C. 2007) (quoting *Doe v. Dist. of Columbia*, 93 F.3d 861, 870 (D.C. Cir. 1996)); *see also Elkins v. Dist. of Columbia*, 690 F.3d 554, 561 (D.C. Cir. 2012) (“To state a procedural due process claim, a complaint must suggest ‘what sort of process is due.’”). Plaintiffs’ Amended Complaint, however, is devoid of any allegations asserting what process or procedures they were due but was not granted. Instead, their allegations regarding the alleged due process violation consist solely of conclusory assertions that “providing Plaintiffs with prior notice and a realistic opportunity to cure would be a substantially more valuable procedure than summarily suspending Plaintiffs without any explanation,” Am. Compl. (ECF No. 8) ¶ 53, and that they were deprived of property, *id.* ¶ 55. These bare-bones allegations do not meet the threshold requirement of identifying the process that is due and thus, dismissal is warranted. *See Gonzalez Boisson v. Pompeo*, 459 F. Supp. 3d 7, 19 (D.D.C. 2020) (dismissing plaintiff’s due process claim where “the only allegations in [the plaintiff’s] complaint regarding [the due process] argument [were] ... ‘that the lack of fair and

meaningful post-deprivation procedures for adjudicating the revocation of a United States passport’ violates the Due Process Clause.”); *Lewis v. Gov’t of the D.C.*, 161 F. Supp. 3d 15, 30–31 (D.D.C. 2015) (dismissing plaintiff’s due process claims “[b]ecause [the complaint] is devoid of allegations as to the actual process purportedly denied ...the [complaint] does not raise [plaintiff’s] procedural due process claim ‘above the speculative level’ to the realm of plausibility.”). Also, here, the agency gave Plaintiffs the rationale for the temporary suspension and the agency’s regulations are clear as far as the procedure going forward.

Similarly, any claim for substantive due process violation also fails. A “substantive due process constrains only egregious government misconduct,” *Decatur Liquors v. Dist. of Columbia*, 478 F.3d 360, 363 (D.C. Cir. 2007). Thus, “a substantive due process violation will only occur where the government’s conduct is so egregious, so outrageous, that it may fairly be said to shock the contemporary conscience,” *Toms v. Off. of the Architect of the Capitol*, 650 F. Supp. 2d 11, 25–27 (D.D.C. 2009) (quoting *Butera v. Dist. of Columbia*, 235 F.3d 637, 651 (D.C. Cir. 2001)). Plaintiffs’ mere complaints about the suspension not going the way they wanted does not rise to any level of “egregious government misconduct.” Compl. ¶¶ 32, 40; *see also Toms*, 650 F. Supp. 2d at 25–27 (finding that “plaintiff’s perceived procedural deficiencies” did not constitute a due process violation); *Solomon v. Off. of the Architect of the Capitol*, 539 F. Supp. 2d 347, 350-51 (D.D.C. 2008) (dismissing substantive due process claim, as procedural issue did not meet “conscience-shocking” test).

\* \* \*

Accordingly, the Court should dismiss Plaintiffs’ Amended Complaint in its entirety because of lack of jurisdiction and Plaintiffs’ failure to state a claim.



**III. Even If the Court Does Not Dismiss This Lawsuit, Plaintiffs Are Not Entitled to a Temporary Restraining Order or Preliminary Injunction.**

Courts cannot grant requests for sweeping mandatory injunctive relief absent a strong showing that all elements of the preliminary injunction standard have been met, namely that Plaintiffs demonstrate: (1) likely success on the merits; (2) likely irreparable harm in the absence of preliminary relief; (3) a balance of the equities in its favor; and (4) accord with the public interest. As discussed previously, Plaintiffs cannot establish that the Court has jurisdiction, let alone demonstrate that it will prevail on the merits. Also, Plaintiffs are unable to demonstrate immediate irreparable harm. Further, Plaintiffs do not seek to preserve the status quo, but instead wants to alter it by enjoining Defendants from protecting consumers' PII and the Exchanges from being compromised or harmed. Finally, the public interest tips against issuance of an injunction since Plaintiffs have not met at least the first two prongs for injunctive relief.

**A. Plaintiffs Have Not Established Irreparable Injury**

The standard for irreparable harm is particularly high in the D.C. Circuit. “[P]roving irreparable injury is a considerable burden, requiring proof that the movant's injury is *certain, great and actual*—not theoretical—and *imminent*, creating a clear and present need for extraordinary equitable relief to prevent harm.” *Power Mobility Coal. v. Leavitt*, 404 F. Supp. 2d 190, 204 (D.D.C. 2005) (quoting *Wis. Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985)) (internal quotation marks omitted) (emphasis in original); see also *Save Jobs USA v. Dep’t of Homeland Sec.*, 105 F. Supp. 3d 108, 112-13 (D.D.C. 2015).

Also, purely economic loss, even when large sums of money are involved, typically will not constitute irreparable injury. See *Wis. Gas Co.*, 758 F.2d at 674 (noting it is “well settled that economic loss does not in and of itself constitute irreparable harm”); *Emily’s List v. FEC*, 362 F. Supp. 2d 43, 52 (D.D.C. 2005). Recoverable monetary loss may constitute irreparable harm only

where the loss threatens the very existence of the movant's business. *See Wash. Metro. Area Transit Comm'n v. Holiday Tours, Inc.*, 559 F.2d 841, 843 n. 2 (D.C. Cir. 1977). The movant may not rely on "bare allegations" that the business will not survive absent a preliminary injunction. *Wis. Gas Co.*, 758 F.2 at 674. Instead, the movant must provide some evidence of irreparable harm: "the movant [must] substantiate the claim that irreparable injury is likely to occur" and "provide proof that the harm has occurred in the past and is likely to occur again, or proof indicating that the harm is certain to occur in the near future." *Id.* at 674 (internal quotation marks and citation omitted). This is because "[i]ssuing a preliminary injunction based only on a possibility of irreparable harm is inconsistent with [the court's] characterization of injunctive relief as an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter*, 555 U.S. at 22.

In addition, "the certain and immediate harm that a movant alleges must also be truly irreparable in the sense that it is 'beyond remediation.'" *Elec. Privacy Info. Ctr. v. Dep't of Just.* 15 F. Supp. 3d 32, 44 (D.D.C. 2014) (citation omitted). The movant must provide some evidence of irreparable harm: "the movant [must] substantiate the claim that irreparable injury is likely to occur" and "provide proof that the harm has occurred in the past and is likely to occur again, or proof indicating that the harm is certain to occur in the near future." *Wis. Gas Co.*, 758 F.2d at 674 (internal quotation marks and citation omitted). This is because "[i]ssuing a preliminary injunction based only on a possibility of irreparable harm is inconsistent with our characterization of injunctive relief as an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter*, 555 U.S. at 22. As these authorities make clear, to meet the standard for irreparable harm the movant must present sufficient evidence that the purported injury is certain, great, actual, imminent, and beyond remediation.

Plaintiffs have not shown that it will suffer an “irreparable” injury absent a preliminary injunction. Plaintiffs argue that their business has come to a halt, some of their clients have terminated their relationship with the business, and the suspensions threatens their revenue. *See* Pls.’ Mot. (ECF No. 9) at 20–21. In terms of the financial loss, while it may harm Plaintiffs, it is neither certain nor irreparable. Instead, it is a purely a financial injury, which Plaintiffs can avoid by earning revenue through their other business. Also, because the loss Plaintiffs have identified is for the most part financial, it cannot support a finding of irreparable harm unless Plaintiff establishes that these losses will indeed threaten the continued existence of its businesses. Plaintiff has not substantiated those claims. First, the fact that Plaintiff remains solvent and operational belies any suggestion that absent an injunction Plaintiffs’ ability to continue operations will be immediately affected. Second, Plaintiff has offered only bare allegations that absent an injunction Plaintiff’s business will not survive or will be competitively disadvantaged. Plaintiff has not submitted audited financial statements or other detailed materials to demonstrate the impact the injunction would have on its viability, the dollar deficit that would allegedly drive them out of business, or any details on the client relationships that have been severed. These “bare allegations” that absent an injunction Plaintiffs will have on-going loss or their business will be harmed in some indefinite time in the future is insufficient to support a finding of irreparable harm. *See Wis. Gas Co.*, 758 F.2d at 654. Thus, it is far from certain that the suspension will cause Plaintiffs’ business to reach a financial deficit so high that Plaintiffs would be driven out of business or suffer irreparable harm. Again, Plaintiff can avoid that result by focusing on their other business enterprises, using the other available enrollment avenues to provide assistance to Exchange consumers, and therefore the alleged threat to its viability will result from Plaintiffs’ decision not to elect other available options.

Even if Plaintiffs' fears of lost revenue were sufficiently imminent, or otherwise met the high standard, Plaintiffs have not shown that such injuries— if they occur at all—are irreparable. CMS has suspended Plaintiffs before. Wu Dec. ¶ 5, submitted herewith. Given that Plaintiffs have survived a past suspension by CMS, it appears highly speculative to claim that this most recent suspension will lead to them losing their business altogether. In addition, Plaintiffs' direct enrollment platforms and participation in the Exchanges are not their only business enterprise. Further, the suspension only affects plans purchased through the Exchanges and should not have any effect on Plaintiffs' other businesses. *See* Grant Decl. ¶ 11 (“If a consumer purchased non-ACA coverage through the [Plaintiffs’] they should still be able to do so, as they do not require a connection to the [Exchanges].”); *id.* ¶ 10 (“Agents, brokers, an agencies, including TrueCoverage’s agents, will continue to be able to serve consumers, even while BenefitAlign and TrueCoverage platforms are suspended.”).

Plaintiffs assert “[t]he CMS suspension threatens practically all of the revenue generated by TrueCoverage and Benefitalign.” Pls.’ Mot. (ECF No. 9) at 24. Such a claim is not borne out by the suspension CMS has imposed thus far. Plaintiffs ignore that CMS’s suspension is narrowly tailored to specifically address its concerns and to protect the Exchanges and consumers from serious harm. The suspension only prevents Plaintiffs from accessing highly sensitive information available through the Exchanges that could be misused and improperly exposed, but the suspension does not prevent Plaintiffs from conducting other business. During the current suspension, Plaintiffs’ Exchange agreements with CMS have not been suspended or terminated, which allows them to continue to assist Exchange consumers using other enrollment avenues and still earn commissions and other compensation for Exchange enrollments. *See* Grant Dec. ¶¶ 10-11. It also does not in any way interfere with Plaintiffs’ non-Exchange activities and other lines of business

(e.g., dental plans, vision plans, etc.). Plaintiffs have the ability to conduct all of these activities and continue to participate in these other lines of business, which they can and do provide. While the suspension may be inconvenient, it is necessary to protect the privacy and security of innocent consumers' data and CMS information technology systems from harmful practices. And Plaintiffs have been unable to propose any action short of a suspension that will address CMS's concerns during the suspension period and accompanying audit. *See* Pls.' Ex. 2 (ECF No. 9-2); Pls.' Ex. 3 (ECF No. 9-3). Plaintiffs will continue to be able to serve consumers, except they will not have direct access to the Exchanges' information technology systems, and they cannot make their direct enrollment platforms available to other entities to transact information with the Exchanges.

According to CMS's records, which identify the other entities approved to use Plaintiff Benefitalign's EDE platform, Benefitalign has only one upstream EDE entity, other than TrueCoverage. This one other additional company is AvMed Health Plans, which, according to CMS records, accounted for only twenty-eight enrollments. Respectfully, this hardly seems to be the number of enrollments that would make or break a business. Plaintiffs assert, as part of their irreparable harm argument, that "health insurance carriers, such as AvMed Health Plans, that use [Plaintiffs'] platforms and whose operations are severely affected by the suspension of these platforms." Pls.' Mot. (ECF No. 9) at 25. AvMed Health Plans is not a party to this litigation and the Court has no obligation to consider Plaintiffs' claims about the effect on a third-party business that is not in this lawsuit. Moreover, it is unclear what prevents AvMed from using any of the multitude of other available platforms to conduct its business on the Exchanges. The theoretical nature of this harm, coupled with the fact it relates to a relatively small number of enrollments (twenty-eight), falls far short of the burden of irreparable harm that can support emergency relief.

Plaintiffs speculate about a series of “cascading” harm that will befall them, including “brokers and carriers’ imminent termination of their relationships with [Plaintiffs].” But Plaintiffs have failed to establish a “certain[] impending” injury when the asserted injury is based on a “speculative chain of possibilities,” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 410 (2013), or on “speculation about the decisions of independent actors,” *id.* at 414. As the D.C. Circuit has cautioned: “Because of the generally contingent nature of predictions of future third-party action,” a court should be “sparing in crediting claims of anticipated injury by market actors and other parties alike.” *Arpaio v. Obama*, 797 F.3d 11, 23 (D.C. Cir. 2015).

The suspension does not prevent Plaintiffs from accessing other available enrollment avenues to assist consumers with submitting applications and enrollments to the Exchanges. According to CMS’s records, TrueCoverage has more than 50 registered agents, and TrueCoverage can still collect commissions and other compensation from insurance issuers notwithstanding the suspension and can also assist consumers with submitting applications and enrollments to the Exchanges by accessing other available enrollment avenues. Plaintiffs may also receive commissions from applications and enrollments submitted on or before the August 8<sup>th</sup> suspension.

Plaintiffs’ main complaint is the suspension prevents BenefitAlign from collecting fees from issuers to be listed on its platform. BenefitAlign charges per member annual fees. We are unsure how this suspension prevents them from collecting fees. TrueCoverage can still receive commissions and other compensation from issuers for enrolling consumers in Exchange coverage before the suspensions. The suspension also has not impact on other lines of business, such as the non-Exchange coverage that TrueCoverage engages in – those activities can continue uninterrupted.

For all these reasons, Plaintiffs failed to demonstrate irreparable harm, which is fatal to their motion seeking emergency, preliminary relief.

**B. Plaintiffs Are Unlikely to Succeed on the Merits.**

Plaintiffs likewise have not shown that they are likely to prevail on the merits of their claims. A plaintiff that cannot demonstrate a significant likelihood of success on the merits has no hope of obtaining a preliminary injunction. *See Trudeau v. Federal Trade Comm'n*, 456 F.3d 178, 182 n.2 (D.C. Cir. 2006); *Katz v. Georgetown Uni.*, 246 F.3d 685, 688 (D.C. Cir. 2001); *Apex, Inc. v. FDA*, 449 F.3d 1249, 1253–54 (D.C. Cir. 2006). “[A]bsent a ‘substantial indication’ of likelihood of success on the merits, ‘there would be no justification for the court’s intrusion into the ordinary processes of administration and judicial review.’” *Biovail Corp. v. FDA*, 448 F. Supp. 2d 154, (D.D.C. 2006) (quoting *American Bankers Ass’n v. Nat’l Credit Union Admin.*, 38 F. Supp. 2d 114, 140 (D.D.C. 1999)). As discussed in great length above, Plaintiff is unlikely to succeed on the merits for a multitude of reasons. First, the Court lacks jurisdiction over Plaintiffs’ claims because any challenges relating to the August 8 Email are moot, any challenges relating to the suspension are not ripe, and there are no allegations to establish subject matter jurisdiction under 8 U.S.C. §§ 2201, 1361, and 1346. Second, Plaintiff failed to state a claim because there is no agency decision, the suspension was authorized under Defendants’ regulations and the agreements between the parties, and Plaintiffs failed to plead a cognizable due process claim. Thus, Plaintiffs have no likelihood of prevailing in this matter.

**C. The Remaining Factors Weigh Against Mandatory Injunction.**

The final two factors required for preliminary injunctive relief—a balancing of the harm to the opposing party, and the public interest—merge when the Government is the opposing party. *See, e.g., Nken v. Holder*, 556 U.S. 418, 435 (2009); *Colo. Wild Horse v. Jewell*, 130 F. Supp. 3d 205, 220-21 (D.D.C. 2015). Courts must “[give] particular regard [to] the public consequences in

employing the extraordinary remedy of injunction.” *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 312-13 (1982). In this case, the balance of equities and the public interest tip strongly in favor of the Government as “the public interest favors applying federal law correctly.” *Small v. Avanti Health Sys, LLC*, 661 F.3d 1180, 1197 (9th Cir. 2011).

CMS’s suspension of Plaintiffs’ access to the Exchanges and the ability of other agents and brokers to use the Plaintiffs’ platforms to transact information with the Exchange during the suspension and audit period protects the privacy and security of Exchange consumers’ data and CMS information technology systems, as well as the integrity of the Exchanges. In addition, with respect to the public interest there is no generalized loss of access to the Exchanges for consumers, brokers, or agents. *See* Grant Decl. ¶ 10 (“Agents, brokers, and agencies will continue to be able to serve consumers, even while [Plaintiffs’] platforms are suspended. Unless contractually restricted, agents and brokers generally can affiliate with multiple insurance agencies simultaneously.”). Thus, for the public and those serving Exchange consumers, the suspension poses no significant adverse consequences—only protection. *See id.* ¶ 11 (“consumers can turn to the ... Exchange Call Center for support. The [] Call Center can access the applications and enrollments of all consumers enrolled through the Exchanges, regardless of whether the enrollment was submitted by an active or suspended EDE partner.”); *id.* ¶ 12 (“Consumers’ health insurance coverage and access to care will be unaffected by [Plaintiffs’] suspensions.”); *see* Wu Decl. ¶ 4 (In Plan Year 2023, there were registered and approved 11 enhanced direct enrollment platforms, 12 web-brokers, numerous health insurance agencies, and around 79,795 independent agents and brokers). Any inconvenience the suspension imposes on Plaintiffs or other entities that use Plaintiffs’ direct enrollment platforms is thus far outweighed by the need to protect the public and



CMS information technology systems until CMS completes its audit and determines the extent of any harm.

Notwithstanding the foregoing, Plaintiffs cannot meet their burden of establishing “that the balance of equities tips in [their] favor, and that an injunction is in the public interest.” *Winter*, 555 U.S. at 20; *Texas v. United States*, 86 F. Supp. 3d 591, 675 (S.D. Tex.), *aff’d*, 809 F.3d 134 (5th Cir. 2015) as revised (Nov. 25, 2015) (citation omitted) (“If no public interest supports granting preliminary relief, [it] should ordinarily be denied ....”); *see also Weinberger*, 456 U.S. at 312 (“[C]ourts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction.”). Here, the public interest weighs heavily against Plaintiffs’ attempt to enjoin CMS’s suspension, which the agency intends to maintain pending the audit to protect the public and CMS information technology systems.

### CONCLUSION

For these reasons, the Court should deny Plaintiffs’ Motion, grant Defendants’ Motion, and dismiss this action.

Dated: September 20, 2024

Respectfully submitted,

MATTHEW M. GRAVES, D.C. Bar # 481052  
United States Attorney

BRIAN P. HUDAK  
Chief, Civil Division

By:                   /s/ Stephanie R. Johnson                  

STEPHANIE R. JOHNSON  
DC Bar # 1632338  
Assistant United States Attorney  
601 D Street, NW  
Washington, DC 20530  
(202) 252-7874  
Stephanie.Johnson5@usdoj.gov

*Attorneys for the United States of America*

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

BENEFITALIGN, LLC, et al.,

Plaintiffs,

v.

CENTERS FOR MEDICARE & MEDICAID  
SERVICES, et al.,

Defendants.

Civil Action No. 24-2494 (JEB)

**PROPOSED ORDER**

UPON CONSIDERATION of Defendants' motion to dismiss, Plaintiffs' amended motion for temporary restraining order and preliminary injunction and request for a hearing, and the entire record herein, it is hereby

ORDERED that Plaintiffs' amended motion is DENIED;

ORDERED that Defendants' motion is GRANTED, and it is further

ORDERED that this matter is DISMISSED WITHOUT PREJUDICE.

SO ORDERED:

\_\_\_\_\_  
Date

\_\_\_\_\_  
James E. Boasberg  
Chief United States District Judge

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

BENEFITALIGN, LLC, *et al.*,

Plaintiffs,

v.

CENTERS FOR MEDICARE & MEDICAID  
SERVICES, *et al.*,

Defendants.

Civil Action No. 24-02494 (JEB)

**DECLARATION OF KEITH BUSBY**

I, Keith Busby, pursuant to 28 U.S.C. § 1746, and based upon my personal knowledge, information I have reviewed in the records of the U.S. Department of Health and Human Services (HHS) and its subsidiary components, or on information provided to me by HHS employees and contractors, hereby make the following declaration with respect to the above-captioned matter. I am aware of, and familiar with, the amended complaint and amended motion for temporary restraining order and preliminary injunction filed by BenefitAlign, LLC and TrueCoverage, LLC, captioned *BenefitAlign, LLC v. Centers for Medicare & Medicaid Services.*, Case No. 24-02494 (JEB) (D.D.C.) (filed Sept. 6, 2024).

---

1. I currently serve as the Acting Chief Information Security Officer in the Office of Information Technology within the Centers for Medicare & Medicaid Services (CMS), an operating division of HHS.

2. I began my career as an information technology (IT) professional while serving in the United States Army from 2003-2011. During that time, I served in a variety of roles within both tactical and strategic environments. Upon discharge, I became a technical consultant supporting chemical plants supporting all levels of the environments. Simultaneously, I attended Drexel University September 2012 to March 2015 where I earned a Bachelor of Science in Computing and Securing Technologies. In 2014, I transitioned into Security Engineering for a large urban school district where I was promoted up through the ranks to the Executive Director of IT Security. I left the urban school district to join CMS's Information Security and Privacy Group (ISPG) as the Director for its Division of Security and Privacy Compliance (DSPC) in March 2021. Since joining CMS, I served as ISPG's Director of the Division of Cyber Threat and Security Operations May 2023-November 2023, the Deputy Chief Information Security Officer (CISO) from November 2023 to present, and I have been the Acting CISO since March 2024, carrying out all agency information security responsibilities.

3. In my role as the Acting CISO, I help oversee information security and privacy for all CMS systems subject to the Federal Information System Modernization Act (FISMA), Public Law 113-283 (Dec. 18, 2014), including the systems that house the personally identifiable information (PII) of consumers who apply for health insurance coverage through a Federally-facilitated Exchange (FFE) or State-based Exchange on the Federal Platform (SBE-FP) (collectively, "Exchange").

---

4. As Acting CISO, I oversaw CMS's review of IT activities related to Enhanced Direct Enrollment (EDE) platforms operated by BenefitAlign, LLC and TrueCoverage, LLC dba Inshura.com. This review also covered TrueCoverage, LLC, in its capacity as a web-broker that assists consumers with Exchange enrollments using a proprietary website.

**CMS's Review of the BenefitAlign and TrueCoverage Systems Results in the Suspension of Their Connections to CMS Systems**

5. The following paragraphs provide the timeline of events that led to CMS suspending BenefitAlign, LLC's and TrueCoverage, LLC's ability to electronically transact information with CMS IT systems on August 8, 2024.

6. On July 23, 2024, CMS's IT Service Desk received an email from Robenson Remelus stating that a company had fraudulently used his credentials to write health insurance policies in states in which he did not do business, causing CMS to suspend his access to all Exchange direct enrollment pathways. Attached to this email was a copy of the Class Action Lawsuit filed in United States District Court, Southern District of Florida, on April 12, 2024, listing TrueCoverage, LLC, and Speridian Technologies, LLC, within the list of defendants. (Exhibit A). As a result, CMS created a 'ticket' under which it would address the agent's or broker's complaint. *See* CMS Security Incident Response Ticket No. SIR0030682. (Exhibit B). This ticket was forwarded to the CMS Security Operations Center (SOC). On July 29, 2024, CMS's SOC created a ticket based on a report of concerns that the Speridian Companies'<sup>1</sup> Customer Relationship Management (CRM) system may be based overseas in violation of its Agreements with CMS. *See* Security Incident Response Ticket No. SIR0030846. (Exhibit C).

---

<sup>1</sup> The Speridian Companies encompass Speridian Global Holdings, LLC; Speridian Technologies, LLC; BenefitAlign, LLC; TrueCoverage, LLC; and True Coverage, LLC dba Inshura.com.

---

This report raised concerns about the privacy and security of Exchange data, including consumer PII, being processed or stored outside of the United States. *Id.* Because federal agencies may become exposed to cybersecurity risks through the software and services they deploy, use, and manage in performing their functions, the SOC engaged its Supply Chain Risk Management (SCRM) team to perform a supply chain risk assessment of BenefitAlign, LLC, TrueCoverage, LLC, and their affiliated companies. The goal of the assessment was to identify and evaluate potential risks to the Exchanges' operations, including risk to the people, organizations, resources, and activities related to Exchange operations.<sup>2</sup>

7. On August 6, 2024, CMS received the results of the supply chain assessment. *See* Supply Chain Risk Assessment on Speridian Technologies, LLC, dated August 5, 2024. (Exhibit D). The assessment concluded that the overall risk<sup>3</sup> to CMS data and information systems was critical, meaning that the BenefitAlign and TrueCoverage platforms have vulnerabilities or weaknesses that are wholly exposed and easily exploitable. [NIST SP 800-161r1 (pg. 228)] The assessment's assignment of critical risk was based on BenefitAlign, LLC's, TrueCoverage, LLC's, and their affiliated companies' overseas ties, sworn testimony submitted under penalty of perjury in the class action lawsuit filed in the United States District Court, mentioned above, and an assessment that indicated the platforms have weak security that could create exploitable vulnerabilities in the platforms' environments, including taking more time than is reasonable to

---

<sup>2</sup> The CMS Supply Chain Risk Assessment utilizes publicly available information to assess five key areas for a company: Foreign Ownership, Control or Influence; Significant Adverse Information (legal, financial, etc.); Supply Chain Tier Structure Concerns; Company Product Related Concerns and Company Cyber Vulnerabilities.

<sup>3</sup> "Risk" is defined as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. NIST Special Publication 800-53 Rev. 5.

---

address known vulnerabilities and implementing lax network security controls that are unlikely to prevent unauthorized access to the Speridian Companies' environment.

8. The agreements BenefitAlign and TrueCoverage voluntarily signed as a precondition to becoming an approved direct enrollment partner provide that direct enrollment partners and their delegated entities, including employees and contracted agents, "cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to EDE Entity's systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America . . . . This includes any such connection through virtual private networks (VPNs)." EDE Agreements with TrueCoverage and BenefitAlign at section X.n. (Exhibit E, F); Web Broker Agreements with TrueCoverage and BenefitAlign at section X.m. (Exhibit G, H). *See generally* Interconnection Security Agreement with BenefitAlign at section 10 (Exhibit I).

9. Likewise, under CMS's requirements, Exchange data must always reside within the United States to reduce the possibility that foreign actors and powers might obtain access to CMS data and information. *See* EDE Agreement at section X.n. (Exhibit E, F). *See* Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, dated June 9, 2021 (Exhibit J: "Foreign adversary access to large repositories of United States' persons' data . . . present a significant risk."). Accordingly, the existence of pathways to access a direct enrollment platform from outside of the United States constitutes a material breach of these agreements and a significant risk to Americans and the security of the nation.

10. On August 7, 2024, CMS began a Privacy Risk Assessment to explore the potential risk to consumers who entrusted their PII to BenefitAlign or TrueCoverage. This

---

assessment reviewed the nature and sensitivity of the PII that may have been compromised, the likelihood of access and use of the PII that may have been compromised and the type of breach that caused the PII to potentially be compromised.

11. On August 8, 2024, CMS preliminarily concluded based upon the findings of the Supply Chain Risk Assessment that there was strong evidence of prohibited foreign access to the BenefitAlign and TrueCoverage direct enrollment platforms. This evidence included multiple danger signals associated with the Speridian Companies:

- The owners of the companies under the Speridian Holdings, LLC's, corporate umbrella have substantial ties to India; a substantial amount of the company's operations appears to be based out of India, where the majority of the employees seem to be operating from; the majority of the company's named executive named officers have ties to or are based in India; the majority of the company's research and development appear to be conducted in India and Pakistan.
  - Multiple domains tied to the Speridian Companies are shown to be based in India, making it further appear that agency data is stored outside of the United States. Speridian uses a hybrid onsite/offshore delivery model which means that a portion of the work and support is conducted from overseas locations. Speridian operates a large, dedicated data center in India, and it is possible that agency data is processed and/or stored in this location. The company has subsidiaries and operations in Canada, India, Pakistan, Saudi Arabia, Singapore, and the UAE.
  - Speridian and its subsidiary, True Coverage, are defendants in an active lawsuit filed in 2024 alleging that they engaged in a variety of illegal practices including violations of the RICO Act, as well as the misuse of PII, and insurance fraud. This was alleged to be
-



accomplished via the use of a Speridian product, “BenefitAlign,” which allows access to the Exchange. The complaint also alleges that BenefitAlign allows access to the exchange and houses CMS data abroad, which is in violation of their EDE agreement with HHS.

- Speridian’s cyber security hygiene is below industry average.

12. Due to the serious nature of these risks and the potential harm to consumers and the Exchange as outlined in the assessment, on August 8, 2024, CMS suspended BenefitAlign’s and TrueCoverage’s ability to transact information with the Exchange and access data in CMS systems. *See* Email from Jeffrey Grant to the Speridian Companies, dated August 8, 2024.

(Exhibit K). CMS informed BenefitAlign and TrueCoverage that the suspensions were temporary but would continue until CMS had completed its review of apparent breaches of consumer data, which is necessary to protect the public until CMS can reasonably conclude that Exchange consumer data has been and will be used and secured appropriately by the platforms.

*Id.*

### **CMS Continues to Review the Speridian Companies’ EDE Platforms**

13. Two business days later, on August 13, 2024, CMS (including CCIIO’s Deputy Director for Operations, Jeffrey Grant, representatives from OIT office, Leslie Nettles and David Paradis, and me) and representatives of the Speridian Companies met by video conference to discuss the August 8, 2024, suspension. CMS and the Speridian Companies discussed reports of improper access to CMS systems from outside of the United States, in addition to reports that Exchange data were being transmitted and stored in non-CMS approved systems in foreign countries. Speridian Companies claimed that these reports were false. The Speridian Company

---

representatives stated that the system blocked all connections from foreign countries and that no data could be accessed from or sent to systems or individuals located in foreign countries. During this meeting, CMS requested system logs and data on the Speridian Companies' IT security practices and rules to evaluate these reports. Speridian Companies supplied additional information by email on the evening of August 13, 2024.

14. On August 14, 2024, CMS reviewed the information BenefitAlign and TrueCoverage supplied on the evening of August 13, 2024. CMS reviewed logs showing when certain persons had logged in and accessed the direct enrollment platform. CMS also reviewed the platform's system settings, focusing on identifying the settings that should be in place to block platform access from locations outside of the United States. CMS also reviewed logs showing when persons accessed the platforms through virtual private networks (VPNs), an information technology tool that creates a secure connection between a device and a network over the internet. VPNs also encrypt data and mask internet protocol (IP) addresses so that a user's location is not divulged.

15. CMS's review of this information raised additional questions and concerns. BenefitAlign had provided CMS information on three corporate VPN solutions that were in place for their workforce. These corporate VPN solutions are the appropriate way for users to connect to BenefitAlign. During CMS's review of the access logs CMS found three unexpected IP addresses indicating that the platforms had been accessed from outside of the United States. These three IP addresses belong to companies known for providing private VPN services, such as M247 Europe, Level 3, and Cloudflare. The presence of these VPN connections raised significant security concerns. Private VPNs like those cited above can be used to mask specific geographic location of the person who has connected to the Speridian Companies' environment.

---

The allowance of private VPN connections is direct evidence that the Speridian Companies cannot offer the assurances they provided in the August 13 teleconference, specifically 1) no individuals could access their platform from a foreign location and 2) that no data had been accessed from or sent to an individual or system located in a foreign country. Furthermore, the lack of control over the source of connections demonstrates a failure on the part of the Speridian Companies to institute a major security control that is a necessary precondition for an Authority to Connect as an EDE entity, further buttressing CMS's decision to suspend the Speridian Companies' EDE connection.

16. That same day, CMS provided the Speridian Companies a list of additional questions by email. See Email from Keith Busby to the Speridian Companies, dated Aug. 14, 2024. (Exhibit L)

17. On August 15, 2024, CMS and the Speridian Companies met again by video conference. The Speridian Companies representative explained that the Speridian Companies employed three different virtual private network (VPN) solutions: two FortiClient VPNs and one PaloAlto VPN. None of those three VPNs were the same as the private VPNs cited above. These corporate VPN services are considered a best practice as they can ensure a secure, private connection to the EDE platform and encrypt internet traffic to prevent unauthorized interception. CMS similarly uses a corporate VPN that all users must go through when connecting to the secure CMS environment. In contrast to what CMS found with respect to Speridian Companies, CMS does not allow private VPNs to connect either directly to the CMS environment or to the CMS-operated VPN, since private VPNs would completely undermine the security benefits we realize from the use of a secure corporate VPN. CMS requested additional system logs from the Speridian Companies to verify the reported location of the internet protocol (IP) addresses

---

connecting to the Speridian Companies' information systems and the data accessed in those information systems. CMS also requested that the Speridian Companies identify what they have put in place to prevent overseas users from using VPNs to connect to the information systems that contained CMS data and transmit the data to other locations.

18. On August 16, 2024, the Speridian Companies produced certain additional information in response to CMS's August 15, 2024, request. CMS reviewed the information and determined that the Speridian Companies had failed to provide some of the requested data, and the data they did provide revealed that data flowing through the Speridian Companies' VPNs was less voluminous than indicated by the VPN traffic CMS observed in the initial logs received. CMS concluded that the Speridian Companies failed to reply in full to the request for full system logs for the three corporate VPNs. The Speridian Companies also failed to respond to the CMS request to explain any steps the Speridian Companies took to prevent overseas users from using VPNs to connect to the information systems that contained CMS data and transmit the data to other locations. CMS contacted the Speridian Companies to notify them of this failure and also to advise that the Speridian Companies had failed to produce other information CMS requested. See Email from David Paradis to the Speridian Companies, dated Aug. 16, 2024, 2:08 PM EST. (Exhibit M).

19. On August 19, 2024, the Speridian Companies responded to CMS's August 16, 2024, follow-up outreach that identified missing information and data that the Speridian Companies failed to produce in response to the August 13, 2024, request from CMS. CMS's review of this information and data began that day. By August 20, 2024, CMS's review had uncovered new facts that raised additional data security concerns. CMS had previously requested logs from the three VPN solutions the Speridian Companies use, but the Speridian Companies

---

still failed to produce the logs from one VPN and the logs from a second VPN lacked the level of detail generally provided in such logs, rendering them useless for CMS's review. The Speridian Companies also again failed to explain the steps they take to prohibit overseas users from using VPNs to connect to the information systems that contain CMS data and transmit the data to other locations. This repeated failure to explain how the Speridian Companies prevent foreign connections, combined with evidence that they could not prevent those connections called into further question the assurances that they made on the August 13 call that no such connections were allowed or possible. On August 20, 2024, CMS contacted Speridian Companies via email. CMS expressed concern that the Speridian Companies' CRM system had been previously reported to be hosted in Pakistan. CMS specifically inquired about how the Speridian Companies ensured that PII belonging to Exchange applicants and enrollees is protected if the Speridian Companies are using an information system overseas. The Speridian Companies submitted additional evidence to support their assertions that their information systems accessing CMS data are entirely inside the United States. See Email from David Paradis to the Speridian Companies, dated Aug. 20, 2024, 3:29 PM EST. (Exhibit N).

20. On August 22, 2024, the Speridian Companies produced the remaining information CMS requested, including data artifacts that were very large and would take days to analyze. CMS completed this data import on August 27, 2024, and immediately began its analysis of the data.

21. CMS's analysis revealed suspicious activity, including impossible changes in location by an individual user. For example, CMS's analysis found that on July 29, 2024, a Speridian Companies employee or contractor was authenticated at a CenturyLink IP address in Florida. Only ten minutes later, the same user showed as authenticated from a Verizon IP address

---

in Ohio, Illinois, or Virginia (depending on the geolocation database used for this research). In another such instance on August 5, 2024, the user was authenticated via a Verizon IP address with an IP address in California or Virginia (depending on the geolocation database), and six minutes later was authenticated via an AT&T IP address in North Carolina or Georgia (depending on the geolocation database). It is impossible for a person to simultaneously be located in multiple states within a 10-minute period. The failure to note that a single user had ‘location hopped’ is a significant security failure that appears sufficient to terminate the Speridian Companies’ authority to connect to CMS systems and their associated EDE Agreements. CMS finds this event particularly concerning in concert with the allegations of foreign connections, because the only way for a single user to show as authenticating from different locations that are a significant distance apart is by using a VPN anonymizer. VPN anonymizers may be used to mask an end user’s actual geographic location and circumvent geofencing rules. That masking would include the ability to mask a user accessing the system from a foreign location.

22. Additional data analysis revealed multiple other anomalies, including access to the Speridian Companies’ EDE platforms by at least eleven unique users from overseas locations, including India and Pakistan. These connections directly contradict the Speridian Companies’ assurances on the August 13 teleconference that no foreign connections were allowable or possible. These connections also appear to constitute grounds for immediate termination of the Speridian Companies’ authority to connect and EDE agreement.

23. On August 28, 2024, CMS requested additional information from the Speridian Companies to evaluate these anomalies. Requested artifacts included virtual private cloud (VPC) flow logs for their Amazon Web Services (AWS) accounts, a list of IP addresses that are on their

---

allowed traffic list, details on controls in place to prevent VPN anonymizing solutions from circumventing geofencing rules and rules around acceptable use of TeamViewer, a desktop sharing service, within the Speridian Companies information systems. *See* Email from David Paradis to the Speridian Companies, dated Aug. 28, 2024, 12:12 PM EST. (Exhibit O).

TrueCoverage and BenefitAlign filed a lawsuit challenging the suspension on August 29, 2024.

24. On September 2, 2024, CMS sent a formal notice informing the Speridian Companies that pursuant to 45 C.F.R. §§ 155.220(c)(4)(ii) and 155.221(e), and attributable to credible allegations of misconduct described in the notice, CMS was immediately suspending True Coverage LLC's, TrueCoverage dba Inshura's, and BenefitAlign's ability to transact information with the Exchanges. CMS also suspended the Speridian Companies' ability to make its non-Exchange websites available to other agents and brokers to transact information with the Exchanges. Pursuant to 45 C.F.R. § 155.220(c)(5) and section X.m. of the executed Enhanced Direct Enrollment (EDE) Agreement, section X.l. of the executed Web-Broker Agreement, and section 15 of the executed Interconnection Security Agreement (ISA), CMS also notified the Speridian Companies of its intent to conduct a compliance review and audit.

25. Specifically, CMS concluded that there was strong evidence showing prohibited foreign access to Direct Enrollment platforms. First, CMS found that the Speridian Companies were using a VPN anonymizer. A VPN anonymizer masks the source of the IP address, which can be used to indicate the geographic location of the user and is often used to get around location-based restrictions or nefarious activities. Second, CMS observed suspicious logins and rapid switching between locations within minutes, which raised additional concerns about the use of VPNs being used to mask the true geographic locations of the users and whether the access to CMS data, particularly Exchange consumer PII, is made accessible from unauthorized

---

locations outside of the United States. Third, CMS also found some users were accessing a cloud environment from IP addresses that we were unable to determine the geographic location(s) of, which indicates location masking. For example, such users may be utilizing a VPN anonymizer or an unregistered third-party. All of these fact patterns are concerning because Speridian entities' allowance of masking of geographic locations coupled with suspicious and rapid login activity allows users to access Exchange consumer data, including PII, purposefully obscuring activity from CMS and other federal oversight. CMS has also found instances of access from overseas, which warrants further investigation via the audit that has now commenced. The agreements Speridian entities signed with CMS do not allow CMS data to flow outside the bounds of the United States given the significant threat it can pose to Exchange consumers and their data if CMS is unable to have full control oversight of the data.

25. As of the time of my execution of this declaration, the Speridian Companies have failed to provide a reasonable explanation for the anomalies CMS first detected on August 6, 2024, and the additional anomalies that have been identified during the review of evidence that the Speridian Companies have produced.

26. The review by myself and my team has uncovered multiple violations of the EDE and web broker agreements, as well as vastly inadequate security protections of consumer data, each of which appear to constitute grounds for termination of these agreements and the authority to connect. CMS is in the process of determining the extent of the Speridian Companies' violations, and the harm to consumers and the Exchange. While we continue with the assessment, we have determined that it is in the interest of the consumers whose data we safeguard to keep the Speridian Companies' suspension in place.

---



27. Thus far, the Speridian Companies have not responded to the identified concerns with information to sufficiently mitigate or otherwise remedy these concerns. CMS is in the process of conducting an audit, during which the Speridian companies will have the opportunity to present documentation of their compliance to all applicable federal regulations and CMS Agreements. After CMS reviews the results of the audit, CMS will use the information garnered through the audit to determine whether the concerning activities rise to the level of violations or non-compliance such that it would be appropriate to move forward with suspending or terminating these entities Exchange Agreements (which ends their ability to participate in the Exchanges) and possibly impose other penalties. That decision is subject to an administrative process which results in a final agency decision. The result of that audit and the ensuing administrative review could uphold the suspension, it could reverse the suspension, or it could otherwise find that our current security risks have been sufficiently mitigated or remedied, but that process is ongoing and is not yet final.

\* \* \*

---

I declare under penalty of perjury under the law that the foregoing is true and correct to the best of my knowledge and understanding.

**Keith Busby** Digitally signed by Keith Busby  
Date: 2024.09.20 22:26:26  
-04'00'

---

Keith Busby

Dated: September 20, 2024

---

# **Exhibit A**

From: Robenson Remelus <REDACTED>  
Sent: Tuesday, July 23, 2024 3:54:16 PM (UTC-07:00) Mountain Time (US & Canada)  
To: CMS\_IT\_Service\_Desk <REDACTED>  
Subject: Ticket: CS2206633

To whom it may concern,

My name is Robenson Remelus, NPN 15479763

I am writing to let you know that there have been fraudulent activities on my account which caused my suspension. There is a company that used my credentials without my permission. My ACA business written is in Florida, so there should be no other State ACA plans under my FFM. I have attached documents showing I was a victim of a data breach and also found out that the same company has a RICOT case pending against them. Please reinstate my FFM as this is causing me a lot of financial hardship. I can be reached at 305-915-2264 or 786-448-7555. if you have any questions..

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

CASE NO.

CONSWALLO TURNER, TIESHA  
FOREMAN, ANGELINA WELLS,  
VERONICA KING, NAVAQUOTE, LLC  
and WINN INSURANCE AGENCY, LLC,  
individually and on behalf of all others  
similarly situated,

**CLASS ACTION**

(Jury Trial Demanded)

Plaintiffs,

v.

ENHANCE HEALTH, LLC,  
TRUECOVERAGE, LLC,  
SPERIDIAN TECHNOLOGIES, LLC,  
NUMBER ONE PROSPECTING, LLC  
d/b/a MINERVA MARKETING,  
MATTHEW B. HERMAN and  
BRANDON BOWSKY,

Defendants.

\_\_\_\_\_ /

**CLASS ACTION COMPLAINT**

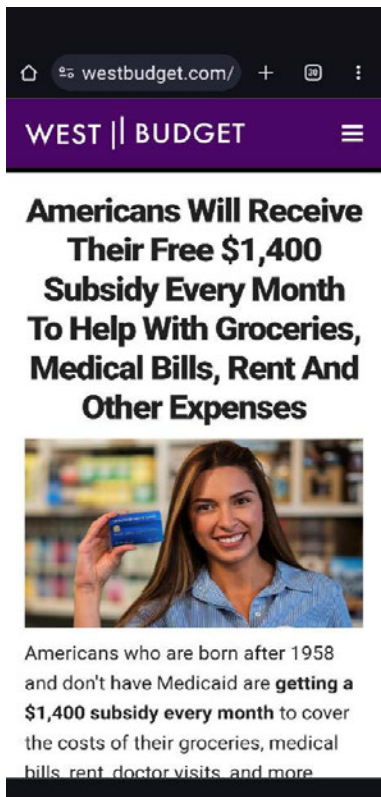
Class Plaintiffs, Conswallo Turner, Tiesha Foreman, Angelina Wells, Veronica King, NavaQuote, LLC (“NavaQuote”) and WINN Insurance Agency LLC (“WINN”), file this class action complaint individually and on behalf of all others similarly situated against Defendants, Enhance Health, LLC (“Enhance Health”), TrueCoverage, LLC (“True Coverage”), Speridian Technologies, LLC (“Speridian”), Matthew B. Herman, Number One Prospecting, LLC d/b/a Minerva Marketing (“Minerva”) and Brandon Bowsky, and allege:

**I. INTRODUCTION**

1. Defendants constitute a RICO Enterprise targeting the poorest members of American society. The consumer victims of this Enterprise comprise the first of two primary

classes in this lawsuit, the “Consumer Class.” Defendants’ motives are simple — maximize profits by seizing the Affordable Care Act (“ACA”) health insurance market for low-income Americans. Defendants’ tactics also directly injure the healthcare insurance agents who comprise this suit’s other primary class, the “Agent Class.”

2. Since at least 2022, Defendant TrueCoverage and its largest “downline” agent, Enhance Health, along with other relevant nonparties that serve as their downline agents, have spent tens of thousands of dollars daily to purchase Consumer Initiated Inbound Calls (“CIICs” or “Leads”) from outside lead-generation firms, including Defendant Minerva, that “capture” those victims by running fraudulent ads on social media. These ads lure consumers with the false promise of hundreds of dollars per month in cash benefits, such as subsidy cash cards to pay for common expenses like rent, groceries and gas:



3. TrueCoverage and Enhance Health, which have sales operations based primarily in Broward County, Florida, know these Leads are generated fraudulently. They know that the ads mischaracterize as “cash” advance premium tax credits (or “APTCs”) paid by the federal government directly to the insurance carriers (not consumers) to offset the cost of premiums for the health insurance. They know consumers are calling for the promise of cash benefits that do not exist.

4. But using uniformly constructed sales scripts designed to deflect consumers’ inquiries about the monthly cash payments, TrueCoverage, Enhance Health and their downline agents mislead consumers to believe that those cash benefits will be coming “in the mail” from health insurance companies like Ambetter, Cigna and others. TrueCoverage, Enhance Health and their downline agents use these sales calls to obtain the consumers’ names, birthdates and states of residence, access their information and enroll them into ACA health insurance plans for a commission.

5. What TrueCoverage, Enhance Health and their downlines *then* do with this personally identifiable information (or “PII”), whether the consumer enrolls in a healthcare plan or not, forms another facet the RICO Enterprise. TrueCoverage, Enhance Health and their downlines use the PII to access the accounts of consumers who already have an ACA health plan, then remove the plan’s agent of record (or “AOR”). They replace that AOR with their own in-house or downline AOR. These “AOR Swaps” are done without the consumer’s knowledge or consent, and allow TrueCoverage, Enhance Health and their downlines to essentially steal the original AOR’s commissions for the policy. Class Plaintiff Veronica King’s AOR was swapped at least eight times.

6. TrueCoverage, Enhance Health and their downlines sometimes go even farther, by “Twisting” the consumer’s existing policy. Twisting is a form of insurance fraud that involves replacing an existing insurance plan with another plan that has similar or worse benefits solely to generate a new commission. TrueCoverage, Enhance Health and their downlines can do this by changing a discrete piece of information about the consumer within the ACA database — for example, by changing the consumer’s address slightly, or adding a middle initial. They do this without the consumer’s knowledge or consent. Class Plaintiffs Turner, Wells and Foreman were all victims of Twisting by TrueCoverage, Enhance Health and/or their downlines.

7. TrueCoverage, Enhance Health and their downlines also use consumers’ PII to create entirely new applications in the ACA database that result in an additional policy or multiple policies for one consumer without that consumer’s knowledge or consent. TrueCoverage, Enhance Health and their downlines sometimes accomplish this “Dual-App” scheme by breaking up a family into two plans — for example, creating a new policy for the husband while leaving the wife and children on the original policy. Class Plaintiff Foreman (and her husband) were victimized by this Dual-App scheme.

8. Class Plaintiffs and Consumer Class members suffered damages as a result of these actions. They suffered out-of-pocket damages relating to the loss of medical treatments, the loss of in-network health care providers and specialists, the loss of prescription coverage, an increase in the amount of the co-pays covered by the policies and/or even the loss of coverage altogether. They suffered out-of-pocket costs relating to correcting the changes to their data and AORs. And some, like Class Plaintiff Tiesha Foreman, suffered tax penalties from being put into plans they did not qualify for.



9. Health insurance agents comprising the “Agent Class” were also damaged. Class Plaintiffs NavaQuote and WINN Insurance Agency, and Agent Class members like them, have each lost thousands of dollars in commissions from these AOR-Swap, Twisting and Dual-App schemes. They have also incurred thousands of dollars in heroic but Sisyphean efforts to stop this practice.

10. The key to the Enterprise’s ability to pull off this scheme lies in the technology at its center. For at least two years, TrueCoverage, Enhance Health and their downlines have utilized a proprietary enhanced direct enrollment platform (or “EDE Platform”) called Benefitalign, which was developed by TrueCoverage’s parent company, Defendant Speridian. Benefitalign gives them direct access to the ACA Marketplace Exchange database (the “Marketplace” or “Exchange”) maintained and facilitated by the U.S. Department of Health and Human Services, Centers for Medicare and Medicaid Services (or “CMS”). Using Benefitalign, TrueCoverage, Enhance Health and their downlines can enroll consumers in ACA health insurance without requiring them to visit [www.healthcare.gov](http://www.healthcare.gov) (or “Healthcare.gov”). Benefitalign enables TrueCoverage, Enhance Health and their downlines to enroll the maximum number of consumers in the shortest amount of time without outside scrutiny. Most importantly, it allows TrueCoverage, Enhance Health and their downlines to make unilateral changes to a consumer’s data on the Exchange database, including canceling in-force health insurance plans or changing the AOR. All that is needed is the consumer’s name, date of birth and state of residence — information gathered from the consumer when he or she reached out, seeking cash benefits, in response to a fraudulent ad. In mid-2023, Enhance Health purchased its own proprietary EDE Platform, JET Health Solutions, to continue doing what it was doing with Benefitalign.

11. Other members of the RICO Enterprise include the individuals who control Enhance Health and Minerva. Matthew Herman, 38, is the CEO of Enhance Health, which acted as TrueCoverage’s downline agent and used Speridian and Benefitalign’s platform technology. Herman touts himself as a “Famed Business Mogul & Investor” on his Instagram account, “moneymatt305.” Herman, too, knew about his company’s purchase of Leads generated by fraudulent ads, yet directed and/or allowed Enhance Health’s ongoing use of the misleading sales scripts and twisting of consumer insurance policies, as well as its use of the AOR-Swap, Twisting and Dual-App schemes.

12. Brandon Bowsky, 31, is founder and CEO of Minerva, which both generates and buys and sells Leads sourced from fraudulent ads. Bowsky has stated publicly that he was the first person to advise insurance agencies to enter the ACA space for low-income consumers. His company Minerva was Enhance Health’s primary lead generator and sold Leads to TrueCoverage and its downlines as well. Bowsky knew that Minerva’s Leads were being used by Enhance Health, TrueCoverage and their downlines to sell health insurance to consumers who were seeking the advertised monthly cash payments. In fact, as explained below, Bowsky and Minerva recorded the confidential calls between consumers and TrueCoverage and Enhance Health agents without the consent of Consumer Plaintiffs and Class Members, in violation of multiple ACA federal regulations. He knew the lure of cash benefits was causing consumers to call, and that the agencies Minerva sold the fraudulent Leads to use them to enroll those consumers into a healthcare plan, thus increasing the demand for Minerva’s Leads.

13. Defendants’ actions constitute a RICO Enterprise. Class Plaintiffs, on behalf of the class members they represent, seek an injunction stopping Defendants from continuing the schemes described in this lawsuit. Class Plaintiffs also seek damages on behalf of themselves, the

Consumer Class and the Agent Class for the economic injuries caused by Defendants’ actions, as well as an award of treble damages and attorney’s fees and costs. Finally, Consumer Class Plaintiffs and class members seek damages arising out of Defendants’ failure to protect Class Plaintiffs’ and class members’ PII from unlawfully being accessed, collected, used and/or disclosed.

## II. PARTIES, JURISDICTION AND VENUE

### A. Plaintiffs

14. Plaintiff Conswallo Turner is a resident and citizen of the state of Texas. Turner is a “person” under 18 U.S.C. § 1964.

15. Plaintiff Tiesha Foreman is a resident and citizen of the state of Georgia. Foreman is a “person” under 18 U.S.C. § 1964.

16. Plaintiff Angelina Wells is a resident and citizen of the state of Texas. Wells is a “person” under 18 U.S.C. § 1964.

17. Plaintiff Veronica King is a resident and citizen of the state of Georgia. King is a “person” under 18 U.S.C. § 1964.

18. Plaintiff NavaQuote, LLC is a Delaware limited liability company with its principal place of business in the state of Georgia. NavaQuote is a “person” under 18 U.S.C. § 1964. NavaQuote’s members are Callie Navrides and Peter Navrides, both residents and citizens of Georgia.

19. Plaintiff WINN Insurance Agency LLC is a Florida limited liability company with its principal place of business in the state of South Carolina. WINN is a “person” under 18 U.S.C. § 1964. WINN’s sole member is Marsha Broyer, a resident and citizen of South Carolina.

**B. Defendants**

20. Defendant Enhance Health, LLC is a Florida limited liability company with its principal place of business in Broward County, Florida. Enhance Health is an entity capable of holding a legal or beneficial interest in property and is therefore a culpable “person” under 18 U.S.C. § 1961. Enhance Health’s sole member and manager is Matthew Herman.

21. Defendant Matthew Herman is a citizen and resident of Broward County, Florida. He is the sole member and manager, and Chief Executive Officer, of Enhance Health.

22. Defendant TrueCoverage, LLC is New Mexico limited liability company registered to do business in the State of Florida. TrueCoverage is an entity capable of holding a legal or beneficial interest in property and is therefore a culpable “person” under 18 U.S.C. § 1961. TrueCoverage’s member is Girija Panicker, a citizen and resident of New Mexico.

23. Defendant Speridian Technologies, LLC is a New Mexico limited liability company registered to do business in the State of Florida. Speridian is an entity capable of holding a legal or beneficial interest in property and is therefore a culpable “person” under 18 U.S.C. § 1961. Speridian’s manager is Girish Panicker and its member is Hari Pillai, who are both residents and citizens of New Mexico.

24. Defendant Number One Prospecting LLC d/b/a Minerva Marketing is a Florida limited liability company with its principal place of business is in Broward County, Florida. Minerva is an entity capable of holding a legal or beneficial interest in property and is therefore a culpable “person” under 18 U.S.C. § 1961. Minerva’s sole member and manager is Brandon Bowsky.

25. Defendant Brandon Bowsky is a resident and citizen of Broward County, Florida, and is the sole member and manager of Minerva, and also serves as its president.

**C. Subject Matter Jurisdiction**

26. The Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d), because (i) the matter in controversy exceeds \$5 million, exclusive of interest and costs; (ii) there are members of the proposed Classes who are citizens of different states than Defendants; and (iii) there are in the aggregate more than 100 members of the proposed classes. This Court also has federal question subject matter jurisdiction pursuant to 18 U.S.C. § 1964.

**D. Personal Jurisdiction**

27. Enhance Health, LLC (“Enhance Health”). This Court has specific personal jurisdiction over Enhance Health pursuant to Section 48.193(1)(a), Fla. Stat. Enhance Health regularly and systematically operates, conducts, engages in and carries on a business or business venture in Florida. It is registered with the Florida Secretary of State’s office to do business in Florida. Enhance Health maintains its headquarters and principal place of business in Sunrise, Florida. It also has offices in Miramar and Coral Springs, Florida. Its sole member is Matthew Herman, a South Florida resident. Enhance Health also caused injury to persons or property within Florida that arose out of acts and omissions it took inside the state while engaging in solicitation of, or service activities for, people within Florida. Moreover, as further alleged in this Complaint, Enhance Health committed one or more tortious acts within Florida.

28. This Court also has general personal jurisdiction over the Enhance Health pursuant to Section 48.193(2), Fla. Stat. Enhance Health is engaged in substantial and not isolated activity within this state.

a. From its offices in South Florida, Enhance Health solicited and interacted with consumers in Florida and throughout the country via telephone, internet, text,

email and mail.

b. Pursuant to an exclusive agreement, it purchased fraudulent Leads from a Florida-based company, Defendant Minerva.

c. Enhance Health's agents, from offices in South Florida, made misrepresentations and omissions that induced Consumer Class members, including a substantial number of Florida consumers, to enroll in ACA health insurance plans.

d. From its offices in South Florida, Enhance Health obtained Consumer Class members' PII, and subsequently used that information to re-enroll Consumer Class members into additional ACA health insurance plan(s) without proper knowledge and consent.

e. From its offices in South Florida, it engaged in AOR Swaps, Twisting and Dual Apps.

f. From its offices in South Florida, Enhance Health submitted Consumer Class members' health insurance applications to the ACA Marketplace.

g. Enhance Health received commission payments to its offices in South Florida.

h. Enhance Health wired commissions to its agents from its offices in South Florida.

i. Enhance Health wired payments to downline agents in Florida.

j. Enhance Health entered into contracts in the State of Florida, including but not limited to contracts with its agents that operated from Enhance Health call centers located in its offices in South Florida.

k. Enhance Health provided customer service to Class Plaintiffs and class members from its offices in Florida.

l. Enhance Health sent enrollment documents to the Marketplace as well as documents and communications to Plaintiffs and class members from its offices in Florida.

m. From its Florida offices, Enhance Health paid advances to its downline agents to support the unlawful misconduct alleged herein.

29. Matthew Herman (“Herman”). Herman is an individual who during all times was a resident and citizen of the state of Florida. Herman is Enhance Health’s managing member and Chief Executive Officer. Working from Enhance Health’s South Florida offices, Herman oversaw and directed the Enhance Health sales team and the misleading scripts that they used with consumers. He directed Enhance Health’s strategy and growth, embracing a strategy that relied upon the use of fraudulent Leads to enroll consumers in ACA health plans, twist those plans and remove and replace agents of record.

30. TrueCoverage, LLC. This Court has specific personal jurisdiction over TrueCoverage pursuant to Section 48.193(1)(a), Fla. Stat. TrueCoverage regularly and systematically operates, conducts, engages in and carries on a business or business venture in Florida. TrueCoverage maintains or maintained within the relevant period offices in Miramar, Deerfield Beach and Miami. It is registered with the Florida Secretary of State’s office to do business in Florida. Its registered agent is Matthew Goldfuss, a Florida resident. True Coverage also caused injury to persons or property within Florida that arose out of acts and omissions it took inside and outside the state while engaging in solicitation of, or service activities for, people within Florida. Moreover, as further alleged in this Complaint, TrueCoverage committed one or more

tortious acts within Florida.

31. This Court also has general personal jurisdiction over TrueCoverage pursuant to Section 48.193(2), Fla. Stat. TrueCoverage is engaged in substantial and not isolated activity within this state.

a. From its offices in South Florida, TrueCoverage solicited and interacted with consumers in Florida and throughout the country via telephone, internet, text, email and mail.

b. It purchased fraudulent Leads from a Florida-based company, Defendant Minerva.

c. TrueCoverage's agents, from offices in South Florida, made misrepresentations and omissions that induced Consumer Class members, including a substantial number of Florida consumers, to enroll in ACA health insurance plans.

d. From its offices in South Florida, it engaged in AOR Swaps, Twisting and Dual Apps.

e. From its offices in South Florida, TrueCoverage obtained Consumer Class members' PII, and subsequently used that information to re-enroll those Consumer Class members (many of whom were in Florida) into new or additional health insurance plan(s) without proper knowledge and consent.

f. From South Florida, TrueCoverage agents submitted Consumer Class members' health insurance applications to the ACA Marketplace.

g. TrueCoverage received commission payments to its offices in South Florida.



- h. TrueCoverage wired commissions to its agents from its offices in South Florida.
- i. TrueCoverage wired payments to downline agents, including Enhance Health, in Florida.
- j. TrueCoverage entered into contracts in the State of Florida, including but not limited to contracts with agents that operated from TrueCoverage call centers located in its offices in South Florida.
- k. TrueCoverage provided customer service to Class Plaintiffs and class members from its offices in Florida.
- l. TrueCoverage sent enrollment documents to the Marketplace as well as documents and communications to Plaintiffs and class members from its offices in Florida.
- m. From its Florida offices, TrueCoverage paid advanced commissions to its downline agents to support the unlawful misconduct alleged herein.

32. Speridian Technologies, LLC (“Speridian”). This Court has specific personal jurisdiction over Speridian pursuant to Section 48.193(1)(a), Fla. Stat. Speridian regularly and systematically operates, conducts, engages in and carries on a business or business venture in in Florida. Speridian is registered with the Florida Secretary of State’s office to do business in Florida. Speridian controls Defendants TrueCoverage and Benefitalign. As further alleged in this Complaint, Speridian committed one or more tortious acts within Florida by controlling and financing the Florida operations of TrueCoverage and Benefitalign, including but not limited to paying the salaries of TrueCoverage’s agents in Florida, with knowledge that TrueCoverage and Benefitalign were committing a fraud.

33. This Court also has general personal jurisdiction over Speridian pursuant to Section 48.193(2), Fla. Stat. Speridian is engaged in substantial and not isolated activity within this state.

a. Speridian developed and provided access to the platform used by Florida-based companies, like Enhance Health, and companies operating in Florida, like True Coverage, to enroll and manage consumers, including a substantial number of Florida-based consumers, as part of the Enterprise and scheme described in this lawsuit.

b. Speridian financed TrueCoverage's and Benefitalign's operations and growth in South Florida by paying advanced commissions as well as by paying the salaries of TrueCoverage's health insurance agents and Benefitalign's employees. These financial arrangements were memorialized in loan agreements and employment agreements executed in Florida.

34. Number One Prospecting, LLC d/b/a Minerva Marketing ("Minerva"). This Court has specific personal jurisdiction over Minerva pursuant to Section 48.193(1)(a), Fla. Stat. Minerva is a Florida limited liability company which maintains its headquarters and principal place of business in Fort Lauderdale, Florida. It regularly and systematically operates, conducts, engages in and carries on a business or business venture in Florida, and has at least one office in Florida. Minerva also caused injury to persons or property within Florida that arose out of acts and omissions it took inside and outside the state while engaging in solicitation of, or service activities for, people within Florida. Minerva committed one or more tortious acts within Florida.

35. This Court also has general personal jurisdiction over the Enhance Health pursuant to Section 48.193(2), Fla. Stat. Minerva is engaged in substantial and not isolated activity within this state.

- a. From its offices in South Florida, Minerva generated and bought Leads and sold them to health insurance brokers in Florida, including but not limited to Enhance Health and TrueCoverage, for the enrollment of consumers into health insurance policies under the ACA.
- b. Minerva received payments for its Leads at its offices in Florida.
- c. Minerva entered into contracts in Florida, including an exclusive agreement whereby Enhance Health, a Florida-based company, agreed to buy all of its Leads from Minerva.
- d. From its offices in South Florida, Minerva obtained Consumer Class members' personally identifiable information and monitored those members' calls in violation of federal regulations.

36. Brandon Bowsky ("Bowsky"). Bowsky is an individual who during all times material was a resident and citizen of the state of Florida. Bowsky is founder and CEO of Minerva. Bowsky has stated publicly that he was the first person to advise agencies like TrueCoverage and Enhance Health to enter the ACA space for low-income consumers. Bowsky knew that the creation of that industry would result in demand for his company's Leads. Indeed, Minerva became Enhance Health's exclusive lead generator and also sold Leads to TrueCoverage. Bowsky directed Minerva's strategy and growth, and caused Minerva to generate and buy, and then sell to Enhance Health, TrueCoverage and their downlines, Leads that misleadingly represented to consumers that they would receive cash benefits. Bowsky knew that Minerva's Leads were being used by Enhance Health, TrueCoverage and their downlines to sell health insurance to consumers who were seeking the advertised monthly cash payments. He knew the lure of cash benefits were causing consumers to call, and that the agencies to whom Minerva sold the fraudulent Leads used

them to enroll those consumers into a healthcare plan, thus increasing the demand for Minerva's Leads.

37. Venue. Venue is proper in this District pursuant to 28 U.S.C. § 1391 and 18 U.S.C. § 1965 because (i) a substantial part of the events or omissions giving rise to Class Plaintiffs' claims occurred in this District, and (ii) each of the Defendants' contacts with this District would be sufficient to subject them to personal jurisdiction in this District if this District were a separate State. Defendants regularly and systematically operate, conduct, engage in and carry on a business or business venture in this District, and have generated significant revenue from consumers in this District. Defendants committed one or more tortious acts within this District. Defendants' contacts within this District were substantial and not isolated.

### **III. RELEVANT NONPARTIES**

38. Benefitalign, LLC ("Benefitalign"). Benefitalign LLC operates a proprietary enhanced direct enrollment platform (or "EDE Platform") owned and developed by Speridian. Benefitalign has provided TrueCoverage (and until June 2023, Enhance Health) direct access to the Exchange. Using Benefitalign, TrueCoverage, Enhance Health and their downlines have enrolled consumers in ACA health insurance without requiring them to visit Healthcare.gov.

39. JET Health Solutions. Like Benefitalign, JET Health Solutions is a CMS-approved, Phase 3 Enhanced Direct Enrollment provider. It was purchased by Enhance Health in July 2023. Upon information and belief, after the acquisition Enhance Health began enrolling class members, possibly including some of the Class Plaintiffs, into ACA plans through the newly acquired EDE platform.

40. Inshura, LLC. Inshura is owned and controlled by Speridian. It is a CMS-approved, Phase 3 Enhanced Direct Enrollment platform. Certain TrueCoverage downlines such

as Protect Health/DMS, listed above, use Inshura to enroll class members, possibly including some of the Class Plaintiffs, into ACA plans through that EDE platform.

41. Girish Panicker (“Panicker”). Panicker is founder and Chairman of the Board of Speridian and its group of companies, including TrueCoverage and Benefitalign. Panicker oversees and directs Speridian, TrueCoverage and Benefitalign. During the relevant timeframe, he directed those companies’ strategy and growth, embracing a strategy that relied upon the use of fraudulent Leads to enroll consumers, including a substantial number of Florida customers, in ACA health plans, and to twist those plans and remove and replace agents of record.

42. Matthew Goldfuss (“Goldfuss”). Goldfuss is TrueCoverage’s National Director: Individual and Medicare Sales. Working from TrueCoverage’s South Florida offices, Goldfuss oversees and directs the TrueCoverage sales team and the misleading scripts that they used with consumers.

43. Bain Capital Insurance. According to its press releases, Bain Capital Insurance provided Enhance Health with \$150 million in capital in November 2021. Bain Capital Insurance is the dedicated insurance investment and solutions business of Bain Capital, a leading global private investment firm with over \$150 billion under management across 22 offices on four continents. Enhance Health uses the capital provided by Bain Capital Insurance to finance its call centers and the commissions of its downline agencies.

44. Protect Health and Digital Media Solutions. Protect Health is a health insurance agency based in Nevada that is owned by the publicly traded company, Digital Media Solutions (“DMS”). Protect Health has agents in numerous states across the country who sell ACA health plans to members of the class. Protect Health has been a downline agency of TrueCoverage since at least October 1, 2023. TrueCoverage has a downline producer agreement with Protect Health

and is involved in the selling of policies based on the fraudulent advertisements described in the complaint. DMS also sold Leads to Enhance Health and TrueCoverage that were generated from the deceptive advertisements at issue in the case.

45. Ensure Health Group Corporation and Barachy Lucian. Ensure Health Group Corporation is a Delaware corporation with a principal place of business in Plantation, Florida. According to the Florida Secretary of State's website, Barachy Lucian is the Vice President of Ensure Health Group. Ensure Health Group is a downline agency of TrueCoverage and has a downline producer agreement with Protect Health and is involved in selling ACA health plans to class members. Beginning in at least 2022, Barachy Lucian was involved in training TrueCoverage's and Enhance Health's agents on selling ACA health insurance plans through Speridian's EDE platform, Benefitalign.

46. Health First Insurance Agency. Health First Insurance Agency is a health insurance agency that sells ACA health plans to class members. According to the Florida Department of Financial Service, Jonathan Massa is the agent in charge of Health First Insurance Agency, and until approximately March 5, 2024, was a downline agency of Enhance Health. Health First Insurance Agency is involved in the selling of policies based on the fraudulent advertisements described in the complaint.

47. My Health Advisers, Inc., Erica Richmond and Gabriel Pasztor. My Health Advisers, Inc. is a Florida corporation created on April 18, 2019. It has a principal place of business in Broward County, Florida. My Health Advisers is an insurance agency located in Oakland Park, Florida. According to records maintained by the Florida Department of Financial Services, Gabriel Pasztor is listed as the agent in charge of My Health Advisers, Inc.

48. According to the Florida Secretary of State's website, Erica Richmond was the

President of My Health Advisers from September 16, 2020, to August 26, 2022. During some of this time period, Erica Richmond was the head of customer service for Enhance Health.

49. Gabriel Pasztor is listed on the Florida Secretary of State's records as President of the company from August 26, 2022, to the present. Upon information and belief, Gabriel Pasztor and his wife Paola Fritz are listed as AOR on many of ACA health plans sold to Plaintiffs and class members. Erica Richmond, Gabriel Pasztor and his wife Paola Fritz have relevant information about the sale of the policies and the allegations related to AOR switching.

50. PolicyBind, LLC. PolicyBind, LLC is a Florida limited liability company with a principal place of business in Miami, Florida. PolicyBind generated Leads from deceptive and fraudulent advertisements and sold them to TrueCoverage and/or Enhance Health.

51. WeCall Media, Inc. WeCall is a Delaware corporation with a principal place of business in North Carolina. WeCall generated Leads from deceptive and fraudulent advertisements and sold them to TrueCoverage and/or Enhance Health.

52. My ACA, LLC. My ACA, LLC is a Delaware limited liability company and is a related entity to WeCall Media, LLC. My ACA, LLC sold Leads to TrueCoverage and/or Enhance Health that were generated from the deceptive and fraudulent advertisements at issue.

53. Retreaver. Retreaver is a Canadian software company based in Ontario, Canada. According to its website, Retreaver is a cloud-based software that provides real-time, inbound call data by tagging, tracking and routing callers to agents. Upon information and belief, Defendants Minerva and Bowsky use(d) Retreaver to tag, track and route incoming calls (Leads) from class members who responded to the fraudulent and deceptive advertisements to Defendants' sales agents. The Retreaver software was/is also used by Minerva and Bowsky to record the confidential phone calls between Enhance Health's agents and consumers without the knowledge

and consent of members of the class.

54. Esotech d/b/a Total Leads Domination (“TLDCRM”). Esotech, Inc. d/b/a Total Leads Domination is a Florida corporation with its principal place of business located in Hialeah, Florida. According to its website, TLDCRM provides, among other things, dialer services, lead management services and data management services. Throughout the class period, Enhance Health and TrueCoverage used the TLDCRM software for their CRM (Customer Relationship Management) system. They used TLDCRM, in part, to accept inbound calls at their call centers that were routed to them by software such as Retreaver throughout the Class Period.

55. John Doe Entities. All lead generation firms, downline agencies and agents referenced in **Exhibit 1**.

#### **IV. FACTUAL BACKGROUND**

56. As a starting point, it is helpful to understand the ACA regulations that address how consumers, including Class Plaintiffs and class members, are enrolled into the ACA health insurance at issue, how Defendants fit into the regulatory framework and how Defendants violate those regulations.

##### **A. The ACA and How the Private Sector Became Involved in the Enrollment Process**

57. The Patient Protection and Affordable Care Act (“ACA”), signed into law on March 23, 2010, was intended to reform aspects of the private health insurance market and expand the availability and affordability of health care coverage. The ACA provides an opportunity for individuals who do not have group health insurance through their employer and are not on Medicare or public assistance programs such as Medicaid, to purchase individual health insurance each year.



58. The ACA required the establishment of a health insurance marketplace in each state and the District of Columbia to assist individuals and small businesses in comparing, selecting and enrolling in health plans offered by participating private issuers of qualified health plans. CMS is responsible for overseeing the establishment of these marketplaces, including creating a federally facilitated marketplace (“FFM” or the “Marketplace”) for states not establishing their own. CMS was responsible for designing, developing and implementing the IT systems needed to support the Marketplace. This included the creation of Healthcare.gov — the website that provides a consumer portal to the Marketplace — and related data systems supporting eligibility and enrollment.

59. The Marketplace began accepting applications for consumer enrollment on October 1, 2013. However, individuals attempting to access Healthcare.gov encountered numerous problems. In response to these problems, CMS began seeking ways to incorporate the private sector into developing and integrating technology into the enrollment process.

**1. The Private Sector Enters the Picture Through “Direct Enrollment”**

60. As an initial step, CMS created and allowed for a service called “Direct Enrollment” or “DE.” Direct Enrollment allows private insurance carriers of approved Qualified Health Plans (or “QHPs”) and private third-party “web-brokers” (online insurance agents) to enroll consumers through the Exchange, with or without the assistance of an agent or broker. In this “classic” DE experience, consumers start at a carrier or web-broker’s website and are redirected to Healthcare.gov to complete an eligibility application. After completing the application, they are sent back to the issuer or web-broker’s website to shop for and enroll in a plan.

61. For the first few years, DE experienced technical challenges, in part because many consumers who attempted to enroll through carriers or web-brokers were dropping off in the

middle of the process while being directed back and forth between Healthcare.gov and the carrier or web-broker's site.

**2. Enhanced Direct Enrollment Is Introduced to Expand and Improve the Private Sector's Enrollment Efforts, But Critics Become Concerned**

62. To address the issue, in 2017 the Department of Human Health and Performance announced that the agency was considering creating an "Enhanced Direct Enrollment" (or "EDE") pathway. EDE allows certain private entities, including insurance carriers and web-brokers, to directly enroll consumers into QHPs through the Exchange without redirecting consumers to Healthcare.gov.

63. In November 2018, CMS issued a release that described the rollout of the EDE pathway as a partnership with the private sector to help make enrollment more user friendly. CMS announced that the EDE program would allow the private sector to connect directly to Healthcare.gov and touted a "great new opportunity [for] the private sector to come up with innovative ways to create a uniquely tailored end-to-end user experience."

64. But critics of the EDE pathway model foresaw problems. They warned that giving the private sector such access to the Marketplace database could expose consumers to fraudulent schemes and misleading information on web-broker sites. For example, on March 15, 2019, the Center on Budget and Policy Priorities published a report entitled "'Direct Enrollment' in Marketplace Coverage Lacks Protections for Consumers, Exposes Them to Harm — New 'Enhanced Direct Enrollment' Heightens Risks." The report warned that web-brokers, through the use of marketing technology, could use the database information to target and harm consumers.

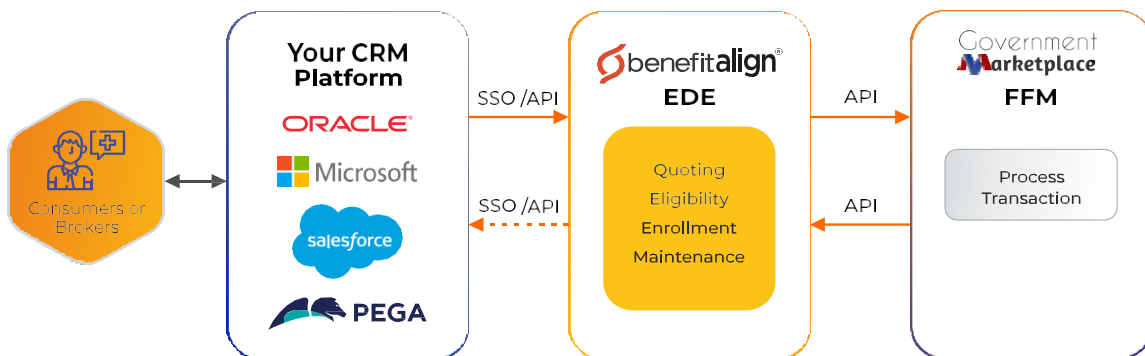
65. CMS released detailed guidance for entities wishing to implement the EDE pathway. These guidelines noted that entities would be allowed to implement one of three phase options of the technology, each successive phase allowing the entity to directly enroll a greater

percentage of consumers. The highest and most stringent level, Phase 3, allows an entity to support all consumer applicants. Phase 3 requires the entity to sign a privacy and security agreement with CMS that contains important consumer protections. Among other things, these protections restrict how consumer PII can be created, collected, used and/or disclosed, and impose safeguards for safeguarding consumer PII.

66. TrueCoverage and Benefitalign are both Phase 3 EDE platforms (and both are owned and controlled by Speridian). Each publicly touts the heightened security and privacy safeguards that need to be implemented to achieve Phase 3 status. For example, Speridian’s website claims that Benefitalign has been audited by a third party for extensive security and privacy, is compliant with nearly 300 CMS security and privacy standards and has been reviewed, approved and audited by CMS.

67. Benefitalign is an *agent-facing* EDE platform, meaning that it is designed to be used by health insurance agents to enroll consumers in ACA health insurance plans on the Marketplace database:

### BENEFITALIGN EDE SOLUTION DATA INTERCHANGE WITH FFM MARKETPLACE



**B. The ACA Imposes Important Regulatory Requirements That Defendants Violated**

68. Before delving into the fraudulent advertisements, sales scripts, AOR Swaps and Twisting conducted by Defendants comprising the RICO Enterprise, it is important to describe the regulatory environment that Defendants exist in — and how they flouted its requirements and restrictions. Viewed within this context, Defendants’ actions directed toward consumers and agents becomes even clearer.

69. Defendants fall within three categories of entities described by the ACA regulations.

70. Enhance Health and TrueCoverage are each considered an “Agent or broker” because they are “licensed by the State as an agent, broker or insurance producer” pursuant to 45 CFR § 155.20.

71. Speridian, Benefitalign and TrueCoverage are each a “Web-broker” under 45 CFR § 155.20. A web-broker is an Exchange-registered individual or group of agents or brokers “that develops and hosts a non-Exchange website that interfaces with an Exchange to assist consumers with direct enrollment in QHPs offered through the Exchange . . . .”

72. And Minerva, Bowsky and Herman are considered “Non-Exchange entities,” defined under 45 CFR § 155.260 to include those who are not part of the Exchange but who obtain and use consumers’ PII. They are “any individual or entity that (i) Gains access to personally identifiable information submitted to an Exchange; or (ii) Collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.”

73. Because they are agents, brokers and/or web-brokers, ACA’s regulations place “standards of conduct” on Speridian, Benefitalign, Enhance Health, TrueCoverage and Bowsky.

Pursuant to 45 CFR § 155.220(j)(2), they must not deceive consumers. They must “[p]rovide consumers with correct information, without omission of material fact, regarding the Federally-facilitated Exchanges, QHPs (ACA health insurance plans) offered through the Federally-facilitated Exchanges, and insurance affordability programs, and refrain from marketing or conduct that is misleading (including by having a direct enrollment website that HHS determines could mislead a consumer into believing they are visiting *HealthCare.gov*), coercive, or discriminates based on race, color, national origin, disability, age, or sex.” (emphasis added).

74. Moreover, because they are each agents, brokers, web-brokers and/or non-Exchange entities, all Defendants must execute an agreement that includes provisions binding them to comply with ACA’s privacy and security standards and obligations and must also execute agreements with any downstream entities binding them to the same privacy and security standards. *See* 45 CFR §§ 155.220(j)(2)(iv), 155.260(b)(2).

75. As described in more detail in the sections below, Speridian, Enhance Health, TrueCoverage and Bowsky flouted the standards of conduct for agents, brokers and web-brokers outlined in 45 CFR § 155.220(j)(2). They purchased and/or financed the purchase of Leads that deceived consumers into thinking they would receive cash cards or other cash benefits. TrueCoverage, controlled and/or directed by Speridian, used misleading sales scripts to deflect questions about those cash benefits, and engaged in twisting and AOR-swapping that harmed consumers. Enhance Health did the same.

76. Moreover, because they are each agents, brokers, web-brokers and/or non-Exchange entities, all Defendants violated the regulations’ security standards and obligations. Enhance Health and Herman never entered into a security agreement with non-Exchange entity Minerva or Bowsky, and allowed them to record customer calls in breach of the security and

privacy regulations. Enhance Health was a downline agent of TrueCoverage and Speridian. Neither TrueCoverage nor Speridian caused Enhance Health to execute a security agreement.

**C. Defendants Engage in a RICO Enterprise**

**1. Changes in the ACA Create a Year-Round Market for Enrolling Low-Income Americans**

77. In the wake of COVID, the federal government took multiple steps to expand the availability of affordable ACA health plans to Americans. In 2021, the American Rescue Plan Act temporarily enhanced eligibility for, and the amount of, APTCs that consumers could use to offset the premiums for ACA health plans.

78. APTCs are tax credits paid by the federal government directly to the insurance carriers (not consumers) to offset the cost of premiums for the health insurance. Importantly, to qualify for premium tax credits, consumers must satisfy income requirements. Consumers can use APTCs to lower their monthly insurance payments when they enroll in a plan through the Marketplace. The consumer's APTC is based on the estimated annual household income and the household size that the consumer reports on their Marketplace application. The consumer's APTC is determined at the end of the year based on the actual household income and household size for the year. Depending on their actual household income for the year, consumers may be required to repay excess APTCs received when filing their federal income tax return.

79. Separately, in September 2021 the U.S. Department of Health & Human Services finalized a new special enrollment period (SEP) in states that use HealthCare.gov, granting year-round enrollment in ACA-compliant health insurance if an applicant's household income does not exceed 150% of the federal poverty level and if the applicant is eligible for an APTC (or subsidy) to cover the cost of the plan. This SEP started on March 22, 2022.

80. According to the U.S. Census Bureau, in 2022, approximately 40 million Americans below the age of 65 fall within this market segment of at or below 150% of the federal poverty level. As explained below, the year-round special enrollment period provided Defendants with the perfect opportunity to market and sell ACA plans to a market segment of low-income individuals that have may be in need for low-cost health insurance.

**2. In 2022, Enhance Health and TrueCoverage Enter the New, Year-Round Market for Enrolling Low-Income Consumers**

81. Using a \$150 million investment from Bain Capital, Enhance went into business in late 2021. Initially, Enhance Health planned to market and sell Medicare Advantage policies to seniors. But Enhance Health quickly redirected its focus to the low-income ACA market, seeking to capitalize on the year-long SEP that was set to begin on March 22, 2022.

82. Enhance Health and Herman determined that ACA health plans that stayed in force for at least two years were the most profitable for agents selling those plans. Furthermore, low-income policyholders were most likely to keep a policy in force for at least two years because they did not have to pay for premiums — those premiums were covered by the government’s APTCs. But Enhance Health and Herman understood that to obtain profitability in such a market, Enhance Health needed to enroll a high volume of consumers.

83. TrueCoverage spotted the opportunity at around the same time. TrueCoverage realized that by using Benefitalign’s readily available EDE platform, it could obtain complete access and control to Marketplace data and enroll large numbers of customers in a short amount of time without scrutiny — in other words, without having to enroll in the Healthcare.gov website.

84. Benefitalign was Speridian and TrueCoverage’s proprietary EDE platform. It was not openly available to other agencies. Yet Speridian, TrueCoverage and Benefitalign allowed Enhance Health, which had just received a \$150 million infusion of capital, to use the platform

and work together to capture the ACA market for low-income Americans. Using the Benefitalign platform, Enhance Health quickly became TrueCoverage’s largest downline agent. TrueCoverage trained Enhance Health’s agents for ACA-related sales calls.

85. To support the large scale of such an operation, TrueCoverage and Enhance Health opened call centers and staffed them with hundreds of insurance agents, mostly from South Florida. In addition, TrueCoverage and Enhance Health created downline networks of other agencies to enroll even more consumers.

86. TrueCoverage and Enhance Health knew that their downlines were using fraudulent ads and misleading scripts and engaging in AOR Swaps, Twisting and Dual-Apping. They shared in the commissions captured by their downlines.

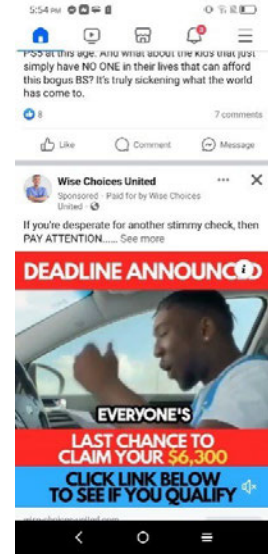
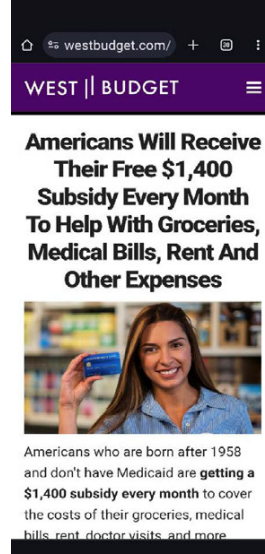
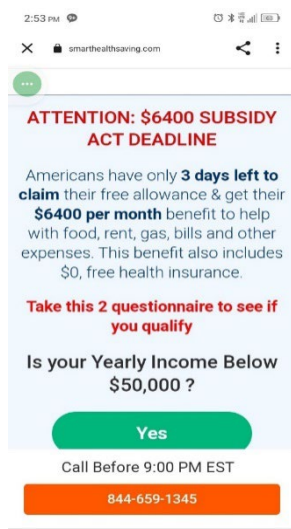
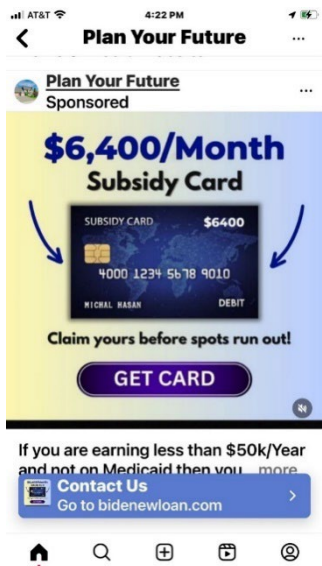
**3. To Drive Enrollments, Defendants Use False Advertisement Campaigns Targeting Low-Income Americans**

87. To drive enrollment, TrueCoverage, Enhance Health and their downlines purchased customer Leads. Enhance Health entered into an agreement to purchase Leads exclusively from Minerva. True Coverage and its other downlines purchased Leads from Minerva and other lead generators.

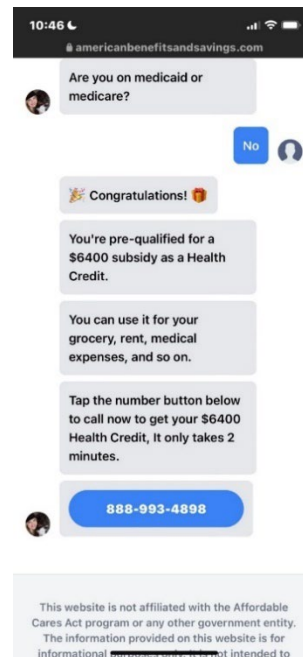
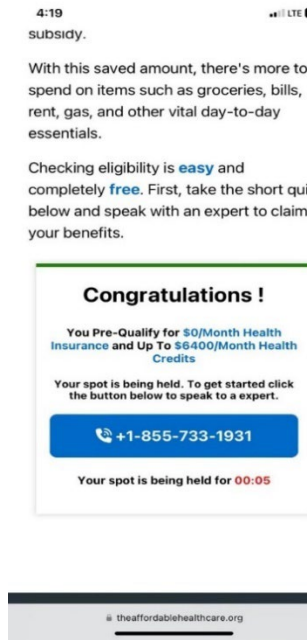
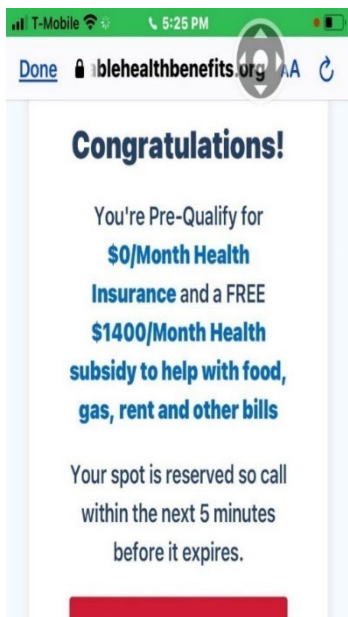
88. Minerva and the other lead generators generated their Leads by posting advertisements on social media like Facebook, and by sending text messages directly to consumers. Minerva both created its own advertisements to generate Leads and purchased Leads from other lead generators who created advertisements.

89. Beginning in 2022, Minerva and other lead generators began posting and texting advertisements that falsely represented that consumers could receive cash benefits, such as cash cards or stimulus checks (“stimmys”), to cover household expenses like groceries, medical bills and rent. Just a few examples of these advertisements include:





90. When customers click these advertisements or text messages, they are asked a couple of short questions, including whether the consumer earned less than a certain amount per year and whether they were on Medicaid. While these questions are made to appear to relate to the consumer’s qualifications for a cash benefit, these questions were actually posed to determine whether the consumer qualified for APTCs to pay for health insurance. If the consumer’s answers qualified him or her for APTCs, that consumer was brought to a landing page that told them they were “prequalified.” The landing pages continued to use language that misled consumers to believe they were applying for cash benefits that could be used for daily expenses:



91. The landing pages contained toll-free phone numbers for consumers to call. These phone numbers led to the sales agents of Enhance Health, TrueCoverage and/or their downlines. The calls were routed through Minerva’s routing software Retreaver, which also records the confidential sales calls without Consumer Class Plaintiffs’ and class members’ consent.

92. Enhance Health, TrueCoverage and their downlines knew that these Leads were being generated by misleading advertisements. The prequalified consumers who were calling them repeatedly asked about the nonexistent cash cards, cash subsidies and other cash benefits being touted in the ads. Rather than try to dispel the belief consumers had obtained from the ads and landing pages, Enhance Health, TrueCoverage and their downlines deflected consumers’ inquiries about the cash benefits to enroll them into a health insurance plan anyway.

93. For example, on December 13, 2023, TrueCoverage’s Senior Director of Quality Assurance, John Runkel, sent an email to TrueCoverage’s sales agents from his Speridian email address acknowledging that “[w]e are misquoting subsidies and additional benefits. . . . We have been quoting to consumers that they are going to receive a ‘subsidy card’ in the mail to help pay

*for groceries, bills, rent and expenses.*” (emphasis added). Runkel explained to TrueCoverage sales agents that the subsidies were not cash benefits. Rather, they were health insurance premium payments made directly from the government to the insurance carrier for the consumer’s benefit. Runkel also explained that while some carriers provided cash rewards (such as a gym membership or “\$10 Subway card”) for healthy activities, TrueCoverage had no authority to speak about additional benefits. Finally, Runkel told TrueCoverage’s sales agents that “[t]he only thing we can do is follow our script and be vague.” (emphasis added).

94. By referring to “our script,” Runkel meant a series of scripts that TrueCoverage used to quickly enroll consumers for ACA health insurance in less than 10 minutes. Again, volume was key.

95. TrueCoverage told its agents that failure to follow the scripts were grounds for termination.

96. TrueCoverage’s sales script was created to work seamlessly with the landing page from the misleading advertisement. It begins with a question that references the landing page: “Fantastic, and you saw that prequalified result that led you to us? Great!” From there, the script asks just a few more simple questions designed to verify the consumer’s qualifications for an ACA insurance plan: current healthcare coverage, name, date of birth, zip code, marital status, dependents and “anticipated” income.

97. If the consumer referenced the cash benefits he or she had seen in the advertisement and landing page, TrueCoverage provided its agents with another script — a rebuttal script — to guide them. The rebuttal script instructed the sales agent to quickly deflect the consumer’s question about a cash card. For example:

## Online Ad Rebuttals

### REBUTTALS TO CASH CARDS AND \$\$ QUESTION

#### They say—I am calling about the cash card?

**Rebuttal:** Yes, you may qualify for additional benefits with eligible plans. Let us start the qualification process to find the plan that fits your needs, what is your zip code?

98. Runkel’s email caused a stir among TrueCoverage’s salespeople, some of whom were worried that they may be misleading consumers, and that they may not be paid commissions on their sales. TrueCoverage’s Regional Director in its Deerfield Beach sales office, Gabriel Harrison, tried to reassure his agents:

That email was mainly directed to Other centers not ours, we are the **TOP PRODUCERS** , if you are putting in your numbers then losing 1 sale or even 3 by the end of the week is not going to Affect you!! Get with the Picture guys , everything is great and you all have been paid very well , plus we feed you, plus we give you Bonus for just doing your job , we give out cash spiffs to push you to hit numbers for your own Gain, we give out Prizes for those of you who Put in that extra work to be successful , Guys we pay out Huge checks and everyone knows it, why would we as a company Harm your pay ? We are here to Help you all Become Fat and Happy With a Wheel Borrow full of **CASH!**

Guys don't get stuck in your head, lets push forward and continue the success we have started and make next year an awesome year with a Big book of Business!

99. One former TrueCoverage agent said the company trained its agents to lie to consumers and not disclose the truth about the nature of the subsidy. Another explained that TrueCoverage’s supervisors attempted to justify the company’s actions by reminding sales agents that even though consumers were not getting a cash card or other cash benefit, they were at least getting health insurance.

100. In a January 11, 2024, email, Goldfuss instructed agents not to speak with any government agent or CMS: “If you receive an email from CMS or a Department of Insurance from any particular state, **DO NOT RESPOND!**”

101. Enhance Health also incorporated sales scripts with aimed to deflect consumers' attention away from the advertised cash subsidies and benefits, and quickly sign them up.

102. Despite knowing that Minerva and other lead generators were generating the advertisements and Leads that were misleading consumers, TrueCoverage, Enhance Health and their downlines continued to pay Minerva and other lead generators millions of dollars for those Leads. As they did, the scheme's reach expanded.

103. Indeed, in a recent, March 29, 2024, article entitled "Enhance Health: Helping Hundreds of Thousands of Americans Find Health Insurance Coverage Every Year," Herman proclaimed that "Enhance Health is the largest enroller of ACA plans in the country — we help hundreds of thousands of Americans find health insurance coverage every year." Herman also noted that nearly all of Enhance Health's clients are low-income Americans, stating "97% of our members pay \$0 a month in insurance premiums while obtaining the coverage they need."

104. Minerva also knew what was going on. It generated some of the Leads itself. For example, when an unrelated agency purchased some of Minerva's Leads and began receiving calls from consumers, that agency quickly realized that those consumers were calling for cash benefits, not health insurance. The agency complained to Minerva's marketing director, who replied in a text that the calls had a healthy success rate, and that the agency should enroll them anyway. He wrote "the calls you're getting are *internally generated* and have a raw to sale rate of about 34%. [W]e'll audit the calls of course, *but agents are usually able to flip these consumers pretty easily and get them on a no cost plan.*" (emphasis added). (The reference to auditing the calls confirms that Minerva was recording consumer calls in violation of ACA regulatory security and privacy policies).

105. As for Class Plaintiffs and class members, they justifiably relied on the advertisements and the statements and omissions made in the scripts. The misleading nature of the advertisements and scripts caused them to enroll and/or provide their PII.

**4. Defendants Engage in Twisting, AOR Swaps and Dual Apps**

106. Even if Class Plaintiffs and class members decided not to enroll, by luring consumers to call in, Defendants received information that allowed defendants to further increase commissions, to the detriment of the Consumer Class and Agent Class.

107. Enhance Health, TrueCoverage and their downline agents engaged in AOR-Swaps to steal other agents' commissions. Using the Benefitalign platform and consumers' names, dates of birth and zip code, they were able change consumers' Agent of Record within the Marketplace database without the consumer's knowledge or consent. In doing so, they captured the monthly commissions of agents like NavaQuote and Broyer who had originally worked with the consumers directly to sign them up. One former agent of TrueCoverage downline ProtectHealth said she was made to do more than 500 AOR Swaps and was instructed to reenroll policies without contacting the consumer.

108. Enhance Health, TrueCoverage and their downline agents also engaged in Twisting. One step beyond an AOR swap, they used the Benefitalign platform and consumers' names, dates of birth and zip code to change a consumer's actual health plan without the consumer's knowledge or consent; for example, by changing the consumer to a new insurance carrier or a different plan within the same carrier. This also allowed Enhance Health, TrueCoverage and their downline agents to capture the monthly commissions of agents like NavaQuote and Broyer.

109. On February 26, 2024, CMS published a notice acknowledging the problem. The first three bullet points outlined the issue:

- CMS has identified instances of consumers being enrolled into an unwanted plan.
- This action, referred to as an Unauthorized Plan Switch (UPS), results in the consumer’s desired policy being cancelled or terminated.
- Many consumers are unaware of the switch until they attempt to use the desired policy to see a doctor or fill a prescription and are denied.

110. Enhance Health, TrueCoverage and their downline agents also engaged in the creation of dual applications, or a “Dual-App.” In this scenario, they would leave a consumer’s original plan in place, but submit a new application — a dual policy — for that consumer without the consumer’s knowledge or consent. This created a new policy and a new commission. Sometimes, this Dual-Apping was achieved by splitting up a family plan; for example, by submitting an application and creating a separate policy for a husband, leaving the wife and children on the original plan.

111. These schemes hurt consumers in multiple ways. Some consumers were signed up into twisted or dual plans that they do not qualify for. The APTCs they received, sometimes unknowingly, caused a tax penalty at the end of the year. Some were put into plans that their doctors are not a part of. Or the new plans had higher deductibles or copays.

112. Agents are damaged by AOR swaps and twisting because they lose their commissions.

##### **5. Thousands of Consumers Have Complained About the Scheme**

113. TrueCoverage’s online reviews contain numerous testimonials from consumers describing their experience with the schemes:



I received this insurance through a \$6,400 subsidy that was offered. I received an insurance with 0 deductible but my doctor or therapist does not accept that insurance.

-Maria

I think that you shouldn't act like people are getting money to get people to get coverage through your agency. Also shouldn't tell people you're on health.gov because I found nothing on health.gov about truecoverage.

-Sarah L.

On November 30th I called and signed up for the \$6,400 subsidy. THEIR WEBSITE said it was to help pay for gas, bills, utilities. I even asked the lady and texted her and she said YES, ITS TO PAY FOR ANYTHING. I was told it would be in 30 days. 30 days later I call back (she would never respond to text when I asked about it) and the guy said that she forgot to finish last step and that it (\$6,400)would be in in \*\*\*\*\* days but they'd make sure it was sent in next week. Never received it. All a huge scam.

-Shane K

On November 30th 2023, I was calling for the stimulus package the government was offering, and the number I was provided sent me to this company. I was told by \*\*\*\*\* that I was going to be getting a stimulus package of \$1730.54 monthly to cover gas, groceries, and bills. I was also getting a medical coverage from \*\*\*\*\* effective Jan. 1 2024 with a \$0 premium. I was told that this was from the Stimulus program to help the middle class stuck in the middle financially and medically, and we took the offer and I had to provide the SSN for my ENTIRE family to be Automatically qualified. I told her my children already had medical coverage from \*\*\*\*\* and she said it was fine. We signed up due to the prior knowledge presented to us, and after a few days I became skeptical and reached out to \*\*\*\*\* on December 11th 2023 to clarify what we were getting and the call was automatically sent to voice-mail. I called the business number and was told that the information presented to us was NOT accurate, and I immediately went to cancel my policy. My concern is my family's personal information (SSN most importantly) is in their system and im worried for potential fraud due to already being misled and lied to.

-“Initial Complaint” 12/11/23

This company is advertising \$6400 for individual that need assistance with health coverage. Once I reached out they tried to sell



me a low cost health coverage. I am complaining because they are using foul advertising practices. I'm sure this is just the tip of the iceberg. Stop them now!!!

-Initial Complaint 10/30/23

Falsely advertising a savings benefit card that you can use to purchase groceries or pay rent get gas. However I never received it and the agent has not responded to any of my calls or messages. I specifically signed up for this for this card only

-Initial Complaint 9/26/23

114. Other putative class members had similar experiences with Enhance Health:

They say you qualify for 0 copay and 0 on prescriptions, but they also said that you qualified for the benefit card to help pay groceries, rent, and Bill's. But only sign you up for the insurance. Then when you call they say that you need to check your perks and rewards and find out that they only give surveys for 25to50 dollars prepaid visa. That you have to wait 5to10 days to receive. Now I don't know about you but I don't know any person that food bills rent comes to 50 dollars. They told all those lies to get you to sign up for insurance. Now I want to know what else they hiding. I will find out stay posted

-Robbie Torres Rivera

Never received anything but spam calls. You are only giving your info to be sold off. Please don't call these scammers don't give ur info. You are not getting any subsidy card or health insurance at all.

-Philemon Blevins

So I signed up because it offer up me a \$550 subsidy that I would get each month to put towards food groceries and other thing so I received the insurance card but not the subsidy card so when I call to check on it I was informed that the \$550 goes towards the cost of your insurance plan and you will not receive a subsidy to do as you would like... it's all a scam and is not explained to u in detail.. so don't sign up thinking you will get a subsidy card to do as you please because you won't... you have to earn rewards to get any cash benefits.. I will keep the insurance because it's affordable but this is so misleading

-Wyshieka Thompson

This place steals your information, cancels your current healthcare plan then enrolls you in a plan without your consent or knowledge.

I have heard many people have the same issue with someone stealing their information and being signed up for terrible healthcare plans and they have all ended with Enhance Health. When I attempted to call the company and find out how they got my information I was transferred multiple times and laughed at.

-Nicole

I got a plan thru AmBetter. But what was misleading was that I was told by an Enhance Health service representative, as well as the advertising, that I will be receiving money on a card to spend on healthy groceries. This is a lie. Why they tell people that, I dunno, it's just a stupid tax credit. That's not gonna help me, I make \$9,000 a year and pay no taxes and get nothing back. I got patched thru to AmBetter after giving a ear full to the Enhance Health representative, they were not so nice that time, and he just wanted to get rid of me. After giving another ear full to the AmBetter representative, she apologized profusely and said she deals with about 15 to 20 calls everyday with people like me. Well, duh, you people are misrepresenting what your offering. I reported it to the FCC and the Fraud Government website. It's ridiculous, they use YouTube and Facebook and put all these pictures of groceries and even the representative when I signed up said that. Very scummy and scammy. I don't appreciate being lied to, I was actually in need of healthy food cause I am poor, thanks for getting my hopes up and crushing them. That's very uncool. Screw you people. Look at the corporate double speak with the reply they gave me. I would NEVER call you people ever again. If I need anything at all, I will call AmBetter, my actual insurance provider. Your just a broker agent and signed me up. Now go away and go lie to someone else. We the people are sick of scumbags like you that pray on the hopes and mislead people. Your words mean nothing to me, just more lies.

-“Account Removed”

Ad said I would get amazing health plan and \$540/m card for expenses for things like groceries but after signing up I was given a bottom of the barrel (bronze with 10k deductable, literally worst plan I've ever seen) and no expense card. I am considering suing.

-Justin McPharison

Not sure if I got the right information, I got connected to them through and add that featured Oprah, and it stated that they were giving \$1,300.00 cash per month for signing up. All a scam. No one can answer my question, insurance company says it was a scam.

-Carlos Marin

Gave me HIGH deductibles, and no mention of the \$1000+ government check that I should qualify for (according to ad - that draws you in). So.. I believe I've been scammed!

-LauraT

My complaint is that what was advertised to me and spoken to me over the phone during my conversation was filled with lies and deceptive information. I was told that I would be getting \$402 each month to be used however I wanted to use it. On anything I wanted to use it on, like bills, food, gas, clothes... But after getting my paperwork in the mail and reading it, it clearly states that the \$402 can only be used towards the cost of the insurance they set up for me. For co-pays and visits. Nothing else can it be used for. I was lied to and misled the whole conversation. I would of never ever had them set this up if I would of known this and now I have to come out of my pocket and switch my insurance and pay for premiums again. Thanks for a whole lot of wasted time and \*\*\*\*\* that I really can't afford to spend.

-“Initial Complaint” 7/23/23

I signed up with healthcare coverage through a licensed agent. That same day my information was stolen and I was registered in a different plan without my authorization or knowledge. The date of the incident is November 7th, 2023. The insurance company is Enhance Health, the agent attached to the policy is \*\*\*\*\* and his license number is \*\*\*\*\*

-“Initial Complaint” 11/28/23

This company is able to change and cancel insurance on the marketplace without the owners permission. My insurance was canceled unsuspectedly and when I called to find out why I was told that this company had put me down on their insurance and canceled my marketplace insurance when I did not ask them to. I called this company three times to find out how they were able to cancel my insurance and they hung up on me all three times.

-“Initial Complaint” 11/03/23

I have never heard of this company before today. An insurance agent by the name of \*\*\*\*\* Madame \*\*\*\* (NPN \*\*\*\*\* ) affiliated with this company somehow got a hold of my personal information and submitted a health insurance application without my knowledge or consent. \*\*\*\*\* Madame \*\*\*\* then proceeded to enroll me into a BlueCross BlueShield plan, again without my knowledge or consent. I have no idea who this insurance agent is or how they obtained my information. I received notice from Healthcare.gov that an application was submitted, after which I received an email from Enhance Health with a reference number and this agent's name stating my eligibility verification was completed. I don't know if this Company is in the business of submitting fraudulent insurance applications or if this agent acted independently. A complaint has been filed with the state \*\*\*\*\* of \*\*\*\*\*

-“Initial Complaint” 9/11/23

Healthcare coverage got changed without consent!

-“Initial Complaint” 8/16/23

**D. Victims Included the Class Plaintiffs**

115. The scheme described above was applied to Class Plaintiffs, including consumers and agents.

**1. The Consumer Class Plaintiffs**

116. Conswallo Turner. Turner is 52 years old and lives in Orange, Texas, with her son, Joshua Janice. In late 2023, she started looking for health insurance. With the help of Callie Navrides at NavaQuote, on December 9, 2023, Turner applied for a UnitedHealthcare Gold plan through the Healthcare marketplace. The application was approved and the policy was set to go into effect on January 1, 2024.

117. Shortly thereafter, Turner saw a Facebook ad promising a monthly cash card to pay household expenses. She called the number on the ad and provided her name, date of birth and state of residence. Armed with this information, agents switched Turner’s plan and her AOR no less than five times in a span of weeks in December 2023 without her knowledge and consent.

This included agent Daniel Pojoga of Enhance Health, who without Turner's knowledge and consent switched Turner to a Blue Advantage Gold HMO in December 2023 that did not include Turner's son, Joshua.

118. As a result of these actions, Turner has been damaged including but not limited to the loss of coverage and resulting medical payments for her son Joshua and higher deductibles and co-pays than the policy sold to her by NavaQuote. In addition, Plaintiff suffered damages resulting from the time and expense she has spent trying to correct the problems caused by the unlawful conduct.

119. Tiesha Foreman. Foreman is 50 years old and lives in Douglasville, Georgia.

120. In or around December 9, 2022, Mrs. Foreman's husband, Larry Foreman, responded to an online ad stating that he prequalified for a cash card. He spoke with a TrueCoverage agent who enrolled him (but not Mrs. Foreman or their child) into an Oscar Health Plan. Upon information and belief, the agent led Mr. Foreman to believe that he would receive a cash card and \$0 health insurance by falsely mischaracterizing that the advanced premium tax credit ("APTC"), which is paid by the government to the insurance carrier, would be paid to Mr. Foreman in the form of a cash card.

121. To qualify Mr. Foreman for the tax credit, TrueCoverage underreported the family's household income. Specifically, TrueCoverage did not include Tiesha Foreman's income in the household income calculation. Mrs. Foreman is an accountant that makes approximately \$95,000 per year, an income amount that disqualified her and her family from receiving the APTC.

122. The following year, the Foremans received a 1095-A showing that that the Oscar policy was only in effect from January 1, 2023, to January 31, 2023 (one month), and that the Foremans owed the IRS approximately \$871 for the APTC that it paid to Oscar Health.

123. On or about February 13, 2023, TrueCoverage agent Marius Boncea re-enrolled Mr. Foreman (but not his wife or child) into a second health insurance policy issued by Cigna HealthCare of Georgia. Mr. Foreman does not recall ever agreeing to enroll into this policy. Once again, TrueCoverage underreported the Foremans' household income to qualify Mr. Foreman for the APTC, even though the Foremans' household income was too high to qualify for the subsidy.

124. The following year, the Foremans received a 1095-A showing that that the Cigna Health of Georgia plan was only in effect from March 1, 2023, to April 30, 2023 (two months), and that the Foremans owed the IRS approximately \$1,741.76 for the APTC that it paid to Cigna.

125. In April 2023, Mrs. Foreman was unaware that her husband had responded to the online ad and had been enrolled in multiple policies in the months prior. At that time, the Foremans' oldest son was removed as a dependent on their income taxes, which qualified as the event that allowed the Foremans to enroll in an ACA plan outside the standard open enrollment period. As a result, Mrs. Foreman enrolled in and purchased an Oscar health plan for her and her family directly through the Marketplace to provide health insurance coverage for the remainder of 2023.

126. On or around October 17, 2023, TrueCoverage agent Hans Mardy enrolled Mrs. Foreman into a Cigna plan without her knowledge and consent. The following year, the Foremans received a 1095-A showing that that the Cigna Health of Georgia plan was only in effect from November 1, 2023, to November 30, 2023 (one month), and that the Foremans owed the IRS approximately \$1,793.32 for the APTC that it paid to Cigna.

127. On or about October 26, 2023, Mr. Foreman was switched into an Ambetter health by another agent, Gabriel Pasztor, an agent affiliated with TrueCoverage.

128. A couple of weeks later, on November 4, 2023, another agent believed to be

affiliated with TrueCoverage, Christopher Morales, submitted another application without the Foremans' knowledge or consent.

129. In December 2023, during the Open Enrollment Period, Mrs. Foreman enrolled in and purchased an Oscar health plan for her and her family directly through the Marketplace, to provide health insurance coverage for 2024, effective January 1, 2024.

130. On January 22, 2024, Foreman learned that the Oscar coverage that she purchased in December 2023 had been cancelled. She called the Marketplace and learned that without her knowledge or consent, Pasztor submitted a health insurance application on her behalf.

131. In addition, on or about February 22, 2024, Enhance Health enrolled Mr. Foreman into an Ambetter health insurance plan without his knowledge and consent.

132. As a result of this switching of plans, the Foremans were left without health insurance for the months of January and February 2024 and incurred uncovered medical expenses.

133. At this point, Mrs. Foreman sought help from Callie Navrides and NavaQuote. Navrides and Mrs. Foreman spent a significant amount of time unwinding the problem through the Marketplace. Ultimately, Mrs. Foreman was able to obtain a new health insurance plan that was effective April 1, 2024, but is still trying to re-instate the Oscar policy that she purchased during the last Open Enrollment Period, so that her medical expenses incurred during the first three months of the year are covered.

134. As a result of these actions, Mrs. Foreman suffered significant damages, including tax damages, loss of benefits, unpaid medical expenses and uncovered medications. Mrs. Foreman has also suffered damage by having to expend unnecessary time fixing these problems.

135. Angelina Wells. Wells is 53 years old and a resident of Texas. On or around November 14, 2023, she saw a Facebook ad stating that she could receive a \$6,400 cash card and

free insurance. She clicked the ad and answered some basic questions that told her she was “preapproved” and provided a phone number to call. Wells believes that she spoke with an agent named Christian Jerome, whom, upon information and belief, works with TrueCoverage or one of its downline agencies. Jerome obtained Wells’ name, date of birth, income and state of residence. According to Healthsherpa’s database, Jerome signed her up for an Ambetter Standard Silver plan. Wells asked Jerome about the cash card, and Jerome told her it would come later. Wells never received the cash card she was promised.

136. In or around January 22, 2024, Wells contacted NavaQuote and expressed concern to Callie Navrides that she had been enrolled in health insurance policies that did not meet her needs without her consent.

137. Specifically, Wells stated at that she learned that she had a United Healthcare plan but that the plan did not meet her needs. Wells stated that she did not recall enrolling into the health plan at all.

138. In response, Navrides researched the issue on Healthsherpa and learned that Wells had been switched at least three times to different policies between November 2023 and January 22, 2024.

139. Specifically, Navrides learned that Wells was switched into a Cigna Bronze plan by TrueCoverage agent Maurice Thrower, and then switched again into a United Healthcare plan by Pasztor.

140. In an effort to help Wells and get her enrolled into a policy that met her needs, on or about January 22, 2024, Navrides enrolled Wells into a Cigna Connect Gold Enhanced Diabetes Care plan, which would ensure that Wells’ diabetes treatment and medication(s) would be covered in an affordable way.



141. Four days later, on January 26, 2024, TrueCoverage removed Navrides as AOR and replaced her with one of its downline agents, Francisco Umana, and then enrolled Wells into an Ambetter Everyday Gold plan. TrueCoverage did so without Wells' knowledge or consent. The change caused Wells' Cigna Connect Gold Enhanced Diabetes Care plan to be canceled.

142. On February 22, 2024, Wells received an unsolicited text message from TrueCoverage thanking her for enrolling into another Cigna health plan. Wells does not recall consenting to enroll in another Cigna plan other than the one sold to her by Navrides.

143. On March 18, 2024, Wells contacted Navrides and expressed concern that the pharmacy told her that her Cigna plan sold by Navrides had been cancelled and that her diabetes medication had a \$50 copay.

144. After learning about these issues, Navrides and Wells spent a significant amount of time unwinding the problem through the Marketplace. Ultimately, they were able to reinstate the Cigna Connect Gold Enhanced Diabetes Care plan originally sold by Callie Navrides.

145. As a result of these actions, which included using false advertising to induce Wells to provide her personal information and then later using that information to "twist" Wells' policy, Wells has been damaged. Setting aside the fact that she did not receive the promised cash card, Wells suffered significant damages including loss of benefits and medication. Wells also suffered damage by having to expend unnecessary time fixing these problems.

146. Veronica King. King is 53 years old and lives in Warner Robins, Georgia. Since 2011, King has used agent Marsha Broyer of WINN Insurance to help her navigate and purchase health insurance.

147. On or about November 30, 2023, Broyer consulted with King and enrolled her into a health plan that met her needs.

148. In a three-month period from November 30, 2023, to February 25, 2024, at least eight other agents switched themselves as AOR on King's health plan and changed when they did so without King's knowledge or consent, including at least two Enhance Health agents.

149. On November 30, 2023, which is the same day that Broyer enrolled King into her policy, agent Christian Crevoisier with Ensure Health Group, a downline of TrueCoverage, canceled the original policy and enrolled King into another health plan.

150. On or about December 19, 2023, Broyer discovered that the plan had been switched and she reenrolled King back into the original health plan.

151. On December 22, 2023, Enhance Health agent Anpherny Simpson accessed King's account and became King's AOR without her consent. And on February 25, 2024, Enhance Health agent Ryan Rossien became King's AOR without her consent.

152. As a result of these twisting actions, King has been damaged including loss of continuity of care resulting from the agent of record and enrollment into additional health plans, and out-of-pocket costs spent attempting to deal with the issues created.

## **2. The Agent Class Plaintiffs**

153. NavaQuote LLC. NavaQuote LLC is a small, family-owned and -operated insurance agency based in Augusta, Georgia. NavaQuote was founded by the husband-and-wife team of Peter and Callie Navrides. It specializes in health, life and Medicare insurance products. Callie Navrides serves as the company's principal agent. Peter Navrides leverages his background in software, marketing and technology to help grow the agency.

154. NavaQuote takes pride in seeking to develop long-term relationships with its clients through trust and open communication. To accomplish this, the Navarides commit themselves to the highest ethical standards and to providing expert guidance to help clients make informed

insurance decisions.

155. NavaQuote expends significant resources to market its services online and maintain an online presence, including its website. The agency's revenue, and by extension its profits, relies on the generation of commissions from the sale of ACA health plans. When NavaQuote sells an insurance policy through the Marketplace, Callie Navrides becomes listed as AOR and NavaQuote receives a monthly sales commission.

156. Since the agency opened in October 2023, NavaQuote sold approximately 50 health plans to consumer, but lost 23 to the AOR Swaps. Through continued and laborious researching, as well as frequent communication with their clients, the Navrides have determined that other agencies are removing Callie Navrides as AOR without the consent or knowledge of either NavaQuote or its clients. In most instances, these agents are changing the clients' health care plans and information within the Marketplace system. By replacing Navrides as AOR, those agents are essentially stealing or poaching NavaQuote's clients — and its commissions.

157. Each time a client is poached, Callie Navrides must spend significant time to reestablish her position as AOR. She spends time each day checking her clients' statuses to see if she has been removed as AOR, because formal notices of removal do not reach her until the end of the month. When she discovers a client has been switched, she must call that client to try and explain what happened. She must then call Healthcare.gov, often waiting on queue for long periods of time, to report that she was removed as AOR without her client's knowledge or consent. The client is then brought into the call for Healthcare.gov to confirm that the client agrees to the reestablishment of Navrides' status as AOR.

158. Through its investigation, which has been difficult, laborious and costly — not only in terms of lost time that could have been used to help more clients and generate more

commissions, but also out-of-pocket costs expended through these efforts — NavaQuote has determined that TrueCoverage and Enhance Health agents are among the biggest offenders.

159. As just a few examples, Enhance Health agent Daniel Pojoga poached NavaQuote client Conswallo Turner. TrueCoverage agents including Christian Jerome, Francisco Umana and Maurice Thrower attempted to poach Angelina Wells from NavaQuote.

160. The actions of TrueCoverage and Enhance Health have damaged NavaQuote through a loss of commissions. It may take weeks for Healthcare.gov to reinstate Callie Navrides as agent of record. If the calendar rolls into a new month during that period, she does not receive that month's commission. It goes to the poacher. NavaQuote has also been damaged through loss of profits and out-of-pocket costs relating to the time spent to investigate and address the problem, and for extra expenses associated with buying additional Leads to replace lost clients.

161. Because of TrueCoverage and Enhance Health's actions, NavaQuote intends to pivot away from sales of health insurance plans in the Marketplace.

162. WINN Insurance Agency. Marsha Broyer, who is licensed to sell insurance in 13 states, owns WINN Insurance Agency LLC. Broyer's mission is to do what is right for her clients by providing the best service and the best health insurance products. Broyer was one of only a handful of the thousands of licensed health insurance agents in the U.S. to be invited to participate in the 2023 CMS Agent and Broker Summit and provide feedback to the government.

163. Broyer experienced first-hand the importance of comprehensive medical insurance. In 2003, Broyer lost sight in her right eye. Doctors discovered a brain tumor. Fortunately, the tumor was treated with gamma knife technology and Broyer regained her eyesight. But because she had inadequate insurance, Broyer was left with tens of thousands of dollars in medical bills and had no choice but to file for bankruptcy. This experience informs every interaction she has

with her clients and potential clients.

164. With the help of a \$94,000 SBA loan, Broyer started WINN in October 2021. Working seven days a week, within a year she had developed 350 customers, largely through client referrals.

165. WINN expends significant resources to market its services, including the creation and maintenance of a website and the purchase of exclusive Leads, which cost \$100 each. The agency's revenue, and by extension its profits, relies on the generation of commissions from the sale of insurance policies. When WINN sells an insurance policy through the Marketplace, Broyer becomes listed as AOR and receives a monthly sales commission of approximately \$30 per month per member for each application. So if a family of four is on a single application, WINN receives \$1,440/year for that policy ( $\$30 \times 4 = \$120$  for 12 months).

166. Since the beginning of 2023, Broyer has been removed as AOR in at least 81 of her clients' policies and replaced by agents that have no relationship to her. More than 20 of those clients have been lost for good. Through continued and laborious researching, as well as frequent communication with their clients, Broyer has determined that other agencies are removing her as AOR without consent. In most instances, these agents are changing the clients' health care plans and information within the Marketplace system. By replacing Broyer as AOR, those agents are essentially stealing or poaching WINN's clients — and its commissions.

167. Through Broyer's investigation, which has been difficult, laborious and costly — not only in terms of lost time that could have been used to help more clients and generate more commissions, but also out-of-pocket costs expended through these efforts — WINN has determined that TrueCoverage and Enhance Health's agents are among the biggest offenders.

168. For example, Enhance Health agent Ryan Rossien poached WINN client Veronica

King and Paula Langley. And TrueCoverage agents and/or downline agents Gabriel Pasztor, Paola Fritz and Christian Jerome poached client Paula Langley.

169. Each time a client is poached, Broyer is forced to spend significant time to reestablish her position as AOR. She spends time each day checking her clients' statuses to see if she has been removed as AOR, because formal notices of removal do not reach her until the end of the month. When she discovers a client has been switched, she must call that client to try and explain what happened. She must then call Healthcare.gov, often waiting on queue for long periods of time, to report that she was removed as AOR without her client's knowledge or consent. The client is then brought into the call for Healthcare.gov to confirm that the client agrees to the reestablishment of Broyer's status as AOR.

170. And then, in all likelihood, Broyer must repeat this process all over again, because the switching occurs over and over. One of WINN's clients, Langley, who is a 59-year-old with a pacemaker and a heart condition, has been switched no less than 20 times since February 2023.

171. In all, Broyer estimates that she spends about 1/3 of her time dealing with this scheme.

172. The actions of TrueCoverage and Enhance Health have damaged WINN through a loss of commissions. It may take weeks for Healthcare.gov to reinstate Broyer as AOR. If the calendar rolls into a new month during that period, WINN does not receive that month's commission. It goes to the poaching agent. WINN has also been damaged through loss of profits and out-of-pocket costs relating to the time spent to investigate and address the problem, and for extra expenses associated with buying additional Leads to replace lost clients.

173. Because of TrueCoverage and Enhance Health's actions, WINN has lost a sizeable percentage of its income, giving Broyer no choice but to take a second job as an agent for a wireless

phone company.

## V. RICO ALLEGATIONS

174. TrueCoverage, Enhance Health, Speridian, Minerva, their officers and employees, including but not limited to Herman, Bowsky, Panicker and Goldfuss; as well as independent contractors; agents including Protect Health, Ensure Health Group, Health First Insurance Agency, My Health Advisers, Inc.; third-party subagents; lead generators such as PolicyBind, WeCall Media and My ACA; EDE Platforms like Benefitalign, JET Health and Inshura; and the John Doe Entities operated, managed, directed and/or conspired with an associated-in-fact enterprise (the “Enterprise”).

175. The Enterprise generated false advertisements to lure low-income consumers to enroll in ACA healthcare plans and provide PII, and to capture commissions through the use of AOR-Swaps, Twisting and Dual-App tactics. The purpose was to maximize revenues and capture a larger share of the ACA health insurance market for low-income Americans.

176. The Enterprise used the wires and mails to perpetrate the fraud. TrueCoverage, Enhance Health and their downline agents used standardized scripts to make misrepresentations and omissions to Class Plaintiffs and class members over the phone. They used email or mail to send confirmatory documentation. They used the internet and phone lines to enroll customers, misuse PII and capture commissions.

177. TrueCoverage and Enhance Health monitored sales calls. Their downlines monitored sales calls without entering into any CMS-approved security or privacy agreement required by ACA regulations. Minerva also monitored sales calls without any of the required CMS approval.

178. Throughout its existence, the Enterprise engaged in, and its activities affected,

interstate commerce. The Enterprise involved commercial activities across state lines, including marketing campaigns, phone and internet solicitations and the solicitation and receipt of money and PII from Class Plaintiffs and class members across the country.

179. TrueCoverage, Enhance Health and Herman participated in the operation and management of the Enterprise's affairs, through among other methods and means, the following:

- a. Developing agencies designed to enroll Class Plaintiffs and class members into ACA healthcare plans;
- b. Recruiting agents;
- c. Developing the third-party distribution channels that ran through their downlines;
- d. Financing the operations of downline agencies through the use of advanced commissions and/or prepaid commissions called "heap deals";
- e. Training each other's sales agents and the sales agents of downline agencies;
- f. Monitoring sales agents, including but not limited to monitoring sales calls;
- g. Accounting for, auditing and distributing commissions;
- h. Dealing with and providing customer service to Class Plaintiffs and class members;
- i. Allowing and coordinating agents to register for licenses;
- j. Reviewing and approving the scripts; and
- k. Purchasing Leads.

180. Minerva and Bowsky participated in the operation and management of the Enterprise's affairs, through among other methods and means, the following:

- a. Developing fraudulent ads;



- b. Creating, buying and selling Leads to Enhance Health, True Coverage and their downlines;
- c. Recording customers' conversations with health insurance agents without their knowledge or consent; and
- d. Tagging, tracking and routing callers to agents.

181. Speridian participated in the operation and management of the Enterprise's affairs, through among other methods and means, entering into employment agreements with TrueCoverage agents and paying them a salary, financing the sales operations of TrueCoverage and Benefitalign, and developing the platform used by TrueCoverage, Enhance Health and their downlines to enroll customers, misuse PII and capture commissions.

182. Enhance Health further participated in the operation and management of the Enterprise's affairs, through among other methods and means, purchasing the platform that Enhance Health and its downlines used after June 2023 to enroll customers, misuse PII and capture commissions.

183. Herman participated in the management and operation of the Enterprise's sales, compliance, training and administrative functions.

184. Defendants were knowing and willing participants in the Enterprise and its scheme, and reaped revenues and/or profits therefrom.

185. Speridian, TrueCoverage, Enhance Health and Minerva each has an ascertainable structure separate and apart from the pattern of racketeering activity in which they engaged. The Enterprise is separate and distinct from Speridian, TrueCoverage, Enhance Health, Minerva, Herman and Bowsky.

186. Speridian, TrueCoverage, Enhance Health, Minerva, Herman and Bowsky, who are

persons associated-in-fact with the Enterprise, knowingly, willfully and unlawfully conducted or participated, directly or indirectly, in the affairs of the Enterprise through a pattern of racketeering activity within the meaning of 18 U.S.C. §§ 1961(1), (5) and 1962(c). The racketeering activity was made possible by the regular and repeated use of the facilities, services, distribution channels and agents of the Enterprise.

187. Defendants committed multiple racketeering acts, including aiding and abetting such acts. The racketeering acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims and methods of commission. Further, the racketeering acts were continuous, occurring on a regular (daily) basis throughout a time period beginning in 2022 through the present.

188. Defendants' predicate racketeering acts within the meaning of 18 U.S.C. § 1961(1) include, but are not limited to:

- a. Wire Fraud. All Defendants violated 18 U.S.C. § 1343 by transmitting or receiving, or causing to be transmitted or received, materials by wire and/or email for the purpose of executing the scheme, which used material misrepresentations and omissions to induce consumers, including Consumer Class Plaintiffs and class members, to enroll customers, misuse PII and capture commissions. The materials that Defendants sent or caused to be sent include but were not limited to social media advertisements, text messages and enrollment packets containing membership cards and customer service-related letters.
- b. Mail Fraud. Speridian, TrueCoverage, Enhance Health and Herman violated 18 U.S.C. § 1341 by sending or receiving, or causing to be sent or received,

materials via U.S. mail or commercial interstate carriers for the purpose of executing the scheme, which used material misrepresentations and omissions to induce consumers, including Class Plaintiffs and class members, to enroll in ACA healthcare plans, including enrollments without knowledge or consent. The materials that Speridian, TrueCoverage, Enhance Health and Herman sent or caused to be sent include but were not limited to enrollment packets containing membership cards, and customer service-related letters.

189. In devising and executing the scheme, Defendants committed acts constituting indictable offenses under 18 U.S.C. §§ 1341 and 1343, in that they directed and carried out a scheme or artifice to defraud or obtain money by means of materially false misrepresentations or omissions. For the purpose of executing the scheme, Defendants committed or caused to be committed these racketeering acts, which number in the thousands, intentionally and knowingly, with the specific intent to advance the scheme.

190. Defendants had knowledge of the essential nature of the scheme. They knew that false advertisements were being used to lure consumers to enroll in ACA healthcare plans, misuse PII and capture commissions. Despite that knowledge, the Defendants committed the predicate acts of wire and mail fraud described above.

## **VI. CLASS ACTION ALLEGATIONS**

191. Class Plaintiffs bring this lawsuit as a class action on behalf of themselves and all others similarly situated as members of the proposed Classes described as follows:

Consumer Class. All individuals enrolled by TrueCoverage, Enhance Health, their agents and/or subagents into ACA plan(s) within the applicable statutes of limitations, and who suffered damages as a result of:

- (i) responding to an advertisement falsely offering immediate cash benefits and enrolling in an ACA plan that they did not need or qualify for;
- (ii) TrueCoverage, Enhance Health, their agents and/or subagents changing and/or cancelling their ACA plan(s) and/or their plans' AOR;
- (iii) TrueCoverage, Enhance Health, their agents and/or subagents applying for and/or enrolling them in a new ACA plan; and/or
- (iv) non-exchange entities, including but not limited to Minerva, obtaining their personally identifiable information without consent.

Agent Class. All individuals or entities who, within the applicable statute(s) of limitation, suffered damages as a result of TrueCoverage, Enhance Health, their agents and/or subagents engaging in AOR Swaps, Twisting and/or Dual-Apping.

192. The Customer Class is represented by Turner, King, Wells and Foreman. The Agent Class is represented by NavaQuote and Broyer.

193. Excluded from the Classes are TrueCoverage, Enhance Health, Speridian, Minerva, their agents and/or subagents, and their directors, officers, employees or independent contractors.

194. This action may be maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, because it meets all the requirements of Rule 23(a)(1-4), including the numerosity, commonality, typicality and adequacy requirements, and it satisfies the requirements of Rule 23(b)(3) in that the predominance and superiority requirements are met.

195. Numerosity. The members of the Classes are so numerous that joinder of all members is impracticable. The Customer Class exceeds the numerosity requirement because hundreds of thousands of consumers have been victimized by the scheme. The false ads that created Leads to TrueCoverage, Enhance Health and their downlines resulted in hundreds of thousands of enrollments by class members. As for the Agent Class, the CMS reported that 74,100 Marketplace-registered agents and brokers assisted on nearly 5.5 million consumers enrolled in

2023 OEP alone.

196. Commonality. There are numerous questions of fact or law that are common to Class Plaintiffs and all the members of the Classes. Common issues of fact and law predominate over any issues unique to individual class members. Issues that are common to all class members include, but are not limited to the following:

- a. Whether TrueCoverage, Enhance Health, their agents and/or subagents engaged in a scheme to buy and utilize Leads stemming from advertisements that falsely offered consumers cash or cash equivalents;
- b. Whether TrueCoverage, Enhance Health, their agents and/or subagents engaged in AOL Swaps, Twisting and/or Dual-Apps;
- c. Obtained Class Plaintiffs' and class members' PII without consent;
- d. Whether Defendants directed, operated and/or managed the scheme;
- e. Whether Defendants violated 18 U.S.C. § 1962(c) or (d);
- f. Whether Defendants violated the terms of the required web-broker agreements with CMS and/or violated applicable federal regulations by failing to protect Class Plaintiffs' and class members' PII from unlawfully being accessed, collected, used or disclosed;
- g. Whether Class Plaintiffs and class members suffered damages; and
- h. Whether Class Plaintiffs and class members are entitled to treble damages, punitive damages, attorneys' fees and/or expenses.

197. Typicality. Turner, King, Wells and Foreman have claims that are typical of the members of the False Advertising Consumer Class. Turner and Wells received a false advertisement that caused them to purchase major medical insurance from TrueCoverage, Enhance

Health, their agents and/or subagents. Turner, King, Wells and Foreman were all the victim of AOL Swaps, Twisting and/or Dual Apps. NavaQuote and Broyer have claims that are typical of the members of the Agent Class. Each was damaged when they were removed as AOR on their clients' ACA health insurance plans. Furthermore, the claims of the Classes arise under legal theories that apply to Class Plaintiffs and all other class members within those respective Classes.

198. Adequacy of Representation. Class Plaintiffs will fairly and adequately represent the interests of the members of the Classes. Class Plaintiffs do not have claims that are unique to Class Plaintiffs and not the other class members within their respective Classes, nor are there defenses unique to Class Plaintiffs that could undermine the efficient resolution of the claims of the Classes. Further, Class Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel, experienced in class action litigation, to represent them. There is no hostility between Class Plaintiffs and the unnamed class members. Class Plaintiffs anticipate no difficulty in the management of this litigation as a class action.

199. Predominance. Common questions of law and fact predominate over questions affecting only individual class members. The only individual issues likely to arise will be the amount of damages recovered by each class member, the calculation of which does not bar certification.

200. Superiority. A class action is superior to all other feasible alternatives for the resolution of this matter. Individual litigation of multiple cases would be highly inefficient and would waste the resources of the courts and of the parties. The damages sought by Class Plaintiffs and class members are relatively small and unlikely to warrant individual lawsuits given the fees and costs, including expert costs, required to prosecute claims for those fees and premiums.

201. Manageability. This case is well suited for treatment as a class action and easily can be managed as a class action since evidence of both liability and damages can be adduced, and proof of liability and damages can be presented, on a class wide basis, while the allocation and distribution of damages to class members would be essentially a ministerial function.

202. Ascertainability. Class members are readily ascertainable. Some or all of Defendants keep detailed electronic records that show, among other information, the false advertisements, the names of those who responded to the false advertisements and the names and transaction histories of class members whose plan or AOR status was changed by one or more Defendants.

**COUNT I**  
**(Violation of RICO § 1962(c) Against All Defendants)**

203. Class Plaintiffs incorporate the allegations of paragraphs 1 through 202 as if fully set forth herein.

204. The Enterprise is engaged in, and its activities affect, interstate commerce.

205. Defendants are entities or individuals capable of holding a legal or beneficial interest in property, and therefore each meets the definition of a culpable “person” under 18 U.S.C. § 1961.

206. Defendants were associated with the Enterprise and conducted and participated in the Enterprise’s affairs through a pattern of racketeering activity, as defined by 18 U.S.C. § 1961(5), comprised of numerous and repeated uses of the mails and interstate wire communications to execute a scheme to defraud in violation of 18 U.S.C. § 1962(c).

207. The Enterprise was created and/or used as a tool to carry out the scheme and pattern of racketeering activity.

208. Defendants have committed or aided and abetted the commission of at least two acts of racketeering activity, i.e., indictable violations of 18 U.S.C. §§ 1341 and 1343, within the past 10 years. The multiple acts of racketeering activity that they committed and/or conspired to, or aided and abetted in the commission of, were related to each other and constituted a “pattern of racketeering activity.”

209. Defendants used thousands of interstate mail, wire and email communications to create and perpetuate the scheme in support of the false advertisement, AOR Swaps, Twisting and Dual Apps that injured consumers and agents, including Class Plaintiffs and class members.

210. Defendants knew about and directed these activities. Defendants obtained money and property belonging to Class Plaintiffs and class members as a result of these violations. Class Plaintiffs and class members have been injured in their business or property by Defendants’ overt acts of mail and wire fraud.

211. Consumer Class Plaintiffs and members of the Consumer Class have been injured in their property by reason of Defendants’ violations of 18 U.S.C. § 1962, including but not limited to payment of out-of-pocket medical expenses, out-of-pocket expenses to address and undo the results of Defendants’ scheme and/or the payment of tax penalties. Class Plaintiffs and class members of the Agent Class have been injured in their property by reason of Defendants’ violations of 18 U.S.C. § 1962, including loss of commissions and/or payment of out-of-pocket expenses to address and undo the results of Defendants’ scheme.

212. Class Plaintiffs and class members’ injuries were directly and proximately caused by Defendants’ racketeering activity.

213. Defendants knew and intended that Class Plaintiffs and class members would rely on the scheme’s misrepresentations and omissions.



214. Under the provisions of 18 U.S.C. § 1964(c), Class Plaintiffs are entitled to bring this action and to recover their treble damages, the costs of bringing this suit and reasonable attorney's fees. Defendants are liable to Class Plaintiffs and class members for three times their actual damages as proved at trial, plus interest and attorneys' fees.

WHEREFORE, Class Plaintiffs, individually and on behalf of all others similarly situated, pray this Court to enter judgment against Defendants that awards actual damages, treble damages, interest and attorney's fees, and/or such other and further relief as the Court deems just and proper.

**COUNT II**  
**(Section 1962(d) RICO Conspiracy Against All Defendants)**

215. Class Plaintiffs incorporate the allegations of paragraphs 1 through 202 as if fully set forth herein.

216. Defendants agreed and conspired to violate 18 U.S.C. § 1962(c). Specifically, Defendants conspired to conduct and participate in the conduct of the affairs of the Enterprise through a pattern of racketeering activity.

217. With knowledge of the essential nature of the scheme, Defendants have intentionally conspired and agreed to directly and indirectly conduct and participate in the conduct of affairs of the Enterprise through a pattern of racketeering activity. Defendants committed predicate acts that they knew were part of a pattern of racketeering activity and agreed to the commission of those acts to further the schemes described above. That conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

218. As a direct and proximate result of Defendants' conspiracy, the overt acts taken in furtherance of that conspiracy and violations of 18 U.S.C. § 1962(d), Plaintiffs have been injured in their business or property.

WHEREFORE, Class Plaintiffs, individually and on behalf of all others similarly situated, pray this Court to enter judgment against Defendants that awards actual damages, treble damages, interest and attorney's fees, and/or such other and further relief as the Court deems just and proper.

**COUNT III**  
**(Aiding and Abetting a Violation of RICO Section 1962(c) Against All Defendants)**

219. Class Plaintiffs incorporate the allegations of paragraphs 1 through 202 as if fully set forth herein.

220. Defendants aided and abetted and shared the intent to aid and abet a scheme to violate 18 U.S.C. § 1962(c), specifically, a scheme that used false advertisement, AOR Swaps, Twisting and Dual Apps activities to improperly collect commissions and/or revenues, injuring consumers and agents, including Class Plaintiffs and class members.

221. Defendants each had knowledge of the scheme and provided substantial assistance toward its commission.

222. Defendants substantially benefited from their participation in the scheme, earning millions of dollars of fees and other revenue from Class Plaintiffs and class members.

223. As a direct and proximate result of Defendants' aiding and abetting of predicate acts of a Section 1962(c) RICO violation, Class Plaintiffs and class members have suffered damages in an amount to be determined at trial.

WHEREFORE, Class Plaintiffs, individually and on behalf of all others similarly situated, pray this Court to enter judgment against Defendants that awards actual damages, treble damages, interest and attorney's fees, and/or such other and further relief as the Court deems just and proper.

**COUNT IV**  
**(Negligence Per Se Against All Defendants)**

224. Plaintiffs restate and reallege Paragraphs 1-76, 91, 104, 115-73 and 191-202 as if fully set forth herein.

225. Defendants Speridian and TrueCoverage and their EDE platforms, Benefitalign and Inshura, as web-brokers under the ACA regulations, entered into agreement(s) with CMS governing the way each is required to operate under federal regulations, including provisions related to protecting Consumer Class Plaintiffs' and class members' PII from unlawful dissemination.

226. CMS's standard web-broker agreement with Speridian, TrueCoverage, Benefitalign and Inshura required those entities to comply with, among other things, all regulations related to preventing Consumer Class Plaintiffs' and class members' PII from being collected, accessed and/or disclosed to any downline persons or entities, including agents, brokers and non-exchange entities such as Enhance Health and the lead generation firm Minerva, without informed consent from Consumer Class Plaintiffs and class members.

227. Federal regulations promulgated under the ACA also impose duties on all Defendants to ensure that all Exchange privacy and security standards implemented were consistent with the following principles: PII should be created, collected, used and/or disclosed only to the extent necessary to accomplish a specified purpose or purposes(s). *See* 45 CFR 155.260(a)(3)(v).

228. These regulations, which are designed to protect consumers' PII from unlawful disclosure, also apply to agents and brokers that are downline of Speridian and TrueCoverage, such as Enhance Health. For example, 45 CFR 155.220(j)(2)(iv) requires all web-brokers, agents and brokers to protect Consumer Class Plaintiffs' and class members' PII. That duty also extends

to Minerva, Bowsky and Herman, who fall within the definition of a non-exchange entity. *See* 45 CFR § 155.260(b)(3).

229. In addition, Defendants TrueCoverage, Speridian and Enhance Health were required to enter into contracts with Minerva, Bowsky and Herman that included provisions that included, among other things, (i) a description of the functions to be performed by the non-Exchange entity, (ii) language binding the non-Exchange entity to comply with the privacy and security standards and obligations adopted in accordance with 45 CFR § 155.260(b)(3) and specifically listing or incorporating those privacy and security standards and obligations, and (iii) language requiring the non-Exchange entities, Minerva, Bowsky and Herman, to bind any other downstream entities, including but not limited to other lead generation firms that Defendants purchased leads from, to the same privacy and security standards and obligations to which the non-Exchange entity has agreed in its contract or agreement with the Exchange. *See* 45 CFR 155.260(b)(2).

230. Upon information and belief, Minerva and Bowsky did not enter into such an agreement with Bowsky and Minerva, and if they did, Bowsky and Minerva did not comply with their obligations to protect Consumer Class Plaintiffs' and class members' PII from being disclosed.

231. For example, each lead that is generated by lead generation firms, including but not limited to Minerva and Bowsky, is routed to TrueCoverage, Enhance Health and/or their downline agencies and agents. Those agencies receive the calls from consumers through routing software that is under the sole control of the lead generating entity such as Minerva.

232. At all times material, Minerva and Bowsky used the routing software, Retreaver, to forward leads to TrueCoverage and Enhance Health. The purpose of the routing software is to

route the incoming calls from consumers to the appropriate agency that purchased the ad. The routed call received by TrueCoverage, Enhance Health and their downline agencies is first received by their dialing software. Then the call is routed to the appropriate call center and individual agent. During the Class Period, Enhance Health and TrueCoverage used Total Leads Domination (TDS) as their dialer software.

233. Importantly, Defendants' routing software (Retreaver) and dialer software (TLD) records the confidential calls between consumers and the agents for Enhance Health, TrueCoverage and their downlines at the same time, without consent of Consumer Class Plaintiffs and class members.

234. Upon information and belief, the other lead generation firms used by Defendants to obtain Leads also use routing software that records the confidential calls between consumers and the agents for Enhance Health, TrueCoverage and their downlines at the same time without consent of Consumer Class Plaintiffs and class members.

235. Once the calls are recorded by the lead generation firms, Speridian, TrueCoverage and Enhance Health permitted Minerva and Bowsky to retain the recordings of the calls between consumers and TrueCoverage and Enhance Health agents. These calls contain confidential PII, including social security numbers and personal medical information, and Minerva and Bowsky have been permitted to retain custody of the recorded calls for their own business purposes without consent of Consumer Class Plaintiffs and class members. This conduct violates the terms of the web-broker agreements and federal regulations described above.

236. Minerva and Bowsky, as well as the other lead generation firms used by Defendants, fall within the definition of non-exchange entities pursuant to 45 CFR 155.260(b)(1) because they: (i) gain access to personally identifiable information submitted to an Exchange; or

(ii) collect, use, or disclose personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.

237. The purpose of web-broker agreements and the above federal regulations is to protect consumers like Consumer Class Plaintiffs and class members by providing that each QHP issuer that uses a provider network must ensure that the provider network consisting of in-network healthcare providers, as available to all enrollees, meet certain standards, including but not limited to requiring QHP issuers to publish an up-to-date, accurate and complete provider directory.

238. Consumer Class Plaintiffs and class members were harmed as a result of Defendants' violations of the web-broker agreement and federal regulations cited above. The harm includes but may not be limited to:

- a. unauthorized use of the Consumer Class Plaintiffs' and class members' PII, resulting in harm including but not limited to unauthorized AOL Swaps, Twisting and/or Dual Apps;
- b. theft of the Consumer Class Plaintiffs and class members' personal, financial and confidential medical information;
- c. costs associated with the detection and prevention of the Consumer Class Plaintiffs and class members' identity theft and unauthorized use of the Consumer Plaintiffs and class members' PII;
- d. the imminent and certainly impending injury flowing from the substantial risk of potential fraud and identity theft posed to the Consumer Class Plaintiffs and class members by their PII being placed in the hands of criminals on the Internet black market; and

e. the loss of the Consumer Class Plaintiffs’ and class members’ privacy.

239. Consumer Class Plaintiffs and class members fall within the class of persons that the web-broker agreement and federal regulations were intended to protect.

240. The harm or injury suffered by the Consumer Class Plaintiffs and class members as a result of Defendants’ violation of the obligations contained in the web-broker agreement and applicable federal regulations is the same harm that the contractual provisions and regulations were intended to guard against.

241. Defendants’ violations are capable of having a causal connection between it and the damage or injury inflicted.

WHEREFORE, Consumer Class Plaintiffs, individually and on behalf of all others similarly situated, pray this Court to enter judgment against Defendants that awards damages, interest and/or such other and further relief as the Court deems just and proper.

**JURY TRIAL DEMANDED**

Class Plaintiffs hereby demand a trial by jury on all allowable claims and forms of relief.

Dated: April 12, 2024.

Respectfully submitted,

LEVINE KELLOGG LEHMAN  
SCHNEIDER + GROSSMAN LLP

THE DOSS FIRM, LLC

By: /s/Jason Kellogg  
Jason K. Kellogg, P.A.  
Florida Bar No. 0578401  
Primary email: [jk@lklsg.com](mailto:jk@lklsg.com)  
Secondary email: [ame@lklsg.com](mailto:ame@lklsg.com)  
100 Southeast Second Street  
Miami Tower, 36th Floor  
Miami, Florida 33131  
Telephone: (305) 403-8788  
Facsimile: (305) 403-8789

By: /s/Jason Doss  
Jason R. Doss  
Florida Bar No. 0569496  
Primary email: [jasondoss@dossfirm.com](mailto:jasondoss@dossfirm.com)  
1827 Powers Ferry Road Southeast  
Atlanta, Georgia 30339  
Telephone: (770) 578-1314  
Facsimile: (770) 578-1302

# Exhibit 1





The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.) NOTICE: Attorneys MUST Indicate All Re-filed Cases Below.

I. (a) PLAINTIFFS

Conswallo Turner, Tiesha Foreman, Angelina W

DEFENDANTS

Enhance Health, LLC, TrueCoverage LLC, Sper

(b) County of Residence of First Listed Plaintiff Orange County, Texas (EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant Broward County, Florida (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys (Firm Name, Address, and Telephone Number)

Attorneys (If Known)

Jason Kellogg, Levine Kellogg Lehman Schneider + Grossman LLP, 1C

(d) Check County Where Action Arose: MIAMI-DADE MONROE BROWARD PALM BEACH MARTIN ST. LUCIE INDIAN RIVER OKEECHOBEE HIGHLANDS

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff
2 U.S. Government Defendant
3 Federal Question (U.S. Government Not a Party)
4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- Citizen of This State
Citizen of Another State
Citizen or Subject of a Foreign Country
PTF DEF
1 1 Incorporated or Principal Place of Business In This State
2 2 Incorporated and Principal Place of Business In Another State
3 3 Foreign Nation
4 4
5 5
6 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Grid of categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN

(Place an "X" in One Box Only)

- 1 Original Proceeding
2 Removed from State Court
3 Re-filed (See VI below)
4 Reinstated or Reopened
5 Transferred from another district (specify)
6 Multidistrict Litigation Transfer
7 Appeal to District Judge from Magistrate Judgment
8 Multidistrict Litigation - Direct File
9 Reremanded from Appellate Court

VI. RELATED/ RE-FILED CASE(S)

(See instructions): a) Re-filed Case YES NO b) Related Cases YES NO

JUDGE:

DOCKET NUMBER:

VII. CAUSE OF ACTION 18 USC 1962(c,d) -- civil RICO claims

Cite the U.S. Civil Statute under which you are filing and Write a Brief Statement of Cause (Do not cite jurisdictional statutes unless diversity):

LENGTH OF TRIAL via days estimated (for both sides to try entire case)

VIII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23 DEMAND \$ 5,000,000 CHECK YES only if demanded in complaint:

JURY DEMAND: X Yes NO

ABOVE INFORMATION IS TRUE & CORRECT TO THE BEST OF MY KNOWLEDGE

DATE SIGNATURE OF ATTORNEY OF RECORD

April 12, 2024

/s/ Jason Kellogg

## INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

### Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

**I. (a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

**(b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)

**(c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment)”.

**II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.C.P., which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.  
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.  
 United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.  
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked. Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; federal question actions take precedence over diversity cases.)

**III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

**IV. Nature of Suit.** Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).

**V. Origin.** Place an “X” in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Refiled (3) Attach copy of Order for Dismissal of Previous case. Also complete VI.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

Appeal to District Judge from Magistrate Judgment. (7) Check this box for an appeal from a magistrate judge’s decision.

Remanded from Appellate Court. (8) Check this box if remanded from Appellate Court.

**VI. Related/Refiled Cases.** This section of the JS 44 is used to reference related pending cases or re-filed cases. Insert the docket numbers and the corresponding judges name for such cases.

**VII. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553

Brief Description: Unauthorized reception of cable service

**VIII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Rule 23, F.R.Cv.P.

Demand. In this space enter the dollar amount (in thousands of dollars) being demanded or indicate other demand such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

**Date and Attorney Signature.** Date and sign the civil cover sheet.

# **Exhibit B**



**Report Title:** Security Incident Details  
**Run Date and Time:** 07/24/2024 11:54 AM Eastern Daylight Time  
**Run by:** Patrick Hunt  
**Table name:** sn\_si\_incident

**Security Incident**

Number:	SIR0030682	Opened:	07/23/2024 06:49 PM
UserID:	cmsitsd	State:	Analysis
Requested by:	ESD User	Substate:	
Email:		On-Hold:	false
Dept/ OpDiv:		On-Hold Reason:	
Office:		Source:	Phone
Cell:		Alert Sensor:	
Requested by Contractor:		Risk score:	42
Created:	07/23/2024 06:49 PM	Override risk score:	false
Category(category):	Improper Usage/Policy Violation	Business impact:	2 - High
Subcategory:		Priority:	3 - Moderate
Phish Email:		Severity:	3 - Low
Security tags:	Service Desk, FFE	CMS Location Impacted:	
Configuration item:		Affected user:	
Number of Notification sent out:		Previous Assignment Group:	
Number of MBI changes:		Assignment group:	CMS SIR IMT
		Assigned to:	Diego Turner
		Error in Submission:	false
		Description of Error:	
		Assigned vendor:	
		Vendor reference:	

Short description:  
 PII: sender / other / improper usage (initial attached)  
 Description:



From: Robenson Remelus [REDACTED]  
 Sent: Tuesday, July 23, 2024 3:54:16 PM (UTC-07:00) Mountain Time (US & Canada)  
 To: CMS\_IT\_Service\_Desk [REDACTED]  
 Subject: Ticket: CS2206633

To whom it may concern,

My name is Robenson Remelus, NPN 15479763

I am writing to let you know that there have been fraudulent activities on my account which caused my suspension. There is a company that used my credentials without my permission. My ACA business written is in Florida, so there should be no other State ACA plans under my FFM. I have attached documents showing I was a victim of a data breach and also found out that the same company has a RICOT case pending against them. Please reinstate my FFM as this is causing me a lot of financial hardship. I can be reached at [REDACTED] if you have any questions..

.....

.....

CS2206633 - IDM – Suspended Accounts

Inbox

Search for all messages with label Inbox

Remove label Inbox from this conversation

[<https://lh3.googleusercontent.com/a/default-user=s40-p>]

CMSConnect [REDACTED]

5:20 PM (16 minutes ago)

[<https://mail.google.com/mail/u/0/images/cleardot.gif>]

[<https://mail.google.com/mail/u/0/images/cleardot.gif>]

[<https://mail.google.com/mail/u/0/images/cleardot.gif>]

to me

[<https://mail.google.com/mail/u/0/images/cleardot.gif>]

Hello Robenson Remelus,

Thank you for contacting the Federally-facilitated Exchange (FFE) Agent/Broker Email Help Desk.

As of 7/23/2024, you are missing a valid license and health-related Line of Authority in Georgia, Missouri, Mississippi, Ohio, and Wisconsin. You are missing an active appointment with a health insurance carrier in Wisconsin.

If you did not register your NPN with the Marketplace and/or suspect this is fraud, please report this Incident to the CMS IT Service Desk by telephone at [REDACTED] or via email notification at

[REDACTED]

For CMS to consider you compliant with licensure requirements and thus reinstate your registration and Exchange access, please confirm this information is reflected in the National Insurance Producer Registry (NIPR) and respond back to this email address at your earliest convenience. To check the NIPR database, you can search for your NPN at <https://nipr.com/PacNpnSearch.htm>. If you have an inquiry regarding your licensure status, you may contact the NIPR customer service at [https://nipr.com/index\\_contacts.htm](https://nipr.com/index_contacts.htm). If NIPR does not reflect the most current information, it is your responsibility to work with the State Departments of Insurance and/or the issuers where you are appointed to ensure that the NIPR is updated.





Please note, CMS is not currently reviewing agent/broker submitted evidence of licensure information. Please respond only when the NIPR reflects the required information detailed above.

As a reminder, it is a violation of Exchange agreements to assist consumers, sell plans, or process any applications in any states for which you do not have valid licensure.

Thank you,

FFM Agent/Broker Email Help Desk Staff

Actions Taken:

IMT analysis: 7/24/24

Summary: Suspended AB/broker account

Work notes:

07/24/2024 08:23 AM - Diego Turner (Work notes)

Assigning to FFE

07/24/2024 07:57 AM - Michael Horton (Work notes)

this incident appears to be reported by an AB. IMT please notify marketplace of this incident in our shared slack channel and route the ticket to DCOM/FFE.

07/23/2024 06:50 PM - Charles Goodan (Work notes)

From INC1589691:

07/23/2024 06:50 PM - Charles Goodan (Work notes)

Thank you for contacting the CMS IT Service Desk.

In response to your inquiry regarding your Security Occurrences,

Incident SIR0030682 has been created and placed "On Hold-Awaiting Evidence".

Please complete and return a Security Incident Reporting (IR) Form for each Security Occurrence.

(See the attached Security Incident Report Template)

Attach the completed Incident Report to a reply to this email or send them to [CMS\\_IT\\_Service\\_Desk@cms.hhs.com](mailto:CMS_IT_Service_Desk@cms.hhs.com).

(This needs to be done immediately)

Please provide your organization type.

(Example: State-Based Administrating Entity, Federal Marketplace, etc.)

To Open the Report, Click on the attached report in the email, click "Save As", choose where to save the file, navigate to file, Right Click the zipped folder, select "SecureZIP" then select "Extract Here".

To Edit the Report, Open the Document, at the top of the window, Click the "View" button, from the menu, select the "Edit Document" Option.

If you need any further assistance, please contact the CMS IT Service Desk at **REDACTED**.



07/23/2024 06:49 PM - Charles Goodan (Work notes)

Attachment 'databeach-07222024113634.pdf' was uploaded by GQHY on 07/23/2024 06:49 PM with a file size of 309965 bytes.

07/23/2024 06:49 PM - Charles Goodan (Work notes)

Attachment '2024-04-12-Complaint lawsuit.pdf' was uploaded by GQHY on 07/23/2024 06:49 PM with a file size of 3728451 bytes.

07/23/2024 06:49 PM - Charles Goodan (Work notes)

07/23/2024 06:49 PM - Charles Goodan (Work notes)

From: Robenson Remelus **REDACTED**

Sent: Tuesday, July 23, 2024 3:54:16 PM (UTC-07:00) Mountain Time (US & Canada)

To: CMS\_IT\_Service\_Desk <cms\_it\_service\_desk@cms.hhs.gov>

Subject: Ticket: CS2206633

To whom it may concern,

My name is Robenson Remelus, NPN 15479763

I am writing to let you know that there have been fraudulent activities on my account which caused my suspension. There is a company that used my credentials without my permission. My ACA business written is in Florida, so there should be no other State ACA plans under my FFM. I have attached documents showing I was a victim of a data breach and also found out that the same company has a RICOT case pending against them. Please reinstate my FFM as this is causing me a lot of financial hardship. I can be reached at **REDACTED** if you have any questions..

.....

.....

CS2206633 - IDM – Suspended Accounts

Inbox

Search for all messages with label Inbox

Remove label Inbox from this conversation

[<https://lh3.googleusercontent.com/a/default-user=s40-p>]

CMSConnect <CMSITSM@cms.hhs.gov<mailto:CMSITSM@cms.hhs.gov>>

5:20 PM (16 minutes ago)

[<https://mail.google.com/mail/u/0/images/cleardot.gif>]

[<https://mail.google.com/mail/u/0/images/cleardot.gif>]

[<https://mail.google.com/mail/u/0/images/cleardot.gif>]

to me

[<https://mail.google.com/mail/u/0/images/cleardot.gif>]

Hello Robenson Remelus,

Thank you for contacting the Federally-facilitated Exchange (FFE) Agent/Broker Email Help Desk.

As of 7/23/2024, you are missing a valid license and health-related Line of Authority in Georgia, Missouri, Mississippi, Ohio, and Wisconsin. You are missing an active appointment with a health insurance carrier in Wisconsin.

If you did not register your NPN with the Marketplace and/or suspect this is fraud, please report this Incident to the CMS IT Service Desk by telephone at **REDACTED** or via email notification at **REDACTED**.

For CMS to consider you compliant with licensure requirements and thus reinstate your registration and Exchange access, please confirm this information is reflected in the National Insurance Producer Registry (NIPR) and respond back to this email address at your earliest convenience. To check the NIPR database, you can search for your NPN at <https://nipr.com/PacNpnSearch.htm>. If you have an inquiry regarding your licensure status, you may contact the NIPR customer service at [https://nipr.com/index\\_contacts.htm](https://nipr.com/index_contacts.htm). If NIPR does not reflect the most current information, it is your responsibility to work with the State Departments

and/or the issuers where you are appointed to ensure that the NIPR is updated.

Please note, CMS is not currently reviewing agent/broker submitted evidence of licensure information. Please respond only when the NIPR reflects the required information detailed above.





As a reminder, it is a violation of Exchange agreements to assist consumers, sell plans, or process any applications in any states for which you do not have valid licensure.

Thank you,

FFM Agent/Broker Email Help Desk Staff

07/23/2024 06:46 PM - Charles Goodan (Work notes)

Attachment 'databeach-07222024113634.pdf' was uploaded by GQHY on 07/23/2024 06:46 PM with a file size of 309965 bytes.

07/23/2024 06:46 PM - Charles Goodan (Work notes)

Attachment '2024-04-12-Complaint lawsuit.pdf' was uploaded by GQHY on 07/23/2024 06:46 PM with a file size of 3728451 bytes.

Secure notes:

**REDACTED**

# **Exhibit C**



**Report Title:** Security Incident Details  
**Run Date and Time:** 09/19/2024 03:46 PM Eastern Daylight Time  
**Run by:** Leslie Nettles  
**Table name:** sn\_si\_incident

**Security Incident**

Number:	SIR0030846	Opened:	07/29/2024 08:20 AM
UserID:	WOOR	State:	Analysis
Requested by:	Seth Whaley	Substate:	
Email:	REDACTED	On-Hold:	true
Dept/ OpDiv:		On-Hold Reason:	Awaiting Internal Resource
Office:	REDACTED	Source:	Phone
Cell:		Alert Sensor:	
Requested by Contractor:	Yes	Risk score:	35
Created:	07/29/2024 08:32 AM	Override risk score:	false
Category(category):	Improper Usage/Policy Violation	Business impact:	3 - Non-critical
Subcategory:		Priority:	4 - Low
Phish Email:		Severity:	2 - Medium
Security tags:	Ad-hoc	CMS Location Impacted:	CMS Baltimore
Configuration item:		Affected user:	
Number of Notification sent out:		Previous Assignment Group:	
Number of MBI changes:		Assignment group:	CMS SIR IMT
		Assigned to:	Seth Whaley
		Error in Submission:	false
		Description of Error:	
		Assigned vendor:	
		Vendor reference:	

**Short description:**  
 Benefit Align / True Coverage | Ad-Hoc | Improper Usage / On Hold  
**Description:**

# Exhibit D

CUI//DL ONLY (CMS DSI)

## Centers for Medicare & Medicaid Services



Office of Information Technology (OIT)  
Information Security & Privacy Group (ISPG)  
Division of Strategic Information (DSI)

# Supply Chain Risk Management Supply Chain Risk Assessment: Speridian Technologies LLC

Controlled Unclassified Information  
Controlled by: CMS OIT ISPG DSI  
CUI Category: Contract Information

---

08/05/2024

SCRM Assessment File Number: 2024 CMS-2024-0050-OIT\_Speridian SCRA\_5 August  
2024

CUI//DL ONLY (CMS DSI)

CUI//DL ONLY (CMS DSI)

**Purpose Statement:** This supply chain risk assessment (SCRA) is being conducted at the request of the Division of Strategic Information (DSI) within the Information Security & Privacy Group (ISPG) under the Office of Information Technology (OIT) of the Centers for Medicare and Medicaid Services (CMS). The scope for this level of review will focus on Foreign Ownership, Control and Influence (FOCI), financial solvency and adherence to U.S. national policies, and cyber factors. **Speridian Technologies LLC hereby referred to as “Speridian,” (Cage Code: 33MM8/ UEI QYQRKK9MFVK4) is affiliated with CMS as a contractor** for several contracts and was evaluated as an incident response for suspected mishandling CMS data outside of the US, which would be a violation of CMS Business Rule 8.

**Executive Summary:** The DSI SCRM Team assessed the overall risk of Speridian as it relates to Foreign Ownership Control and Influence (FOCI), financial solvency, adherence to U.S. national policies, and cyber factors. **DSI SCRM determined the Company’s overall SCRM risk to CMS as being Critical.** There has been no evidence found that Speridian is currently being targeted by US adversaries. However, multiple concerns were noted with the company. The company’s owners have substantial ties to **India**. A substantial amount of the company’s operations appear to be based out of **India**, where the majority of the employees seem to be operating from. The majority of the company’s named executive named officers have ties to or are based in **India**. The majority of the company’s research and development appear to be conducted in **India** and **Pakistan**. The number of H-1B visas issued to the company suggests that a large amount of the company’s workforce are not US citizens. Speridian and its subsidiary, True Coverage, are defendants in an active lawsuit filed in 2024 alleging that they engaged in a variety of illegal practices including violations of the RICO Act, as well as the misuse of PII, and insurance fraud. This was alleged to be accomplished via the use of a Speridian product, “Benefitalign,” which allows access to the ACA Marketplace Exchange. Benefitalign allows access to the exchange and houses CMS data abroad, which is in violation of their EDE agreement with HHS. Speridian’s cyber security hygiene is below industry average. Multiple domains tied to Speridian are shown to be based in India, making it appear that agency data is stored outside of the US. Speridian uses a hybrid onsite/offshore delivery model which means that a portion of the work and support is conducted from overseas locations. Speridian operates a large, dedicated data center in India, and it is possible that agency data is processed and/or stored in this location. The company has subsidiaries and operations in **Canada, India, Pakistan, Saudi Arabia, Singapore,** and the **UAE**. There may be further locations and subsidiaries which have not yet been discovered.

The following table identifies the areas evaluated by the DSI SCRM Team and the corresponding risk rating:

Risk Ratings	
Overall Risk (Based off highest risk rating below)	Critical
Foreign Ownership, Control, or Influence	Moderate
Significant Adverse Information (Legal, Financial, Compliance with United States Government Prohibitions)	Moderate
Supply Chain Tier Structure Concerns (Presence of Sanctioned / Restricted Suppliers within Supplier’s Logistics Network)	Low
Company Product Related Concerns	Low
Company Cyber Vulnerabilities	Critical

**Company Background:** Speridian Technologies is an information technology and services company that designs and develops technology enabled software solutions to its clients. It specializes in customer relationship management (CRM) implementation, application development, Oracle SOA, Oracle fusion, systems integration, infrastructure management and application integration. The company was founded in 2003 and is headquartered in Albuquerque, New Mexico. It seeks to acquire other companies that provide IT and business consulting services.<sup>1</sup>

<sup>1</sup> Pitchbook

CUI//DL ONLY (CMS DSI)

CUI//DL ONLY (CMS DSI)

**Foreign Ownership, Control, or Influence:** While ultimate beneficial ownership is unclear due to the company's status as a privately owned entity, co-founders KP Hari and Girish Panicker were educated in India and are believed to have continuing ties to India.<sup>2,3</sup>

This company does not have a foreign headquarters address officially. However, the company has an Indian based subsidiary which appears to be where most of their employees are operating from, and therefore is presumed to be the de facto HQ.<sup>4,5</sup>

No traditional partnerships were noted; however, the company's customers included the UAE Armed forces and multiple UAE civil authorities.<sup>6</sup>

The majority of the named executive officers at the company have been educated in, or are currently based in India, including the Cofounders, Chairman, Vice Chairman, and Chief Technology Officer.<sup>7</sup>

Based off of hiring patterns, it appears that Speridian almost exclusively conducts their research and development in India and Pakistan.<sup>8</sup>

In 2012 the company announced a major expansion of its operations in Kerala, India. The city's Technopark location already housed the bulk of Speridian's workforce, which grew to more than 600 in 2013.<sup>9</sup>

Since 2009, Speridian has sponsored 394 initial H-1B approvals, and 565 continuing approvals, indicating that their workforce is largely reliant on non-U.S. citizen labor. Additionally, they have sponsored 65 total visas which were denied. The amount of visas issued to the company indicates that a large amount of the company's workforce are not U.S. citizens.<sup>10</sup>

**Significant Adverse Information:** Speridian and its subsidiary, True Coverage, are defendants in a lawsuit filed in 2024 alleging that they engaged in a variety of illegal practices including violations of the RICO Act as well as the misuse of PII and insurance fraud. This was allegedly done through the use of Speridian's platform Benefitalign, which allows access to the ACA Marketplace Exchange.<sup>11</sup>

**Supply Chain Tier Structure Concerns:** Open source research did not yield any evidence of restricted suppliers within this firm.

**Company Product Related Concerns:** Benefitalign, one of Speridian's products which allows access to the exchange, appears to be in violation of their EDE agreement which stipulates that Any Web-broker and its assignees or

---

<sup>2</sup> Pitchbook

<sup>3</sup> [Speridian](#)

<sup>4</sup> Govini

<sup>5</sup> [Speridian](#)

<sup>6</sup> [AmbitionBox](#)

<sup>7</sup> [Speridian](#)

<sup>8</sup> [Speridian](#)

<sup>9</sup> [JRank](#)

<sup>10</sup> [USCIS](#)

<sup>11</sup> [Georgetown.edu](#)

CUI//DL ONLY (CMS DSI)

## CUI//DL ONLY (CMS DSI)

subcontractors—including, employees, developers, agents, representatives, or contractors—cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor can such entities remotely connect or transmit data to a Web-broker’s systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations.<sup>12</sup> This includes any such connection through virtual private networks (“VPNs”).<sup>13</sup> This is due to the fact that a portion of Speridian’s infrastructure appears to be based outside of the United States.

**Company Cyber Vulnerabilities:** Security Scorecard grades Speridian as a “C” with an overall cyber score of “72 out of 100.” Of all the threat indicators scanned by Security Scorecard (Cubit Score, Application Security, IP Reputation, Endpoint Security, Patching Cadence, DNS Health, Network Security, Social Engineering, Information Leak, Hacker Chatter), Application Security was ranked lowest with a “66 out of 100”. Patching Cadence was rated as “75 out of 100”, Network security was rated as a “76 out of 100”, and DNS Health was rated as an “90 out of 100”, all except DNS Health of which are characterized as below industry average.<sup>14</sup>

Corresponding to the suspicions of operating in a foreign country, multiple domains attached to Speridian traced to servers outside of the United States. This was verified on multiple country nodes, proving that this is not a local content delivery setting. Noted domains include speridiano360.com which traces to Singapore; the company’s own internal benefits portal benefits.speridian.com traces to India; o360.speridian.com traces to India; mail.speridian.com traces to India; lms.benefitalign.com traces to India; https://121.242.120.107/account/lost\_password which is the Benefitalign password reset link traces to India; o360.benefitalign.com traces to India; and https://support.sesameindia.com/ traces to India.<sup>15</sup>

An interview with a Speridian executive and a separate statement of work given to a municipal government state that Speridian uses a blended onshore/offshore delivery and support model, which means that a portion of the work and support is conducted from overseas locations.<sup>16,17,18,19</sup>

In 2006 Speridian opened a 10,000-square-foot data center in India.<sup>20</sup>

**Recommended Mitigation Strategies:** Risk level is grave and all associations with this company are recommended for immediate action. DSI SCRM will NOT endorse any business relationship with this entity. It is recommended that CMS seeks an alternative supplier for the services that company currently provides. Further, it is recommended that company be suspended or disbarred from further participation in CMS contracts due to their foreign development and presumed foreign data storage. Lastly, it is recommended that an assessment be conducted to ascertain the level of compromise which CMS may have suffered due to the relationship with this company.

**Appendix A: Classified Findings: Research for this assessment was conducted using publicly available information.**

No classified research was conducted as part of this report.

---

<sup>12</sup> [HHS](#)

<sup>13</sup> [HHS](#)

<sup>14</sup> Security Scorecard

<sup>15</sup> [IPLocation](#)

<sup>16</sup> [Oracle](#)

<sup>17</sup> [NAHAC](#)

<sup>18</sup> [Speridian](#)

<sup>19</sup> [Slideshare](#)

<sup>20</sup> [JRank](#)



CUI//DL ONLY (CMS DSI)

**Appendix B: Methodology:** Open-Source Intelligence (OSINT) Collection

The CMS SCRM Team uses OSINT methodologies to conduct supplier assessments. The Office of the Director of National Intelligence (ODNI) defines OSINT as “intelligence derived exclusively from publicly available information that addresses specific intelligence priorities, requirements, or gaps.”<sup>21</sup>

**Disclaimer:** This report may contain information that is CONTROLLED UNCLASSIFIED INFORMATION (CUI) and is intended to be used for official use only. The report or any of its attachments should not be disseminated, distributed, or copied to persons not authorized to receive such information. The contents of this report are not intended for public release. Please contact the originator prior to sharing this information and ensure that all sensitive correspondence is properly labeled prior to dissemination. If you are not the intended recipient or have received this report in error, please notify the originator immediately and erase all copies of the report and its attachments.

---

<sup>21</sup> [ODNI](#)

CUI//DL ONLY (CMS DSI)

# **Exhibit E**

**ENHANCED DIRECT ENROLLMENT AGREEMENT BETWEEN ENHANCED  
DIRECT ENROLLMENT ENTITY AND THE CENTERS FOR MEDICARE &  
MEDICAID SERVICES FOR THE INDIVIDUAL MARKET FEDERALLY-  
FACILITATED EXCHANGES AND STATE-BASED EXCHANGES ON THE FEDERAL  
PLATFORM**

---

**THIS ENHANCED DIRECT ENROLLMENT AGREEMENT** (“Agreement”) is entered into by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES (“CMS”), as the Party (as defined below) responsible for the management and oversight of the Federally-facilitated Exchanges (“FFE”), also referred to as “Federally-facilitated Marketplaces” or “FFMs” and the operation of the federal eligibility and enrollment platform, which includes the CMS Data Services Hub (“Hub”), relied upon by certain State-based Exchanges (SBEs) for their eligibility and enrollment functions (including State-based Exchanges on the Federal Platform (SBE-FPs)), and Truecoverage LLC (dba) Inshura (hereinafter referred to as “Enhanced Direct Enrollment [EDE] Entity”), which uses a non-FFE Internet website in accordance with 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or 156.1230 to assist Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives in applying for Advance Payments of the Premium Tax Credit (“APTC”) and Cost-sharing Reductions (“CSRs”); applying for enrollment in Qualified Health Plans (“QHPs”); completing enrollment in QHPs; and providing related Customer Service. CMS and EDE Entity are hereinafter referred to as the “Party” or, collectively, as the “Parties.”

**WHEREAS:**

Section 1312(e) of the Affordable Care Act (“ACA”) provides that the Secretary of the U.S. Department of Health & Human Services (“HHS”) shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals in QHPs through an Exchange, and to assist individuals in applying for APTC and CSRs, to the extent allowed by States. To participate in the FFEs or SBE-FPs, Agents and Brokers, including Web-brokers, must complete all applicable registration and training requirements under 45 C.F.R. § 155.220.

Section 1301(a) of the ACA provides that QHPs are health plans that are certified by an Exchange and, among other things, comply with the regulations developed by the HHS under Section 1321(a) of the ACA and other requirements that an applicable Exchange may establish.

To facilitate the eligibility determination and enrollment processes, CMS will provide centralized and standardized business and technical services (“Hub Web Services”) through application programming interfaces (“APIs”) to EDE Entity that will enable EDE Entity to host application, enrollment, and post-enrollment services on EDE Entity’s own website. The APIs will enable the secure transmission of key eligibility and enrollment information between CMS and EDE Entity.

To facilitate the operation of the FFEs and SBE-FPs, CMS desires to: (a) allow EDE Entity to create, collect, disclose, access, maintain, store, and use Personally Identifiable

Information (“PII”) it receives directly from CMS and from Consumers, Applicants, Qualified Individuals, and Enrollees through EDE Entity’s website—or from these individuals’ legal representatives or Authorized Representatives—for the sole purpose of performing activities that are necessary to carry out functions that the ACA and its implementing regulations permit EDE Entity to perform; and (b) allow EDE Entity to provide such PII and other Consumer, Applicant, Qualified Individual, and Enrollee information to the FFEs and SBE-FPs through specific APIs to be provided by CMS.

EDE Entity desires to use an EDE Environment to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—to perform the Authorized Functions described in Section III.a of this Agreement.

45 C.F.R. § 155.260(b) provides that an Exchange must, among other things, require as a condition of contract or agreement that Non-Exchange Entities comply with privacy and security standards that are consistent with the standards in 45 C.F.R. §§ 155.260(a)(1) through (a)(6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 C.F.R. § 155.260(a)(3). 45 C.F.R. § 155.280 requires HHS to oversee and monitor Non-Exchange Entities for compliance with Exchange-established privacy and security requirements.

CMS has adopted privacy and security standards with which EDE Entity must comply, as specified in the Non-Exchange Entity System Security and Privacy Plan (“NEE SSP”)<sup>1</sup> and referenced in Appendix A (“Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities”), which are specifically incorporated herein. The security and privacy controls and implementation standards documented in the NEE SSP are established in accordance with Section 1411(g) of the ACA (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 (“FISMA”) (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the standards in 45 C.F.R. §§ 155.260(a)(1) through (a)(6).

Now, therefore, in consideration of the promises and covenants herein contained, the adequacy of which the Parties acknowledge, the Parties agree as follows:

I. Definitions.

Capitalized terms not otherwise specifically defined herein shall have the meaning set forth in the attached Appendix B (“Definitions”). Any capitalized term that is not defined herein or in Appendix B has the meaning provided in 45 C.F.R. § 155.20.

---

<sup>1</sup> The NEE SSP template is located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

II. Interconnection Security Agreement (ISA) Between Centers for Medicare & Medicaid Services (CMS) and Enhanced Direct Enrollment (EDE) Entity (“ISA”).

If EDE Entity is a Primary EDE Entity, it must enter into an ISA with CMS. EDE Entity must comply with all terms of the ISA,<sup>2</sup> including the privacy and security compliance requirements set forth in the ISA. The ISA shall be in effect for the full duration of this Agreement. If an Upstream EDE Entity is using a Primary EDE Entity’s EDE Environment, the Primary EDE Entity must supply an NEE SSP to each Upstream EDE Entity using the Primary EDE Entity’s EDE Environment that identifies all Common Controls and Hybrid Controls implemented in the EDE Environment. All Common Controls and Hybrid Controls must be documented between each applicable Upstream EDE Entity and its Primary EDE Entity as required by the NEE SSP section “Common and Hybrid Controls.” Furthermore, Appendix B of the ISA requires a Primary EDE Entity to attest that it has documented and shared the NEE SSP inheritable Common Controls and Hybrid Controls with applicable Upstream EDE Entities.

III. Acceptance of Standard Rules of Conduct.

EDE Entity and CMS are entering into this Agreement to satisfy the requirements under 45 C.F.R. §§ 155.260(b)(2) and 155.221(b)(4)(v). EDE Entity hereby acknowledges and agrees to accept and abide by the standard rules of conduct set forth below and in the Appendices, which are incorporated by reference in this Agreement, while and as engaging in any activity as EDE Entity for purposes of the ACA. EDE Entity shall strictly adhere to the privacy and security standards—and ensure that its employees, officers, directors, contractors, subcontractors, agents, Auditors, and representatives strictly adhere to the same—to gain and maintain access to the Hub Web Services and to create, collect, disclose, access, maintain, store, and use PII for the efficient operation of the FFEs and SBE-FPs. To the extent the privacy and security standards set forth in this Agreement are different than privacy and security standards applied to EDE Entity through any existing agreements with CMS, the more stringent privacy and security standards shall control.

- a. Authorized Functions. EDE Entity may create, collect, disclose, access, maintain, store, and use PII for the following, if applicable:
1. Assisting with completing applications for QHP eligibility;
  2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons;
  3. Assisting with completing applications for the receipt of APTC or CSRs and with selecting an APTC amount;
  4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR determination, if applicable;
  5. Assisting with the application for and determination of certificates of exemption;

---

<sup>2</sup> Unless specifically indicated otherwise, references to the ISA refer to the current, legally enforceable version of the agreement. The ISA is available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

6. Assisting with filing appeals of eligibility determinations in connection with the FFEs and SBE-FPs;
7. Transmitting information about the Consumer's, Applicant's, Qualified Individual's, or Enrollee's decisions regarding QHP enrollment and/or CSR and APTC information to the FFEs and SBE-FPs;
8. Facilitating payment of the initial premium amount to the appropriate QHP Issuer;
9. Facilitating an Enrollee's ability to disenroll from a QHP;
10. Educating Consumers, Applicants, Qualified Individuals or Enrollees—or these individuals' legal representatives or Authorized Representatives—on Insurance Affordability Programs and, if applicable, informing such individuals of eligibility for Medicaid or the Children's Health Insurance Program (CHIP);
11. Assisting an Enrollee in reporting changes in eligibility status to the FFEs and SBE-FPs throughout the coverage year, including changes that may affect eligibility (e.g., adding a dependent);
12. Correcting errors in the application for QHP enrollment;
13. Informing or reminding Enrollees when QHP coverage should be renewed, when Enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform Enrollees of QHP coverage options at renewal;
14. Providing appropriate information, materials, and programs to Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to inform and educate them about the use and management of their health information, as well as medical services and benefit options offered through the selected QHP or among the available QHP options;
15. Contacting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to assess their satisfaction or resolve complaints with services provided by EDE Entity in connection with the FFEs, SBE-FPs, EDE Entity, or QHPs;
16. Providing assistance in communicating with QHP Issuers;
17. Fulfilling the legal responsibilities related to the efficient functions of QHP Issuers in the FFEs and SBE-FPs, as permitted or required by a Web-broker EDE Entity's contractual relationships with QHP Issuers; and
18. Performing other functions substantially similar to those enumerated above and such other functions that CMS may approve in writing from time to time.

- b. Collection of PII. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, EDE Entity may create, collect, disclose, access, maintain, store, and use the following PII from Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives— including, but not limited to:
- APTC percentage and amount applied
  - Auto disenrollment information
  - Applicant name
  - Applicant address
  - Applicant birthdate
  - Applicant telephone number
  - Applicant email
  - Applicant Social Security Number
  - Applicant spoken and written language preference
  - Applicant Medicaid Eligibility indicator, start and end dates
  - Applicant CHIP eligibility indicator, start and end dates
  - Applicant QHP eligibility indicator, start and end dates
  - Applicant APTC percentage and amount applied eligibility indicator, start and end dates
  - Applicant household income
  - Applicant maximum APTC amount
  - Applicant CSR eligibility indicator, start and end dates
  - Applicant CSR level
  - Applicant QHP eligibility status change
  - Applicant APTC eligibility status change
  - Applicant CSR eligibility status change
  - Applicant Initial or Annual Open Enrollment Indicator, start and end dates
  - Applicant Special Enrollment Period (“SEP”) eligibility indicator and reason code
  - Contact name
  - Contact address
  - Contact birthdate
  - Contact telephone number
  - Contact email
  - Contact spoken and written language preference
  - Enrollment group history (past six months)
  - Enrollment type period
  - FFE Applicant ID
  - FFE Member ID
  - Issuer Member ID
  - Net premium amount
  - Premium amount, start and end dates

- Credit or Debit Card Number, name on card
  - Checking account and routing number
  - SEP reason
  - Subscriber indicator and relationship to subscriber
  - Tobacco use indicator and last date of tobacco use
  - Custodial parent
  - Health coverage
  - American Indian/Alaska Native status and name of tribe
  - Marital status
  - Race/ethnicity
  - Requesting financial assistance
  - Responsible person
  - Dependent name
  - Applicant/dependent sex
  - Student status
  - Subscriber indicator and relationship to subscriber
  - Total individual responsibility amount
  - Immigration status
  - Immigration document number
  - Naturalization document number
- c. Security and Privacy Controls. EDE Entity agrees to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including the NEE SSP. Furthermore, EDE Entity agrees to timely inform the Exchange of any material change in its administrative, technical, or operational environments, or any material change that would require an alteration of the privacy and security standards within this Agreement through the EDE Entity-initiated Change Request process (Section IX.c of this Agreement).
- d. Use of PII. PII collected from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—in the context of completing an application for QHP, APTC, or CSR eligibility, if applicable, or enrolling in a QHP, or any data transmitted from or through the Hub, if applicable, may be used only for Authorized Functions specified in Section III.a of this Agreement. Such PII may not be used for purposes other than authorized by this Agreement or as consented to by a Consumer, Applicant, Qualified Individual, and Enrollee—or these individuals’ legal representatives or Authorized Representatives.
- e. Collection and Use of PII Provided Under Other Authorities. This Agreement does not preclude EDE Entity from collecting PII from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—for a non-FFE/non-SBE-FP/non-Hub purpose, and using, reusing, and disclosing PII obtained as permitted by applicable law and/or other applicable



authorities. Such PII must be stored separately from any PII collected in accordance with Section III.b of this Agreement.

- f. Ability of Individuals to Limit Collection and Use of PII. EDE Entity agrees to provide the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—the opportunity to opt in to have EDE Entity collect, create, disclose, access, maintain, store, and use their PII. EDE Entity agrees to provide a mechanism through which the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—can limit the collection, creation, disclosure, access, maintenance, storage and use of his or her PII for the sole purpose of obtaining EDE Entity’s assistance in performing Authorized Functions specified in Section III.a of this Agreement.
- g. Downstream and Delegated Entities. EDE Entity will satisfy the requirement in 45 C.F.R. § 155.260(b)(2)(v) to require Downstream and Delegated Entities to adhere to the same privacy and security standards that apply to Non-Exchange Entities by entering into written agreements with any Downstream and Delegated Entities that will have access to PII collected in accordance with this Agreement. EDE Entity must require in writing all Downstream and Delegated Entities adhere to the terms of this Agreement.

Upon request, EDE Entity must provide CMS with information about its downstream Agents/Brokers, EDE Entity’s oversight of its downstream Agents/Brokers, and the EDE Environment(s) it provides to each of its downstream Agents/Brokers.

- h. Commitment to Protect PII. EDE Entity shall not release, publish, or disclose Consumer, Applicant, Qualified Individual, or Enrollee PII to unauthorized personnel, and shall protect such information in accordance with provisions of any laws and regulations governing the adequate safeguarding of Consumer, Applicant, Qualified Individual, or Enrollee PII, the misuse of which carries with it the potential to cause financial, reputational, and other types of harm.
  - 1. Technical leads must be designated to facilitate direct contacts between the Parties to support the management and operation of the interconnection.
  - 2. The overall sensitivity level of data or information that will be made available or exchanged across the interconnection will be designated as MODERATE as determined by Federal Information Processing Standards (FIPS) Publication 199.
  - 3. EDE Entity agrees to comply with all federal laws and regulations regarding the handling of PII—regardless of where the organization is located or where the data are stored and accessed.
  - 4. EDE Entity’s Rules of Behavior must be at least as stringent as the HHS Rules of Behavior.<sup>3</sup>

---

<sup>3</sup> The HHS Rules of Behavior are available at the following link: <https://www.hhs.gov/ocio/policy/hhs-rob.html>.

5. EDE Entity understands and agrees that all financial and legal liabilities arising from inappropriate disclosure or Breach of Consumer, Applicant, Qualified Individual, or Enrollee PII while such information is in the possession of EDE Entity shall be borne exclusively by EDE Entity.
6. EDE Entity shall train and monitor staff on the requirements related to the authorized use and sharing of PII with third parties and the consequences of unauthorized use or sharing of PII, and periodically audit their actual use and disclosure of PII.

IV. Effective Date and Term; Renewal.

- a. Effective Date and Term. This Agreement becomes effective on the date the last of the two Parties executes this Agreement and ends the Day before the first Day of the open enrollment period (“OEP”) under 45 C.F.R. § 155.410(e)(3) for the benefit year beginning January 1, 2025.
- b. Renewal. This Agreement may be renewed upon the mutual agreement of the Parties for subsequent and consecutive one (1) year periods upon thirty (30) Days’ advance written notice to EDE Entity.

V. Termination.

- a. Termination without Cause. Either Party may terminate this Agreement without cause and for its convenience upon thirty (30) Days’ prior written notice to the other Party.  
  
EDE Entity must reference and complete the NEE Decommissioning Plan and NEE Decommissioning Close Out Letter in situations where EDE Entity will retire or decommission its EDE Environment.<sup>4</sup>
- b. Termination of Agreement with Notice by CMS. The termination of this Agreement and the reconsideration of any such termination shall be governed by the termination and reconsideration standards adopted by the FFEs or SBE-FPs under 45 C.F.R. § 155.220. Notwithstanding the foregoing, EDE Entity shall be considered in “Habitual Default” of this Agreement in the event that it has been served with a non-compliance notice under 45 C.F.R. § 155.220(g) or an immediate suspension notice under Section V.c of this Agreement more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately terminate this Agreement upon notice to EDE Entity without any further opportunity to resolve the Breach and/or non-compliance.
- c. Termination of Interconnection for Non-compliance. Instances of non-compliance with the privacy and security standards and operational requirements under this Agreement by EDE Entity, which may or may not rise to the level of a material Breach of this Agreement, may lead to termination of the interconnection between the Parties. CMS may block EDE Entity’s access to CMS systems if EDE Entity does not

---

<sup>4</sup> The Non-Exchange Entity (NEE) Decommissioning Plan and NEE Decommissioning Close Out Letter are available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

- implement reasonable precautions to prevent the risk of Security Incidents spreading to CMS' network or based on the existence of unmitigated privacy or security risks, or the misuse of the PII of Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives. In accordance with Section X.m of this Agreement, CMS is authorized to audit the security of EDE Entity's network and systems periodically by requesting that EDE Entity provide documentation of compliance with the privacy and security requirements in this Agreement and in the ISA. EDE Entity shall provide CMS access to its information technology resources impacted by this Agreement for the purposes of audits. CMS may suspend or terminate the interconnection if EDE Entity does not comply with such a compliance review request within seven (7) business days, or within such longer time period as determined by CMS. Further, notwithstanding Section V.b of this Agreement, CMS may immediately suspend EDE Entity's ability to transact information with the FFEs or SBE-FPs via use of its EDE Environment if CMS discovers circumstances that pose unacceptable or unmitigated risk to FFE operations or CMS information technology systems. If EDE Entity's ability to transact information with the FFEs or SBE-FPs is suspended, CMS will provide EDE Entity with written notice within two (2) business days.
- d. Effect of Termination. Termination of this Agreement will result in termination of the functionality and electronic interconnection(s) covered by this Agreement, but will not affect obligations under EDE Entity's other respective agreement(s) with CMS, including the QHP Issuer Agreement, the Web-broker Agreement, or the Agent Broker General Agreement for Individual Market Federally-Facilitated Exchanges and State-Based Exchanges on the Federal Platform (Agent/Broker Agreement). However, the termination of EDE Entity's ISA, QHP Issuer Agreement, or Web-broker Agreement will result in termination of this Agreement and termination of EDE Entity's connection to CMS systems, including its connection to the Hub and ability to access the EDE suite of APIs as allowed by this Agreement. CMS may terminate this Agreement and EDE Entity's connection to CMS systems, consistent with this clause, if a Designated Representative, who is associated with the EDE Entity, has their Agent/Broker Agreement terminated by CMS.
- e. Notice to Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—of Termination of the Interconnection/Agreement, Suspension of Interconnection, and Nonrenewal of Agreement. EDE Entity must provide Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—with written notice of termination of this Agreement without cause, as permitted under Section V.a of this Agreement, no less than ten (10) Days prior to the date of termination. Within ten (10) Days after termination or expiration of this Agreement or termination or suspension of the interconnection, EDE Entity must provide Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—with written notice of termination of this Agreement with cause under Section V.b of this Agreement; termination or suspension of the interconnection for non-compliance under Section V.c of this Agreement; termination resulting from termination of EDE Entity's ISA,

QHP Issuer Agreement, or Web-broker Agreement under Section V.d of this Agreement; or non-renewal of this Agreement.

The written notice required by this Section shall notify each Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—of the date the termination or suspension of the interconnection will or did occur and direct the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—to access his or her application through the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]) after that date. The written notice shall also provide sufficient details to the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—, including, but not limited to the Consumer's, Applicant's, Qualified Individual's, or Enrollee's Application ID, pending actions, and enrollment status, to allow the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—to update his or her application and provide the next steps necessary to update the Consumer's, Applicant's, Qualified Individual's, or Enrollee's application through the FFE. If EDE Entity's interconnection has been suspended, the written notice must also state that EDE Entity will provide updates to the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—regarding the Consumer's, Applicant's, Qualified Individual's, or Enrollee's—or these individuals' legal representatives or Authorized Representatives—ability to access his or her application through EDE Entity's website in the future.

In addition to providing written notice to Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—EDE Entity must also prominently display notice of the termination or suspension of the interconnection on EDE Entity's website, including language directing Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—to access their applications through the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]).

This clause will survive the expiration or termination of this Agreement.

- f. Destruction of PII. EDE Entity covenants and agrees to destroy all PII in its possession at the end of the record retention period required under the NEE SSP. EDE Entity's duty to protect and maintain the privacy and security of PII, as provided for in the NEE SSP, shall continue in full force and effect until such PII is destroyed and shall survive the termination or expiration of this Agreement.

This clause will survive expiration or termination of this Agreement.

VI. Use of EDE Entity's EDE Environment by Agents, Brokers, or DE Entity Application Assisters.

- a. General. EDE Entity may allow third-party Agents, Brokers, or DE Entity Application Assisters that are not or will not be a party to their own EDE Agreement with CMS to enroll Qualified Individuals in QHPs and to assist individuals in applying for APTC and CSRs through EDE Entity's EDE Environment. EDE Entity, or an Upstream EDE Entity<sup>5</sup> for which EDE Entity provides an EDE Environment, must have a contractual and legally binding relationship with its third-party Agents, Brokers, or DE Entity Application Assisters reflected in a signed, written agreement between the third-party Agents, Brokers, or DE Entity Application Assisters and EDE Entity.

Except as provided in this Section, or as documented for CMS review and approval consistent with Section IX.c of this Agreement as a data connection in the ISA, EDE Entity may not establish a data connection between a third-party Agent's or Broker's website and the EDE Entity's EDE Environment that transmits any data.

The use of embedding tools and programming techniques, such as iframe technical implementations, which may enable the distortion, manipulation, or modification of the audited and approved EDE Environment and the overall EDE End-User Experience developed by a Primary EDE Entity, are prohibited unless explicitly approved through the EDE Entity-initiated Change Request process consistent with Section IX.c of this Agreement.

The EDE Entity environment must limit the number of concurrent sessions to one (1) session per a single set of credentials/FFE user ID. However, multiple sessions associated with a single set of credentials/FFE user ID that is traceable to a single device/browser is permitted.

- b. Downstream White-Label Third-Party User Arrangement Requirements. Downstream third-party Agent and Broker arrangements may be Downstream White-Label Third-Party User Arrangements for which a Primary EDE Entity enables the third-party Agent or Broker to only make minor branding changes to the Primary EDE Entity's EDE Environment (i.e., adding an Agent's or Broker's logo or name to an EDE Environment). The use of embedding tools and programming techniques, such as iframe technical implementations, which may enable the distortion, manipulation, or modification of the audited and approved EDE Environment and the overall EDE End-User Experience developed by a Primary EDE Entity, are prohibited unless explicitly approved through the EDE Entity-initiated Change Request process consistent with Section IX.c of this Agreement.
- c. Downstream White-Label Third-Party User Arrangement Data Exchange Limited Flexibility. With prior written approval from CMS, Downstream White-Label Third-Party User Arrangements may allow limited data collection from the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal

---

<sup>5</sup> Permissible Upstream EDE Entity arrangements are defined in Sections VIII.f, VIII.g, and VIII.h of this Agreement.

representatives or Authorized Representatives—on the Downstream third-party Agent’s or Broker’s website that can be used in the EDE End-User Experience via a one-way limited data connection to the Primary EDE Entity’s EDE Environment. The following types of limited data collection by the third-party Agent’s or Broker’s website are permissible under this clause: 1) data to determine if a Consumer, Applicant, Qualified Individual, or Enrollee is (or should be) shopping for QHPs, such as basic information to assess potential eligibility for financial assistance, as well as to estimate premiums (e.g., household income, ages of household members, number of household members, and tobacco use status); and 2) data related to the Consumer’s, Applicant’s, Qualified Individual’s, or Enrollee’s service area (e.g., zip code, county, and State).

As part of the EDE-facilitated application and QHP enrollment processes, EDE Entity must not enable or allow the selection of QHPs by a Consumer or Agent/Broker on a third-party website that exists outside of the EDE Entity’s approved DE Environment. This includes pre-populating or pre-selecting a QHP for a Consumer that was selected on a downstream Agent’s/Broker’s website or a lead generator’s website. This prohibition does not extend to websites that are provided, owned, and maintained by entities subject to CMS regulations for QHP display (i.e., Web-brokers and QHP Issuers).

In any limited data collection arrangement, the data must be transmitted securely and in one direction only (i.e., from the downstream Agent or Broker to the Primary EDE Entity’s EDE Environment). EDE Entity must not provide access to Consumer, Applicant, Qualified Individual, or Enrollee data to the third-party Agent or Broker outside of the EDE End-User Experience unless otherwise specified in Sections III.d, III.e, and III.f of this Agreement. Additionally, the Downstream White-Label Third-Party User Arrangement must not involve additional data exchanges beyond what is outlined above as permissible, which takes place in conjunction with the initial redirect prior to the beginning of the EDE End-User Experience on the Primary EDE Entity’s EDE Environment.

- d. Oversight Responsibilities. EDE Entity may only allow third-party Agents, Brokers, and DE Entity Application Assisters who are validly registered with the FFE for the applicable plan year to use its approved EDE Environment. EDE Entity must not provide access to its approved EDE Environment, the EDE End-User Experience or any data obtained via the EDE End-User Experience to an Agent or Broker until the Agent or Broker has completed the process for Agent or Broker Identity Proofing consistent with the requirements in Section IX.r of this Agreement.

## VII. QHP Issuer Use of an EDE Environment.

QHP Issuer EDE Entities, operating as Primary EDE Entities or Upstream EDE Entities, must bind all affiliated Issuer organizations (i.e., HIOS IDs) that use its EDE Environment or EDE End-User Experience—either for Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—use or Agent or Broker use—to the terms and provisions of this Agreement. QHP Issuer EDE Entities must identify all applicable affiliated Issuer organizations that will use its EDE Environment during the



onboarding process in the “Operational and Oversight Information” form provided by CMS<sup>6</sup>. The signatory of this Agreement on behalf of the QHP Issuer EDE Entity must have sufficient authority to execute an agreement with CMS on behalf of the QHP Issuer EDE Entity and all affiliated QHP Issuer organizations that use the QHP Issuer EDE Entity’s EDE Environment or EDE End-User Experience. QHP Issuer EDE Entities must identify all applicable affiliated QHP Issuer organizations in the “Operational and Oversight Information” form provided by CMS.

#### VIII. Audit Requirements.

- a. Operational Readiness Review (“ORR”). In order to receive approval to participate in EDE and utilize an integrated EDE Environment, EDE Entity must contract with one or more independent Auditor(s) consistent with this Agreement’s provisions and applicable regulatory requirements to conduct an ORR, composed of a business requirements audit and a privacy and security audit.<sup>7</sup> EDE Entity must follow the detailed guidance CMS provided in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.<sup>8</sup>

The Auditor must document and attest in the ORR report that EDE Entity’s EDE Environment, including its website and operations, complies with the terms of this Agreement, the ISA, EDE Entity’s respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement), the Framework for the Independent Assessment of Security and Privacy Controls for Enhanced Direct Enrollment Entities,<sup>9</sup> and applicable program requirements. If an EDE Entity will offer its EDE Environment in a State in which a non-English language is spoken by a Limited English Proficient (LEP) population that reaches ten (10) percent or more of the State’s population, as determined in guidance published by the Secretary of HHS,<sup>10</sup> the Auditor conducting EDE Entity’s business requirements audit must also audit the non-English language version of the application user interface (UI) and any critical communications EDE Entity sends Consumers, Applicants, Qualified Individuals, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—in relation to their use of its EDE Environment for compliance with

<sup>6</sup> The Operational and Oversight Information form is available in the PY 2023 DE Documentation Package zip file on CMS zONE at the following link: <https://zone.cms.gov/document/business-audit>.

<sup>7</sup> The Auditor must use NIST SP 800-53A, which describes the appropriate assessment procedure (examine, interview, and test) for each control to evaluate that the control is effectively implemented and operating as intended.

<sup>8</sup> This document is available at the following link: <https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf>.

<sup>9</sup> This document is available at the following link within the Privacy and Security Templates Resources: <https://zone.cms.gov/document/privacy-and-security-audit>.

<sup>10</sup> Guidance and Population Data for Exchanges, Qualified Health Plan Issuers, and Web-Brokers to Ensure Meaningful Access by Limited-English Proficient Speakers Under 45 CFR §155.205(c) and §156.250 (March 30, 2016) <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Language-access-guidance.pdf> and “Appendix A- Top 15 Non-English Languages by State” [https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508\\_update12-20-16.pdf](https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508_update12-20-16.pdf). HHS may release revised guidance. DE Entity should refer to the most current HHS guidance.

applicable CMS requirements. EDE Entity must submit the resulting business requirements and privacy and security audit packages to CMS.

The ORR must detail EDE Entity's compliance with the requirements set forth in Appendix C, including any requirements set forth in CMS guidance referenced in Appendix C.<sup>11</sup> The business requirements and privacy and security audit packages EDE Entity submits to CMS must demonstrate that EDE Entity's Auditor(s) conducted its review in accordance with the review standards set forth in Appendix C and in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.

CMS will approve EDE Entity's EDE Environment only once it has reviewed and approved the business requirements audit and privacy and security audit findings reports. Final approval of EDE Entity's EDE Environment will be evidenced by CMS countersigning the ISA with EDE Entity. Upon receipt of the counter-signed ISA, EDE Entity will be approved to use its approved EDE Environment consistent with applicable regulations, this Agreement, and the ISA.

- b. Identification of Auditor(s) and Subcontractors of Auditor(s). All Auditor(s), including any Auditor(s) that has subcontracted with EDE Entity's Auditor(s), will be considered Downstream or Delegated Entities of EDE Entity pursuant to EDE Entity's respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement) and applicable program requirements. EDE Entity must identify each Auditor it selects, and any subcontractor(s) of the Auditor(s), in Appendix E of this Agreement. EDE Entity must also submit a copy of the signed agreement or contract between the Auditor(s) and EDE Entity to CMS.
- c. Conflict of Interest. For any arrangement between EDE Entity and an Auditor for audit purposes covered by this Agreement, EDE Entity must select an Auditor that is free from any real or perceived conflict(s) of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. EDE Entity must disclose to HHS any financial relationships between the Auditor, and individuals who own or are employed by the Auditor, and individuals who own or are employed by an EDE Entity for which the Auditor is conducting an ORR pursuant to 45 C.F.R. §§ 155.221(b)(4) and (f). EDE Entity must document and disclose any conflict(s) of interest in the form in Appendix F, if applicable.
- d. Auditor Independence and Objectivity. EDE Entity's Auditor(s) must remain independent and objective throughout the audit process for both audits. An Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the EDE Environment and the determination of security and privacy control effectiveness or business requirement compliance. EDE Entity must not take any actions that impair

---

<sup>11</sup> The table in Appendix C is an updated version of Exhibit 2 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."



the independence and objectivity of EDE Entity's Auditor. EDE Entity's Auditor must attest to their independence and objectivity in completing the EDE audit(s).

- e. Required Documentation. EDE Entity must maintain and/or submit the required documentation detailed in Appendix D, including templates provided by CMS, to CMS in the manner specified in Appendix D.<sup>12</sup> Documentation that EDE Entity must submit to CMS (as set forth in Appendix D) will constitute EDE Entity's EDE Application.
- f. Use of an EDE Environment by a QHP Issuer with Minor Branding Deviations (White-Label Issuer Upstream EDE Entity).

A QHP Issuer EDE Entity may use an approved EDE Environment provided by a Primary EDE Entity. If a QHP Issuer EDE Entity implements and uses an EDE Environment that is identical to its Primary EDE Entity's EDE Environment, except for minor deviations for branding or QHP display changes relevant to the Issuer's QHPs, the QHP Issuer EDE Entity is not required to submit a business requirements audit package and privacy and security audit package. CMS refers to a QHP Issuer EDE Entity operating consistent with this Section as a White-Label Issuer Upstream EDE Entity. In all arrangements permitted under this Section, all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions specified in Section III.a of this Agreement must be conducted within the confines of the Primary EDE Entity's approved EDE Environment.

In all arrangements permitted under this Section, the White-Label Issuer Upstream EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265 and 156.1230, operational requirements, this Agreement, and the ISA. Any Primary EDE Entity supplying an EDE Environment to a White-Label Issuer Upstream EDE Entity will be considered a Downstream or Delegated Entity of the White-Label Issuer Upstream EDE Entity. A White-Label Issuer Upstream EDE Entity must identify its Primary EDE Entity in the "Operational and Oversight Information" form provided by CMS. A White-Label Issuer Upstream EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the White-Label Issuer Upstream EDE Entity and the Primary EDE Entity.

- g. Use of an EDE Environment by a QHP Issuer with Additional Functionality or Systems (Hybrid Issuer Upstream EDE Entity).

If a QHP Issuer EDE Entity will implement its own EDE Environment composed, in part, of an approved EDE Environment provided by a Primary EDE Entity and, in

---

<sup>12</sup> The table in Appendix D is a combined version of Exhibits 4 and 7 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

part, of additional functionality or systems implemented by or on behalf of the QHP Issuer EDE Entity, the QHP Issuer EDE Entity may be required to retain an Auditor to conduct part(s) of the ORR relevant to functionalities and systems implemented by the QHP Issuer EDE Entity outside of the Primary EDE Entity's EDE Environment, or in addition to the Primary EDE Entity's approved EDE Environment, and to analyze the effect, if any, of those functionalities and systems on the operations and compliance of the Primary EDE Entity's approved EDE Environment. CMS refers to a QHP Issuer EDE Entity operating consistent with this Section as a Hybrid Issuer Upstream EDE Entity. In this scenario, the Hybrid Issuer Upstream EDE Entity may be required to submit to CMS an ORR audit package that contains the results of the supplemental business requirements audit and/or privacy and security audit, as appropriate, in which the Auditor reviewed the additional functionality or systems implemented by or on behalf of the Hybrid Issuer Upstream EDE Entity. The Hybrid Issuer Upstream EDE Entity may be required to submit to CMS an ORR consisting of the results of its Auditor's review of its implementation of non-inheritable, Hybrid and inheritable but not inherited EDE privacy and security controls. The ORR audit package that contains the results of the business requirements audit and/or privacy and security audit covering additional functionality or systems implemented by or on behalf of the Hybrid Issuer Upstream EDE Entity must demonstrate the Hybrid Issuer Upstream EDE Entity's compliance with applicable regulations, operational requirements, this Agreement, and the ISA. The Hybrid Issuer Upstream EDE Entity does not need to submit the Primary EDE Entity's ORR.

CMS considers any changes to the Primary EDE Entity's approved EDE Environment or the overall EDE End-User Experience—beyond minor deviations for branding or QHP display changes relevant to the Issuer's QHPs—to be the addition of functionality or systems to an approved EDE Environment subject to the requirements of this Section.

CMS has identified the following non-exclusive list as additional functionality that requires a supplemental audit submission:

1. Hybrid Issuer Upstream EDE Entities implementing a single sign-on (SSO) solution must retain an Auditor to conduct a supplemental security and privacy audit and submit the results to CMS consistent with the EDE Guidelines.<sup>13</sup>

In all arrangements permitted under this paragraph, the Hybrid Issuer Upstream EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265, and 156.1230, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265 and 156.1230, operational requirements, this Agreement, and the ISA. Any

---

<sup>13</sup> A Hybrid Issuer Upstream EDE Entity implementing a SSO solution may leverage prior audit results that assessed some or all control requirements listed in Exhibit 14 of the EDE Guidelines, available at the following link: <https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf> if the prior audit was conducted within one year of the date of submission of the audit documentation to CMS.

Primary EDE Entity supplying an EDE Environment to the Hybrid Issuer Upstream EDE Entity will be considered a Downstream or Delegated Entity of the Hybrid Issuer Upstream EDE Entity. A Hybrid Issuer Upstream EDE Entity must identify its Primary EDE Entity in the “Operational and Oversight Information” form provided by CMS . The Hybrid Issuer Upstream EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the Hybrid Issuer Upstream EDE Entity and the Primary EDE Entity. The Primary EDE Entity must identify inheritable Common Controls and Hybrid Controls that the Hybrid Issuer Upstream EDE Entity should leverage. The inherited Common Controls and Hybrid Controls must be documented in the NEE SSP Template and must also be documented as part of the written contract between the Primary EDE Entity and the Hybrid Issuer Upstream EDE Entity.

A Hybrid Issuer Upstream EDE Entity operating under this provision cannot provide access to its EDE Environment to another Issuer or a Hybrid Non-Issuer Upstream EDE Entity.

h. Use of an EDE Environment by a Non-Issuer Entity with Additional Functionality or Systems (Hybrid Non-Issuer Upstream EDE Entity).

If a Hybrid Non-Issuer Upstream EDE Entity will implement its own EDE Environment composed, in part, of an approved EDE Environment provided by a Primary EDE Entity and, in part, of additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer Upstream EDE Entity, the Hybrid Non-Issuer EDE Entity must retain an Auditor to conduct part(s) of the ORR relevant to functionalities and systems implemented by the Hybrid Non-Issuer EDE Entity outside of the Primary EDE Entity’s EDE Environment, or in addition to the Primary EDE Entity’s approved EDE Environment, and to analyze the effect, if any, of those functionalities and systems on the operations and compliance of the Primary EDE Entity’s approved EDE Environment.<sup>14</sup> In this scenario, the Hybrid Non-Issuer EDE Entity must submit an ORR consisting of the results of its Auditor’s review of its implementation of non-inheritable, Hybrid and inheritable but not inherited EDE privacy and security controls. The Hybrid Non-Issuer EDE Entity may also be required to submit to CMS a supplemental ORR audit package that contains the results of any supplemental business requirements and/or privacy and security audits, as appropriate, in which the Auditor reviewed the additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer EDE Entity.<sup>15</sup> The ORR, and

---

<sup>14</sup> With respect to Agents and Brokers regulated by this section as Hybrid Non-Issuer Upstream EDE Entities, these arrangements are distinct and independent from those arrangements regulated under Section VI of this Agreement. An Agent or Broker in a limited data-sharing arrangement consistent with Section VI.c of this Agreement would not necessarily also be subject to the requirements for Hybrid Non-Issuer Upstream EDE Entities under Section VIII.h of this Agreement. The determination of what requirements apply to a particular arrangement will be a fact heavy analysis that takes into account the specific details of the arrangement.

<sup>15</sup> A Hybrid Non-Issuer Upstream EDE Entity may leverage prior audit results that assessed some or all control requirements listed in Exhibit 12 and Exhibit 13 of Appendix A of the EDE Guidelines, if the prior audit was conducted within one year of the date of submission of the audit documentation to CMS. The EDE Guidelines are available at the following link:

<https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf>.

supplemental ORR audit package that contains the results of the supplemental business requirements audit and/or privacy and security audit covering additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer EDE Entity (when required), must demonstrate the Hybrid Non-Issuer EDE Entity's compliance with applicable regulations, operational requirements, this Agreement, and the ISA. The Hybrid Non-Issuer EDE Entity does not need to submit the Primary EDE Entity's ORR.

CMS considers any changes to the Primary EDE Entity's approved EDE Environment or the overall EDE End-User Experience beyond minor deviations for branding to be the addition of functionality or systems to an approved EDE Environment subject to the requirements of this Section. In all arrangements permitted under this paragraph, the Hybrid Non-Issuer EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements as defined in 45 C.F.R. §§ 155.220(c) and 155.221, operational requirements, this Agreement, and the ISA. Any Primary EDE Entity supplying an EDE Environment to the Hybrid Non-Issuer EDE Entity will be considered a Downstream or Delegated Entity of the Hybrid Non-Issuer EDE Entity. A Hybrid Non-Issuer EDE Entity must identify its Primary EDE Entity in the "Operational and Oversight Information" form provided by CMS. The Hybrid Non-Issuer EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the Hybrid Non-Issuer EDE Entity and the Primary EDE Entity. The Primary EDE Entity must identify inheritable Common Controls and Hybrid Controls that the Hybrid Non-Issuer EDE Entity should leverage. The inherited Common Controls and Hybrid Controls must be documented in the NEE SSP Template and must also be documented as part of the written contract between the Primary EDE Entity and the Hybrid Non-Issuer EDE Entity.

Depending on the additional functionality and systems added, the Hybrid Non-Issuer EDE Entity may also need to onboard and register with CMS as a Web-broker. For example, a Hybrid Non-Issuer EDE Entity that hosts its own QHP display or plan shopping experience as part of the EDE End-User Experience must be registered with CMS as a Web-broker.

The QHP display or plan shopping experience displayed in the EDE End-User Experience provided to or operated by a Hybrid Non-Issuer EDE Entity must comply with the requirements of 45 C.F.R. §§ 155.220 and 155.221.

When onboarding, annually during agreement renewal, and upon request, the Hybrid Non-Issuer EDE Entity must provide CMS operational information, including, but not limited to, its Designated Representative's National Producer Number (NPN), State licensure information, and information about its downstream agents/brokers, if applicable. The Designated Representative designated by the Hybrid Non-Issuer EDE

Entity must have completed registration and, if applicable, training with the FFE consistent with 45 C.F.R. § 155.220(d).

A Hybrid Non-Issuer EDE Entity operating under this provision cannot provide access to its EDE Environment to an Issuer or another Hybrid Non-Issuer Upstream EDE Entity.

IX. FFE Eligibility Application and Enrollment Requirements.

- a. FFE Eligibility Application End-State Phases and Phase-Dependent Screener Questions. Appendix G describes each of the three end-state phases for hosting applications using the EDE Pathway (Phase 1, Phase 2, and Phase 3).<sup>16</sup> EDE Entity must select and implement an end-state phase. If EDE Entity has selected application end-state Phase 1 or Phase 2, it must implement the requirements related to phase-dependent screener questions set forth in Appendix C. In addition, EDE Entity must meet any end-state phase-related communications requirements established by CMS. EDE Entity must indicate the phase it has selected in the “Operational and Oversight Information” form provided by CMS.

The business requirements audit package EDE Entity submits to CMS must demonstrate that EDE Entity’s EDE Environment meets all requirements associated with EDE Entity’s selected phase, as set forth in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements,<sup>17</sup> Enhanced Direct Enrollment API Companion Guide,<sup>18</sup> and FFE UI Application Principles for Integration with FFE APIs.<sup>19</sup> EDE Entity must consult CMS prior to switching phases. If EDE Entity decides to switch to a different phase after its Auditor has completed the business requirements audit, EDE Entity’s Auditor must conduct portions of a revised business requirements audit to account for the changes to the EDE Environment necessary to implement the new end-state phase selected by EDE Entity to confirm compliance with all applicable requirements.

- b. EDE Entity Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—Support for Term of Agreement. EDE Entity’s EDE Environment must support Consumer-, Applicant-, Qualified Individual-, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—reported Changes in Circumstances (CiCs), inclusive of SEP CiCs and non-SEP CiCs, and SEPs within EDE Entity’s chosen end-state phase for the full term of this Agreement, as well as supporting re-enrollment application activities. Furthermore, all EDE Entities, regardless of the phase chosen, must support households that wish to enroll in more than one enrollment group. Consistent with the general expectations for EDE requirements—that the EDE requirements are

<sup>16</sup> The table in Appendix G is an updated version of Exhibit 3 in the “Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.”

<sup>17</sup> See *supra* note 8.

<sup>18</sup> The document Enhanced Direct Enrollment API Companion *Guide* is available at the following link: <https://zone.cms.gov/document/api-information>.

<sup>19</sup> The document FFE UI Application Principles for Integration with FFE APIs is available at the following link: <https://zone.cms.gov/document/eligibility-information>.



implemented for and provided to all users of an EDE Environment—Primary EDE Entities must provide the functionalities described in this paragraph for all users of the Primary EDE Entity’s EDE Environment, including any Upstream EDE Entities and their users (e.g., Downstream Agents and Brokers).

If EDE Entity is no longer operating an EDE Environment, EDE Entity must direct the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—to the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]). EDE Entity should take reasonable steps to continue supporting households that have used their EDE Environment in the past to transfer to the new EDE Pathway. CMS suggests that reasonable steps would include: send written notices to Consumers of the steps to create an account/transfer their account to the different Primary EDE Entity, provide the requisite information for them to create an account on that other site or carry their information to a different pathway, and provide a notice on the site that EDE Entity has transitioned its EDE Pathway to a different environment. EDE Entity can go beyond these limited, minimum requirements in easing the Consumer transition to [New Entity] and should follow the EDE Entity-initiated Change Request process as described in Section IX.c of this Agreement for this functionality as appropriate

This provision survives the termination of the Agreement.

- c. EDE Entity-initiated Modifications to EDE Environment (EDE Entity-initiated Change Requests and EDE Entity-initiated Phase Change Requests). EDE Entity must notify CMS immediately if it intends to make any change to its audited or approved EDE Environment, including when EDE Entity opts to change to a different EDE application phase (from its approved or audited EDE phase), consistent with the processes and standards defined by CMS in the Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems.<sup>20</sup> CMS excludes changes made in response to an Auditor’s documented findings (if the findings were submitted to CMS), to CMS technical assistance, or to resolve compliance findings from being subject to the procedures detailed in the Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems.
- d. CMS-initiated Modifications to EDE Program Requirements (CMS-initiated Change Requests). CMS will periodically release updates to EDE program requirements in the form of CMS-initiated Change Requests (CRs); these CMS-initiated CRs are documented in the EDE Change Request Tracker.<sup>21</sup> EDE Entity must provide specified documentation to CMS demonstrating its implementation of applicable CMS-initiated CRs by the CMS-established deadline. EDE Entity must make any CMS-mandated changes within the timeline established by CMS to make such changes. If an EDE Entity does not timely submit documentation of its

<sup>20</sup> The document Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems is available at the following link: <https://zone.cms.gov/document/business-audit>.

<sup>21</sup> The EDE Change Request Tracker is located on CMS zONE: <https://zone.cms.gov/document/business-audit>.

implementation of such CRs, CMS may suspend the non-compliant EDE Entity's access to the EDE Pathway.

- e. Maintenance of an Accurate Testing Environment. EDE Entity must maintain a testing environment that accurately represents the EDE Entity's production environment and integration with the EDE Pathway, including functional use of all EDE APIs. Approved and Prospective Phase Change EDE Entities must maintain at least one testing environment that reflects their current production EDE environments when developing and testing any prospective changes to their production EDE environments. This will require Approved and Prospective Phase Change EDE Entities to develop one or more separate environments (other than production and the testing environment that reflects production) for developing and testing prospective changes to their production environments. Network traffic into and out of all non-production environments is only permitted to facilitate system testing and must be restricted by source and destination access control lists, as well as ports and protocols, as documented in the NEE SSP, SA-11 implementation standard. The EDE Entity shall not submit actual PII to the FFE Testing Environments. The EDE Entity shall not submit test data to the FFE Production Environments. The EDE Entity's testing environments shall be readily accessible to applicable CMS staff and contractors via the Internet to complete CMS audits.

EDE Entity must provide CMS, via the DE Help Desk, with a set of credentials and any additional instructions necessary so that CMS can access the testing environment that reflects the EDE Entity's production environment to complete audits of the EDE Entity's EDE Environment. EDE Entity must ensure that the testing credentials are valid and that all APIs and components of the EDE Environment in the testing environment, including the remote identity proofing (RIDP) services, are accessible for CMS to audit EDE Entity's EDE Environment as determined necessary by CMS.

- f. Penetration Testing. The EDE Entity must conduct penetration testing which examines the network, application, device, and physical security of its EDE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Before conducting the penetration testing, the EDE Entity must execute a Rules of Engagement with their Auditor's penetration testing team. The EDE Entity must also notify their CMS designated technical counterparts on their annual penetration testing schedule a minimum of five (5) business days prior to initiation of the penetration testing using the CMS-provided form.<sup>22</sup> During the penetration testing, the Auditor's testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment. The penetration testing shall be conducted in the lower environment that reflects the EDE Entity's current production environment, consistent with Section IX.e.

---

<sup>22</sup> The Penetration Testing Notification Form is available at the following links:  
<https://zone.cms.gov/document/privacy-and-security-audit>.

- g. Identity Proofing. EDE Entity must meet the identity proofing implementation requirements set forth in Appendix C.
- h. Accurate and Streamlined Eligibility Application UI. EDE Entity must meet the accurate and streamlined eligibility application UI requirements set forth in Appendix C.
- i. Post-Eligibility Application Communications. EDE Entity must provide account management functions for Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—and timely communicate with Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—regarding their application and coverage status. EDE Entity must meet all requirements related to post-eligibility application communications and account management functions set forth in Appendix C. In addition to those requirements, EDE Entity must update and report changes to the Consumer’s, Applicant’s, Qualified Individual’s, or Enrollee’s application and enrollment information to the FFE and must comply with future CMS guidance that elaborates upon EDE Entity’s duties under this Agreement and applicable regulations.
- j. Accurate Information About Exchanges and Consumer, Applicant, Qualified Individual, or Enrollee Communications. EDE Entity must meet the requirements related to providing to Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—accurate information about Exchanges and the Consumer, Applicant, Qualified Individual, or Enrollee communications requirements set forth in Appendix C. In addition, EDE Entity must meet the marketing-related communications requirements defined by CMS in the Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements and the Communications Toolkit.<sup>23</sup>
- k. Documentation of Interactions with Consumer, Applicant, Qualified Individual, or Enrollee Applications or the Exchange. EDE Entity must meet the requirements related to documentation of interactions with Consumer, Applicant, Qualified Individual, or Enrollee applications or the Exchange set forth in Appendix C.
- l. Eligibility Results Testing and Standalone Eligibility Service (SES) Testing. EDE Entity must meet the requirements related to eligibility results testing and SES testing set forth in Appendix C.
- m. API Functional Integration Requirements. EDE Entity must meet the API functional integration requirements set forth in Appendix C.
- n. Application UI Validation. EDE Entity must meet the application UI validation requirements set forth in Appendix C.

---

<sup>23</sup> The Communications Toolkit is stored within the Business Report Template and Toolkits file available at the following link: <https://zone.cms.gov/document/business-audit>.



- o. Section 508-compliant UI. EDE Entity must meet the 508-compliant UI requirements set forth in Appendix C.
- p. Non-English-Language Version of the Application UI and Communication Materials. EDE Entity must translate the Application UI and any critical communications EDE Entity sends Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—in relation to their use of its EDE Environment into any non-English language that is spoken by an LEP population that reaches ten percent or more of the population of the relevant State as set forth in Appendix C.
- q. Correction of Consumer, Applicant, Qualified Individual, or Enrollee Application Information. If EDE Entity identifies issues in its EDE Environment constituting noncompliance with the EDE program requirements as documented in Section IX of this Agreement that may affect the accuracy of a Consumer’s, Applicant’s, Qualified Individual’s, or Enrollee’s Application Information—including the Exchange’s eligibility determination or enrollment status—EDE Entity must notify CMS immediately by email to [directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov). For any such issues identified by EDE Entity or CMS, EDE Entity must provide CMS-requested data on a timeline established by CMS. CMS-requested data includes all data that CMS deems necessary to determine the scope of the issues and identify potentially affected Consumers, Applicants, Qualified Individuals, or Enrollees, including records maintained by EDE Entity consistent with Section IX.k of this Agreement. EDE Entity must provide assistance to CMS to identify the population of Consumers, Applicants, Qualified Individuals, or Enrollees potentially affected by the identified issues. EDE Entity must remedy CMS- or EDE Entity-identified issues in EDE Entity’s EDE Environment in a manner and timeline subject to CMS’ approval. CMS may require that EDE Entity submit updated application information within thirty (30) Days to correct inaccuracies in previously submitted applications. CMS may require that EDE Entity conduct necessary CMS-approved outreach to notify the potentially affected Consumers, Applicants, Qualified Individuals, or Enrollees of any action required by the Consumers, Applicants, Qualified Individuals, or Enrollees, if applicable, and of any changes in eligibility or enrollment status as a result of the issues.
- r. Agent/Broker Identity Proofing Requirements. EDE Entity must implement Agent and Broker identity verification procedures that consist of the following requirements:
  - 1. EDE Entity must provide the User ID of the requester in each EDE API call. For Agents and Brokers, the User ID must exactly match the FFE-assigned User-ID for the Agent or Broker using the EDE Environment or the request will fail FFE User ID validation.<sup>24</sup> As a reminder, for Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—the User ID should be the account User ID for the

---

<sup>24</sup> In order for an Agent or Broker to obtain and maintain an FFE User ID, the Agent or Broker must complete registration and training with the Exchange annually.

Consumer, Applicant, Qualified Individual, or Enrollee or a distinct identifier for the Consumer, Applicant, Qualified Individual, or Enrollee.

2. EDE Entity must identity proof all Agents and Brokers prior to allowing the Agents and Brokers to use the EDE Environment. EDE Entity may conduct identity proofing in one of the following ways:
  - a. Use the FFE-provided Remote Identity Proofing/Fraud Solutions Archive Reporting Service (RIDP/FARS) or a Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS)-approved service to remotely identity-proof Agents and Brokers; OR
  - b. Manually identity-proof Agents and Brokers following the guidelines outlined in the document “Acceptable Documentation for Identity Proofing.”<sup>25</sup>
3. EDE Entity must validate an Agent’s or Broker’s National Producer number (NPN) using the National Insurance Producer Registry (<https://www.nipr.com>) prior to allowing the Agent or Broker to use the EDE Environment.
4. EDE Entity must review the Agent/Broker Suspension and Termination list prior to allowing the Agent or Broker to initially use the EDE Environment.<sup>26</sup>
5. If EDE Entity does not provide Agent or Broker identity proofing functionality consistent with the requirements above, EDE Entity cannot provide access to its EDE Environment to third-party Agents or Brokers. Furthermore, if a Primary EDE Entity does not provide Agent or Broker identity proofing functionality consistent with the requirements above, any Upstream EDE Entities that wish to use the Agent or Broker EDE Pathway must implement an Agent or Broker identity proofing approach consistent with these requirements prior to offering Agents or Brokers access to their EDE Environments. In such cases, the Upstream EDE Entities must contract with an independent Auditor to conduct an audit to evaluate the Agent or Broker identity proofing requirements consistent with this Section, and submit the audit to CMS for approval.
6. EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3.
7. EDE Entity must not permit Agents and Brokers using the EDE Environment to share access control credentials.
- s. Implement Full EDE API Suite of Required Services. EDE Entity must implement the full EDE API suite of required services, regardless of EDE Entity’s chosen application end-state phase. The suite of required services consists of the following APIs: Store ID Proofing, Person Search, Create App, Create App from Prior Year

---

<sup>25</sup> The document Acceptable Documentation for Identity Proofing is available on CMS zONE at the following link: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>.

<sup>26</sup> The Agent/Broker Suspension and Termination List is available at: <https://data.healthcare.gov/ab-suspension-and-termination-list>.

App, Store Permission, Revoke Permission, Get App, Add Member, Remove Member, Update App, Submit App, Get Data Matching Issue (DMI), Get Special Enrollment Period Verification Issue (SVI), Metadata Search, Notice Retrieval, Submit Enrollment, Document Upload, System and State Reference Data, Get Enrollment, Payment Redirect<sup>27</sup>, Update Policy, and Event-Based Processing (EBP). CMS may release additional required or optional APIs during the term of this Agreement. If CMS releases a required API, the change will be considered a CMS-initiated Change Request consistent with Section IX.d of this Agreement.

- t. Maintain Full EDE API Suite of Required Services. In addition to any CMS-initiated Change Requests, CMS may make technical updates to Exchange systems or APIs that may affect EDE Entity's use of the EDE APIs. In order to maintain a functional EDE Environment and avoid errors or discrepancies when submitting data to and receiving data from the Exchange, EDE Entity must maintain an EDE Environment that implements changes as needed and documented in EDE technical documentation provided by CMS.<sup>28</sup>
- u. Health Reimbursement Arrangement (HRA) Offer Disclaimer. EDE Entity must implement disclaimers for Qualified Individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the Qualified Individuals consistent with CMS guidance. Disclaimers for various scenarios are detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.<sup>29</sup>
- v. Inactive, Approved Primary EDE Entities to Demonstrate Operational Readiness and Compliance. In order for an approved Primary EDE Entity to maintain status as an approved Primary EDE Entity during the annual renewal process for this Agreement, EDE Entity must demonstrate a history of enrollments completed via EDE during the term of the prior year's Agreement if the approved Primary EDE Entity has been approved for at least one year as determined by the date of the initial approval of the Primary EDE Entity and initial execution of the ISA. If the EDE Entity has been approved for at least one year and does not have a history of enrollments completed via EDE during the term of the prior year's Agreement, EDE Entity must demonstrate operational readiness and compliance with applicable requirements as documented in the EDE Guidelines in order to continue to participate as an approved Primary EDE Entity. Under this section, CMS may withhold execution of the subsequent plan year's Agreement and ISA or delay approval of an Upstream EDE Entity until EDE Entity has demonstrated operational readiness and compliance with applicable requirements to CMS's satisfaction.

---

<sup>27</sup> For information on exceptions to the requirement for EDE Entities to integrate with the Payment Redirect API, see Section 13.3, Payment Redirect Integration Requirements, of the EDE API Companion Guide, available at the following link: <https://zone.cms.gov/document/api-information>.

<sup>28</sup> EDE APIs technical documentation is available on CMS zONE at the following link: <https://zone.cms.gov/document/api-information>.

<sup>29</sup> The document Direct Enrollment API Specs is available on CMS zONE at the following link: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.

X. Miscellaneous.

- a. Notice. All notices to Parties specifically required under this Agreement shall be given in writing and shall be delivered as follows:

If to CMS:

By email:

[directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov)

By mail:

Centers for Medicare & Medicaid Services (CMS)

Center for Consumer Information and Insurance Oversight (CCIIO)

Attn: Office of the Director

Room 739H

200 Independence Avenue, SW

Washington, DC 20201

If to EDE Entity, to EDE Entity's primary contact's email address on record.

Notices sent by hand or overnight courier service, or mailed by certified or registered mail, shall be deemed to have been given when received; notices sent by email shall be deemed to have been given when the appropriate confirmation of receipt has been received; provided that notices not given on a business day (i.e., Monday-Friday excluding federal holidays) between 9:00 a.m. and 5:00 p.m. local time where the recipient is located shall be deemed to have been given at 9:00 a.m. on the next business day for the recipient. A Party to this Agreement may change its contact information for notices and other communications by providing written notice of such changes in accordance with this provision. Such notice should be provided thirty (30) Days in advance of such change, unless circumstances warrant a shorter timeframe.

- b. Assignment and Subcontracting. Except as otherwise provided in this Section, EDE Entity shall not assign this Agreement in whole or in part, whether by merger, acquisition, consolidated, reorganization, or otherwise any portion of the services to be provided by EDE Entity under this Agreement without the express, prior written consent of CMS, which consent may be withheld, conditioned, granted, or denied in CMS' sole discretion. EDE Entity must provide written notice at least thirty (30) Days prior to any such proposed assignment, including any change in ownership of EDE Entity or any change in management or ownership of the EDE Environment. Notwithstanding the foregoing, CMS does not require prior written consent for subcontracting arrangements that do not involve the operation, management, or control of the EDE Environment. EDE Entity must report all subcontracting arrangements on its annual Operational and Oversight Information form during the annual EDE Agreement Renewal process and submit revisions annually thereafter. EDE Entity shall assume ultimate responsibility for all services and functions described under this Agreement, including those that are subcontracted to other entities, and must ensure that subcontractors will perform all functions in accordance with all applicable requirements. EDE Entity shall further be subject to such oversight and enforcement actions for functions or activities performed by subcontractors as may otherwise be provided for under applicable law and program requirements,

including EDE Entity's respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement). Notwithstanding any subcontracting of any responsibility under this Agreement, EDE Entity shall not be released from any of its performance or compliance obligations hereunder, and shall remain fully bound to the terms and conditions of this Agreement as unaltered and unaffected by such subcontracting.

If EDE Entity attempts to make an assignment, subcontracting arrangement or otherwise delegate its obligations hereunder in violation of this provision, such assignment, subcontract, or delegation shall be deemed void *ab initio* and of no force or effect, and EDE Entity shall remain legally bound hereto and responsible for all obligations under this Agreement.

- c. Use of the FFE Web Services. EDE Entity will only use a CMS-approved EDE Environment when accessing the APIs and web services that facilitate EDE functionality to enroll Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix H.
- d. Incident Reporting Procedures: EDE Entity must implement Incident and Breach Handling procedures as required by the NEE SSP and that are consistent with CMS's Incident and Breach Notification Procedures. Such policies and procedures must identify EDE Entity's Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents or Breaches and provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes. EDE Entity agrees to report any Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at [cms\\_it\\_service\\_desk@cms.hhs.gov](mailto:cms_it_service_desk@cms.hhs.gov) within 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.
- e. Survival. EDE Entity's obligation under this Agreement to protect and maintain the privacy and security of PII and any other obligation of EDE Entity in this Agreement which, by its express terms or nature and context is intended to survive expiration or termination of this Agreement, shall survive the expiration or termination of this Agreement.
- f. Severability. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement. In the event that any provision of this Agreement is determined to be invalid, unenforceable or otherwise illegal, such provision shall be deemed restated, in accordance with applicable law, to reflect as nearly as possible the original intention of the Parties, and the remainder of the Agreement shall be in full force and effect.

- g. Disclaimer of Joint Venture. Neither this Agreement nor the activities of EDE Entity contemplated by and under this Agreement shall be deemed or construed to create in any way any partnership, joint venture, or agency relationship between CMS and EDE Entity. Neither Party is, nor shall either Party hold itself out to be, vested with any power or right to bind the other Party contractually or to act on behalf of the other Party, except to the extent expressly set forth in the ACA and the regulations codified thereunder, including as codified at 45 C.F.R. part 155.
- h. Remedies Cumulative. No remedy herein conferred upon or reserved to CMS under this Agreement is intended to be exclusive of any other remedy or remedies available to CMS under operative law and regulation, and each and every such remedy, to the extent permitted by law, shall be cumulative and in addition to any other remedy now or hereafter existing at law or in equity or otherwise.
- i. Records. EDE Entity shall maintain all records that it creates in the normal course of its business in connection with activity under this Agreement for the term of this Agreement in accordance with 45 C.F.R. §§ 155.220(c)(3)(i)(E) or 156.705(c), as applicable. Subject to applicable legal requirements and reasonable policies, such records shall be made available to CMS to ensure compliance with the terms and conditions of this Agreement. The records shall be made available during regular business hours at EDE Entity's offices, and CMS's review shall not interfere unreasonably with EDE Entity's business activities. This clause survives the expiration or termination of this Agreement.
- j. Compliance with Law. EDE Entity covenants and agrees to comply with any and all applicable laws, statutes, regulations, or ordinances of the United States of America and any Federal Government agency, board, or court that are applicable to the conduct of the activities that are the subject of this Agreement, including, but not necessarily limited to, any additional and applicable standards required by statute, and any regulations or policies implementing or interpreting such statutory provisions hereafter issued by CMS. In the event of a conflict between the terms of this Agreement and any statutory, regulatory, or sub-regulatory guidance released by CMS, the requirement that constitutes the stricter, higher, or more stringent level of compliance shall control.
- k. Governing Law and Consent to Jurisdiction. This Agreement will be governed by the laws and common law of the United States of America, including without limitation such regulations as may be promulgated by HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. EDE Entity further agrees and consents to the jurisdiction of the Federal Courts located within the District of Columbia and the courts of appeal therefrom, and waives any claim of lack of jurisdiction or *forum non conveniens*.
- l. Amendment. CMS may amend this Agreement for purposes of reflecting changes in applicable law or regulations, with such amendments taking effect upon thirty (30) Days' written notice to EDE Entity ("CMS notice period"), unless circumstances warrant an earlier effective date. Any amendments made under this provision will only have prospective effect and will not be applied retrospectively. EDE Entity may reject such amendment by providing to CMS, during the CMS notice period, written



notice of its intent to reject the amendment (“rejection notice period”). Any such rejection of an amendment made by CMS shall result in the termination of this Agreement upon expiration of the rejection notice period.

- m. Audit and Compliance Review. EDE Entity agrees that CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees may conduct compliance reviews or audits, which includes the right to interview employees, contractors, and business partners of EDE Entity and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of EDE Entity’s compliance with the requirements of this Agreement and applicable program requirements upon reasonable notice to EDE Entity, during EDE Entity’s regular business hours, and at EDE Entity’s regular business location. These audit and review rights include the right to audit EDE Entity’s compliance with and implementation of the privacy and security requirements under this Agreement, the ISA, EDE Entity’s respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement), and applicable program requirements. EDE Entity further agrees to allow reasonable access to the information and facilities, including, but not limited to, EDE Entity website testing environments, requested by CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees for the purpose of such a compliance review or audit. EDE Entity is also responsible for ensuring cooperation by its Downstream and Delegated Entities, including EDE Entity’s subcontractors and assignees, as well as the Auditor(s) and any of its subcontractors, with audits and reviews. CMS may suspend or terminate this Agreement if EDE Entity does not comply with such a compliance review request within seven (7) business days. If any of EDE Entity’s obligations under this Agreement are delegated to other parties, the EDE Entity’s agreement with any Downstream and Delegated Entities must incorporate this Agreement provision.

This clause survives the expiration or termination of this Agreement.

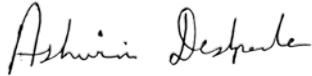
- n. Access to the FFEs and SBE-FPs. EDE Entity; its Downstream and Delegated Entities, including downstream Agents/Brokers; and its assignees or subcontractors—including, employees, developers, agents, representatives, or contractors—cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to EDE Entity’s systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through virtual private networks (VPNs).

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

This “Agreement between EDE Entity and the Centers for Medicare & Medicaid Services for the Individual Market Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform” has been signed and executed by:

**TO BE FILLED OUT BY EDE ENTITY**

The undersigned is an authorized official of EDE Entity who is authorized to represent and bind EDE Entity for purposes of this Agreement. The undersigned attests to the accuracy and completeness of all information provided in this Agreement.



10/20/2023

Signature of Authorized Official of EDE Entity

Date

Ashwini Deshpande, CEO


Printed Name and Title of Authorized Official of EDE Entity

TrueCoverage LLC(dba) Inshura

EDE Entity Name

04.TCL.MD\*.347.921

EDE Entity Partner IDs



Signature of Privacy Officer

Sarika Balakrishnan, Manager

Printed Name and Title of Privacy Officer

Suite No.100, Bldg 3

2400 Louisiana Blvd NE,

Albuquerque, NM 87110

EDE Entity Address

**REDACTED**

EDE Entity Contact Number



Centers for Medicare & Medicaid Services

---

**FOR CMS**

The undersigned are officials of CMS who are authorized to represent and bind CMS for purposes of this Agreement.

**Jeffrey Grant -S** Digitally signed by Jeffrey Grant -S  
Date: 2023.10.19 15:50:03 -04'00'

---

**Jeffrey D. Grant**

**Date**

Deputy Director for Operations

Center for Consumer Information and Insurance Oversight

Centers for Medicare & Medicaid Services

**George C. Hoffmann -S** Digitally signed by George C. Hoffmann -S  
Date: 2023.10.30 07:12:02 -04'00'

---

**George C. Hoffmann**

**Date**

CMS Deputy CIO

Deputy Director, Office of Information Technology (OIT)

Centers for Medicare & Medicaid Services (CMS)

## **APPENDIX A: PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS FOR NON-EXCHANGE ENTITIES**

---

Federally-facilitated Exchanges (“FFE”) will enter into contractual agreements with all Non-Exchange Entities, including EDE Entities, that gain access to Personally Identifiable Information (“PII”) exchanged with the FFEs (including FF-SHOPs) and State-based Exchanges on the Federal Platform (“SBE-FPs”) (including SBE-FP-SHOPs), or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals’ legal representatives or Authorized Representatives. This Agreement and its appendices govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by EDE Entities in the context of the FFEs and SBE-FPs. In signing this contractual Agreement, in which this Appendix A has been incorporated, EDE Entities agree to comply with the security and privacy standards and implementation specifications outlined in the Non-Exchange Entity System Security and Privacy Plan (“NEE SSP”)<sup>30</sup> and Section A<sup>31</sup> below while performing the Authorized Functions outlined in their respective Agreement(s) with CMS.

The standards documented in the NEE SSP and Section A below are established in accordance with Section 1411(g) of the Affordable Care Act (“ACA”) (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 (“FISMA”) (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the principles in 45 C.F.R. §§ 155.260(a)(1) through (a)(6). All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

### **A. NON-EXCHANGE ENTITY PRIVACY AND SECURITY IMPLEMENTATION SPECIFICATIONS**

Non-Exchange Entities must meet privacy and security implementation specifications that are consistent with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 P.L. 104-191 and the Privacy Act of 1974, 5 U.S.C. § 552a, including:

- (1) Openness and Transparency. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, and Enrollees and their PII.
  - a. Standard: Privacy Notice Statement. Prior to collecting PII, the Non-Exchange Entity must provide a notice that is prominently and conspicuously displayed on a public-facing website, if applicable, or on the electronic and/or paper form the

---

<sup>30</sup> The NEE SSP template is located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

<sup>31</sup> Section A contains excerpts from the NEE SSP of two requirements for ease of reference. This does not alter the need to comply with other applicable EDE Entity requirements, including those outlined within 45 C.F.R. § 155.260(a)(1) through (a)(6) or the NEE SSP.

Non-Exchange Entity will use to gather and/or request PII. The EDE Entity must comply with any additional standards and implementation specifications described in NEE SSP TR-1: Privacy Notice.

i. Implementation Specifications.

1. The statement must be written in plain language and provided in a manner that is timely and accessible to people living with disabilities and with limited English proficiency.
2. The statement must contain at a minimum the following information:
  - a. Legal authority to collect PII;
  - b. Purpose of the information collection;
  - c. To whom PII might be disclosed, and for what purposes;
  - d. Authorized uses and disclosures of any collected information;
  - e. Whether the request to collect PII is voluntary or mandatory under the applicable law; and
  - f. Effects of non-disclosure if an individual chooses not to provide the requested information.
3. The Non-Exchange Entity shall maintain its Privacy Notice Statement content by reviewing and revising as necessary on an annual basis, at a minimum, and before or as soon as possible after any change to its privacy policies and procedures.
4. If the Non-Exchange Entity operates a website, it shall ensure that descriptions of its privacy and security practices, and information on how to file complaints with CMS and the Non-Exchange Entity, are publicly available through its website.<sup>32</sup>

(2) Individual Choice. In keeping with the standards and implementation specifications used by the FFEs, the Non-Exchange Entity should ensure that Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—are provided a reasonable opportunity and capability to make informed decisions about the creation, collection, disclosure, access, maintenance, storage, and use of their PII.

- a. Standard: Informed Consent. The Non-Exchange Entity may create, collect, disclose, access, maintain, store, and use PII from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—only for the functions and purposes listed in the

---

<sup>32</sup> CMS recommends that EDE Entities direct consumers, who are seeking to file a complaint, to the Secretary of the U.S. Department of Health and Human Services, 200 Independence Ave, S.W., Washington, D.C. 20201. Call (202) 619-0257 (or toll free (877) 696-6775) or go to the website of the Office for Civil Rights, [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa).

Privacy Notice Statement and any relevant agreements in effect as of the time the information is collected, unless the FFE, SBE-FP, or Non-Exchange Entity obtains informed consent from such individuals. The EDE Entity must comply with any additional standards and implementation specifications described in NEE SSP IP-1: Consent.

i. Implementation Specifications.

1. The Non-Exchange Entity must obtain informed consent from individuals for any use or disclosure of information that is not permissible within the scope of the Privacy Notice Statement and any relevant agreements that were in effect as of the time the PII was collected. Such consent must be subject to a right of revocation.
2. Any such consent that serves as the basis of a use or disclosure must:
  - a. Be provided in specific terms and in plain language,
  - b. Identify the entity collecting or using the PII, and/or making the disclosure,
  - c. Identify the specific collections, use(s), and disclosure(s) of specified PII with respect to a specific recipient(s), and
  - d. Provide notice of an individual's ability to revoke the consent at any time.
3. Consent documents must be appropriately secured and retained for ten (10) Years.

## APPENDIX B: DEFINITIONS

---

This Appendix defines terms that are used in the Agreement and other Appendices. Any capitalized term used in the Agreement that is not defined therein or in this Appendix has the meaning provided in 45 C.F.R. § 155.20.

- (1) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 C.F.R. § 155.20.
- (2) **Affordable Care Act (ACA)** means the Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), which are referred to collectively as the Affordable Care Act or ACA.
- (3) **Agent** or **Broker** has the meaning set forth in 45 C.F.R. § 155.20.
- (4) **Agent or Broker Direct Enrollment (DE) Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.
- (5) **Applicant** has the meaning set forth in 45 C.F.R. § 155.20.
- (6) **Auditor** means a person or organization that meets the requirements set forth in this Agreement and contracts with a Direct Enrollment (DE) Entity for the purposes of conducting an Operational Readiness Review (ORR) in accordance with 45 C.F.R. §§ 155.221(b)(4) and (f), this Agreement and CMS-issued guidance.
- (7) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in the Agreement that incorporates this Appendix B.
- (8) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 C.F.R. § 155.227.
- (9) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information for anything other than an authorized purpose.
- (10) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (CMS).
- (11) **Classic Direct Enrollment (Classic DE)** means, for purposes of this Agreement, the original version of Direct Enrollment, which utilizes a double redirect from a Direct Enrollment (DE) Entity's website to HealthCare.gov where the eligibility application is submitted and an eligibility determination is received, and back to the DE Entity's

website for QHP shopping and plan selection consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(i), 155.221, 156.265 and/or 156.1230(b).

- (12) **Classic Direct Enrollment Pathway (Classic DE Pathway)** means, for the purposes of this Agreement, the application and enrollment process used by Direct Enrollment (DE) Entities for Classic DE.
- (13) **CMS** means the Centers for Medicare & Medicaid Services.
- (14) **CMS Companion Guides** means a CMS-authored guide, available on the CMS website, which is meant to be used in conjunction with and supplement relevant implementation guides published by the Accredited Standards Committee.
- (15) **CMS Data Services Hub (Hub)** is the CMS Federally-managed service to interface data among connecting entities, including HHS, certain other Federal agencies, and State Medicaid agencies.
- (16) **CMS Data Services Hub Web Services (Hub Web Services)** means business and technical services made available by CMS to enable the determination of certain eligibility and enrollment or federal financial payment data through the Federally-facilitated Exchange (FFE) website, including the collection of personal and financial information necessary for Consumer, Applicant, Qualified Individual, or Enrollee account creations; Qualified Health Plan (QHP) application submissions; and Insurance Affordability Program eligibility determinations.
- (17) **Common Control** means a security or privacy control whose implementation results in a security or privacy capability that is inheritable by multiple information systems being served by the Primary EDE Entity.
- (18) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (QHP) offered through an Exchange or Insurance Affordability Program, or whom an Agent or Broker (including Web-brokers) registered with the FFE, Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a QHP, applying for APTC and CSRs, and/or completing enrollment in a QHP through the FFEs or State-based Exchanges on the Federal Platform (SBE-FPs) for individual market coverage.
- (19) **Cost-sharing Reductions (CSRs)** has the meaning set forth in 45 C.F.R. § 155.20.
- (20) **Customer Service** means assistance regarding eligibility and Health Insurance Coverage provided to a Consumer, Applicant, Qualified Individual, and Enrollee, including, but not limited to, responding to questions and complaints; providing information about eligibility; applying for APTC and/or CSRs, and Health Insurance Coverage; and explaining enrollment processes in connection with the FFEs or SBE-FPs.
- (21) **Day or Days** means calendar days, unless otherwise expressly indicated in the relevant provision of the Agreement that incorporates this Appendix B.

- (22) **Delegated Entity** means, for purposes of this Agreement, any party, including an Agent or Broker, that enters into an agreement with an Enhanced Direct Enrollment (EDE Entity) to provide administrative or other services to or on behalf of the EDE Entity or to provide administrative or other services to Consumers and their dependents.
- (23) **Designated Privacy Official** means a contact person or office responsible for receiving complaints related to Breaches or Incidents, able to provide further information about matters covered by the Privacy Notice statement, responsible for the development and implementation of the privacy policies and procedures of the Non-Exchange Entity, and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy of Personally Identifiable Information (PII).
- (24) **Designated Representative** means an Agent or Broker that has the legal authority to act on behalf of the Web-broker.
- (25) **Designated Security Official** means a contact person or office responsible for the development and implementation of the security policies and procedures of the Non-Exchange Entity and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the security of Personally Identifiable Information (PII).
- (26) **Direct Enrollment (DE)** means, for the purposes of this Agreement, the process by which a Direct Enrollment (DE) Entity may assist an Applicant or Enrollee with enrolling in a QHP in a manner that is considered through the Exchange consistent with applicable requirements in 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or 156.1230. Direct Enrollment is the collective term used when referring to both Classic Direct Enrollment and Enhanced Direct Enrollment.
- (27) **Direct Enrollment (DE) Entity** has the meaning set forth in 45 C.F.R. § 155.20.
- (28) **Direct Enrollment Entity Application Assister** has the meaning set forth in 45 C.F.R. § 155.20.
- (29) **Direct Enrollment (DE) Environment** means an information technology application or platform provided, owned, and maintained by a DE Entity through which a DE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.
- (30) **Downstream Entity** means, for purposes of this Agreement, any party, including an Agent or Broker, that enters into an agreement with a Delegated Entity or with another Downstream Entity for purposes of providing administrative or other services related to the agreement between the Delegated Entity and the Enhanced Direct Enrollment (EDE) Entity. The term “Downstream Entity” is intended to refer to the



entity that directly provides administrative services or other services to or on behalf of the EDE Entity or that provides administrative or other services to Consumers and their dependents.

- (31) **Downstream White-Label Third-Party User Arrangements** means an arrangement between an Agent or Broker and a Primary EDE Entity to use the Primary EDE Entity's EDE Environment. In this arrangement, a Primary EDE Entity enables the Downstream White-Label Agent or Broker to only make minor branding changes to the Primary EDE Entity's EDE Environment.
- (32) **Enhanced Direct Enrollment (EDE)** means, for purposes of this Agreement, the version of Direct Enrollment which allows Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—to complete all steps in the application, eligibility and enrollment processes on an EDE Entity's website consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(ii), 155.221, 156.265 and/or 156.1230(b) using application programming interfaces (APIs) as provided, owned, and maintained by CMS to transfer data between the Exchange and the EDE Entity's website.
- (33) **Enhanced Direct Enrollment (EDE) End-User Experience** means all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions under this Agreement.
- (34) **Enhanced Direct Enrollment (EDE) Entity** means a DE Entity that has been approved by CMS to use the EDE Pathway. This term includes both Primary EDE Entities and Upstream EDE Entities.
- (35) **Enhanced Direct Enrollment (EDE) Environment** means an information technology application or platform provided, owned, and maintained by an EDE Entity through which an EDE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.
- (36) **Enhanced Direct Enrollment (EDE) Pathway** means the APIs and functionality comprising the systems that enable EDE as provided, owned, and maintained by CMS.
- (37) **Enrollee** has the meaning set forth in 45 C.F.R. § 155.20.
- (38) **Exchange** has the meaning set forth in 45 C.F.R. § 155.20.
- (39) **Federally-facilitated Exchange (FFE)** means an **Exchange (or Marketplace)** established by the Department of Health and Human Services (HHS) and operated by



CMS under Section 1321(c)(1) of the ACA for individual market coverage.  
**Federally-facilitated Marketplaces (FFMs)** has the same meaning as FFEs.

- (40) **Health Insurance Coverage** has the meaning set forth in 45 C.F.R. § 155.20.
- (41) **Health Insurance Portability and Accountability Act (HIPAA)** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and its implementing regulations.
- (42) **Health Reimbursement Arrangement (HRA)** has the meaning set forth in 45 C.F.R. § 146.123(c).
- (43) **HHS** means the United States Department of Health & Human Services.
- (44) **Hybrid Control** means those controls for which both a Primary EDE Entity and its Upstream EDE Entity share the responsibility of implementing the full control objectives and implementation standards. Hybrid Controls refer to arrangements in which an Upstream EDE Entity information system inherits part of a control from a Primary EDE Entity, with the remainder of the control provided by the Upstream EDE Entity leveraging the Primary EDE Entity's EDE Environment.
- (45) **Hybrid Issuer Upstream EDE Entity** means a QHP Issuer EDE Entity that uses the EDE Environment of a Primary EDE Entity and adds functionality or systems to the Primary EDE Entity's EDE Environment such that the Primary EDE Entity's EDE Environment or overall EDE End-User Experience is modified beyond minor deviations for branding or QHP display changes relevant to the Issuer's QHPs.
- (46) **Hybrid Non-Issuer Upstream EDE Entity** means an Agent, Broker, or Web-broker under 45 C.F.R. §§ 155.220(c)(3) and 155.221 that uses the EDE Environment of a Primary EDE Entity and adds functionality or systems to the Primary EDE Entity's EDE Environment such that the Primary EDE Entity's EDE Environment or overall EDE End-User Experience is modified beyond minor branding changes.
- (47) **Incident, or Security Incident**, has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and means an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- (48) **Insurance Affordability Program** means a program that is one of the following:
  - (1) A State Medicaid program under title XIX of the Social Security Act.
  - (2) A State Children's Health Insurance Program (CHIP) under title XXI of the Social Security Act.
  - (3) A State basic health program established under section 1331 of the Care Act.

- (4) A program that makes coverage in a Qualified Health Plan (QHP) through the Exchange with APTC established under section 36B of the Internal Revenue Code available to Qualified Individuals.
- (5) A program that makes available coverage in a QHP through the Exchange with CSRs established under section 1402 of the ACA.
- (49) **Interconnection Security Agreement** means a distinct agreement that outlines the technical solution and security requirements for an interconnection between CMS and EDE Entity.
- (50) **Issuer** has the meaning set forth in 45 C.F.R. § 144.103.
- (51) **Non-Exchange Entity** has the meaning at 45 C.F.R. § 155.260(b)(1), including, but not limited to, Qualified Health Plan (QHP) Issuers, Navigators, Agents, Brokers, and Web-brokers.
- (52) **OMB** means the Office of Management and Budget.
- (53) **Operational Readiness Review (ORR)** means an audit conducted under 45 C.F.R. §§ 155.221(b)(4) and (f) and includes the reports submitted by an EDE Entity detailing its compliance with CMS requirements and readiness to implement and use the EDE Environment.
- (54) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- (55) **Primary EDE Entity** means an entity that has developed and maintains an EDE Environment. A Primary EDE Entity may provide its EDE Environment to an Upstream EDE Entity and the Primary EDE Entity may provide an EDE Environment for use by Consumers, Applicants, Qualified Individuals, Enrollees—or these individuals' legal representatives or Authorized Representatives—, Agents, Brokers, or DE Entity Application Assisters.
- (56) **Prospective EDE Entity** means an entity that has not yet been approved by CMS to use the EDE Pathway.
- (57) **Prospective Phase Change EDE Entity** means a Primary EDE Entity already approved to use the EDE Pathway that is seeking to implement a new eligibility application phase using the EDE Entity-initiated Change Request process.
- (58) **Qualified Health Plan (QHP)** has the meaning set forth in 45 C.F.R. § 155.20.
- (59) **Qualified Health Plan (QHP) Issuer** has the meaning set forth in 45 C.F.R. § 155.20.
- (60) **Qualified Health Plan (QHP) Issuer Agreement** means the QHP Certification Agreement and Privacy and Security Agreement Between QHP Issuer and CMS.

- (61) **Qualified Health Plan (QHP) Direct Enrollment (DE) Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.
- (62) **Qualified Individual** has the meaning set forth in 45 C.F.R. § 155.20.
- (63) **Rules of Engagement (ROE)** means the detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test and gives the test team authority to conduct defined activities without the need for additional permissions.
- (64) **Special Enrollment Period (SEP)** has the meaning set forth in 45 C.F.R. § 155.20.
- (65) **Standalone Eligibility Service (SES)** means a suite of application program interfaces (APIs) that will allow an EDE Entity to create, update, submit, and ultimately retrieve eligibility results for an application.
- (66) **State** means the State that has licensed the Agent, Broker, Web-broker, or Issuer that is a party to this Agreement and in which the Agent, Broker, Web-broker, or Issuer is operating.
- (67) **State-based Exchange (SBE)** means an Exchange established by a State that receives approval to operate under 45 C.F.R. § 155.105. **State-based Marketplace (“SBM”)** has the same meaning as SBE.
- (68) **State-based Exchange on the Federal Platform (SBE-FP)** means an Exchange established by a State that receives approval under 45 C.F.R. § 155.106(c) to utilize the Federal platform to support select eligibility and enrollment functions. **State-based Marketplace on the Federal Platform (“SBM-FP”)** has the same meaning as SBE-FP.
- (69) **Streamlined Eligibility Application User Interface (UI)** means the application UI on HealthCare.gov available for Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—with non-complex eligibility application responses determined by an initial set of eligibility questions for determining the complexity of an Applicant’s eligibility profile.
- (70) **Upstream EDE Entity** means an EDE Entity that uses the EDE Environment of a Primary EDE Entity and meets the definition of a Hybrid Issuer Upstream EDE Entity; a Hybrid Non-Issuer Upstream EDE Entity; or a White-Label Issuer Upstream EDE Entity.
- (71) **Web-broker** has the meaning set forth in 45 C.F.R. § 155.20.
- (72) **Web-broker Agreement** means the Agreement between a Web-broker and CMS for the FFEs and SBE-FPs.
- (73) **White-Label Issuer Upstream EDE Entity** means a QHP Issuer that uses the EDE Environment of a Primary EDE Entity without modifications beyond minor branding changes or QHP display changes.

- (74) **Workforce** means a Non-Exchange Entity's employees, contractors, subcontractors, officers, directors, agents, representatives, and any other individual who may create, collect, disclose, access, maintain, store, or use PII in the performance of his or her duties.



## APPENDIX C: EDE BUSINESS REQUIREMENTS<sup>33</sup>

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

Review Category	Requirement and Audit Standard
<b>Consumer Identity Proofing Implementation</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> The EDE Entity must conduct identity proofing (ID proofing) for Consumers entering the EDE pathway for enrollments through both Consumer and in-person Agent and Broker pathways.<sup>34</sup> The EDE Entity must conduct ID proofing prior to submitting a Consumer's application to the Exchange. If an EDE Entity is unable to complete ID proofing of the Consumer, the EDE Entity may either direct the Consumer to the classic DE (i.e., double-redirect) pathway or direct the Consumer to the Exchange (HealthCare.gov or the Exchange Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]).               <ul style="list-style-type: none"> <li>– <u>Remote ID Proofing/Fraud Solutions Archive Reporting Services (RIDP/FARS) or Third-Party ID Proofing Service:</u> CMS will make the Exchange RIDP and FARS services available for the EDE Entity to use when remote ID proofing Consumers for the Consumer pathway (i.e., when a Consumer is interacting directly with the EDE environment without the assistance of an individual Agent or Broker). If an EDE Entity uses the Exchange RIDP service, it must use the RIDP service only after confirming the Consumer is seeking coverage in a State supported by the Exchange/Federal Platform, and only after confirming the Consumer is eligible for the EDE Entity's chosen phase. However, CMS does not require that EDE Entities use the Exchange RIDP and FARS services, specifically, to complete ID proofing. An EDE Entity may instead opt to use a third-party ID proofing service for ID proofing in the Consumer pathway. If an EDE Entity uses a third-party identity proofing service, the service must be Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS)-approved, and the EDE Entity must be able to produce documentary evidence that each Applicant has been successfully ID proofed. Documentation related to a third-party service could be requested in an audit or investigation by CMS (or its designee), pursuant to the EDE Business Agreement. Applicants do not need to be ID proofed on subsequent interactions with the EDE Entity if the Applicant creates an account (i.e., username and password) on the EDE Entity's website, and the EDE Entity tracks that ID proofing has occurred when the Applicant's account was created.</li> <li>– <u>Manual ID Proofing in the In-Person Agent and Broker Pathway:</u> EDE Entities may also offer a manual ID proofing process. Consumers being ID proofed in the in-person Agent and Broker pathway (i.e., when an Agent or Broker is working with a Consumer and conducting ID proofing in-person, rather than remotely) must be ID proofed following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE (<a href="https://zone.cms.gov/document/api-information">https://zone.cms.gov/document/api-information</a>).</li> </ul> </li> </ul>

<sup>33</sup> The table in Appendix C is an updated version of Exhibit 2 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

<sup>34</sup> Consumer pathway means the workflow, UI, and accompanying APIs for an EDE environment that is intended for use by a Consumer to complete an eligibility application and enrollment. Agent and Broker pathway means the workflow, UI, and accompanying APIs for an EDE environment that is intended for use by an Agent or Broker to assist a Consumer with completing an eligibility application and enrollment.

Review Category	Requirement and Audit Standard
<b>Consumer Identity Proofing Implementation (continued)</b>	<ul style="list-style-type: none"> <li>– For the Consumer pathway, the EDE Entity must provide the User ID of the requester in the header for each EDE API call. For the Consumer pathway, the User ID should be the User ID for the Consumer’s account on the EDE Entity’s site, or some other distinct identifier the EDE Entity assigns to the Consumer.</li> <li>– Additionally, if an EDE Entity is using the Fetch Eligibility API, the same User ID requirements apply. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID.</li> <li>▪ Review Standard: <ul style="list-style-type: none"> <li>– If an EDE Entity uses the Exchange RIDP service, the Auditor must verify that the EDE Entity has successfully passed testing with the Hub.<sup>35</sup></li> <li>– If an EDE Entity uses a third-party ID proofing service, the Auditor must evaluate and certify the following: <ul style="list-style-type: none"> <li>The ID proofing service is FICAM TFS-approved, and</li> <li>The EDE Entity has implemented the service correctly.</li> </ul> </li> <li>– If an EDE Entity offers a Manual ID proofing option for an in-person Agent and Broker pathway, the Auditor must verify that the EDE Entity requires Agents and Brokers to ID proof Consumers as described in the “Acceptable Documentation for Identity Proofing” document.</li> <li>– EDE Entity’s inclusion of the appropriate Consumer User ID fields in the EDE and Fetch Eligibility API calls.</li> </ul> </li> </ul>

<sup>35</sup> RIDP/FARS testing requirements for the Hub can be found at the following link on CMS zONE: <https://zone.cms.gov/document/api-information>.

Review Category	Requirement and Audit Standard
<b>Agent and Broker Identity Proofing Verification</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> If an EDE Entity is implementing an Agent and Broker pathway for its EDE environment, the EDE Entity must implement Agent and Broker ID proofing verification procedures that consist of the following requirements: <ul style="list-style-type: none"> <li>– EDE Entity must integrate with IDM-Okta<sup>36</sup> and provide the User ID of the requester and IDM-Okta token in the header for each EDE API call. For Agents and Brokers, the User ID must exactly match the Exchange User ID (i.e. the Agent's or Broker's portal.cms.gov User ID) for the Agent or Broker, or the request will fail Exchange User ID validation. The same User ID requirements apply to the Fetch Eligibility and Submit Enrollment APIs. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID.</li> <li>– EDE Entity must ID proof all Agents and Brokers prior to allowing the Agents and Brokers to use its EDE environment. EDE Entity may conduct ID proofing in one of the following ways: <ul style="list-style-type: none"> <li>Use the Exchange-provided RIDP/FARS APIs to remotely ID proof Agents and Brokers; OR</li> <li>Manually ID proof Agents and Brokers following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE EDE webpage (<a href="https://zone.cms.gov/document/api-information">https://zone.cms.gov/document/api-information</a>). EDE Entities are permitted to use manual ID proofing as an alternative for Agents and Brokers that cannot be ID proofed via the RIDP/FARS services.</li> </ul> </li> <li>– EDE Entity must validate an Agent's or Broker's National Producer Number (NPN) using the National Insurance Producer Registry (<a href="https://www.nipr.com">https://www.nipr.com</a>) prior to allowing the Agent or Broker to use its EDE environment.</li> <li>– EDE Entity must systematically provide an Agent and Broker ID proofing process—that meets all of the requirements defined here—that applies to all downstream Agents and Brokers of the Primary EDE Entity.</li> <li>– Additionally, all Agent and Broker users of an Upstream EDE Entity's EDE website (hosted by a Primary EDE Entity) must be ID proofed consistent with these requirements. The Primary EDE Entity may provide one centralized ID proofing approach for any Agents and Brokers that will use the Primary EDE Entity's EDE environment (including when utilized by Upstream EDE Entities and their downstream Agents and Brokers).</li> </ul> </li> </ul>

<sup>36</sup> For instructions on how to integrate with IDM-Okta, see the Change Request #55 Integration Manual (IDM Integration), available at: <https://zone.cms.gov/document/business-audit> and *Hub Onboarding Form*, available at: <https://zone.cms.gov/document/hub-onboarding-form>.



Review Category	Requirement and Audit Standard
<b>Agent and Broker Identity Proofing Verification (continued)</b>	<p>Alternatively, the Upstream EDE Entity may conduct its own ID proofing process of its downstream Agents and Brokers consistent with these requirements. The Upstream EDE Entity must provide the information for Agents and Brokers that have passed and failed ID proofing to the Primary EDE Entity using a secure data transfer. If an Upstream EDE Entity wants to pursue this flexibility, its ID proofing process must be audited by an Auditor consistent with these standards and the arrangement will be considered a hybrid arrangement.</p> <ul style="list-style-type: none"> <li>– Note: If a Primary EDE Entity does not provide a centralized process for ID proofing an Upstream EDE Entity’s downstream Agent and Broker and if the Primary EDE Entity intends to provide the EDE environment to Upstream EDE Entities, the Upstream EDE Entities will be required to provide documentation of an Auditor’s evaluation of its ID proofing approach consistent with these standards. This process must be categorized as an EDE Entity-initiated Change Request (Section XI.A, EDE Entity-initiated Change Requests) if it occurs after the Primary EDE Entity’s initial audit submission and the arrangement with the Upstream EDE Entity will be considered a hybrid arrangement.</li> <li>– All Agents and Brokers that will use EDE must be ID proofed consistent with these standards. This includes downstream Agents and Brokers of Primary EDE Entities and Upstream EDE Entities. If applicable, the Auditor must evaluate the Primary EDE Entity’s centralized implementation for ID proofing or the Upstream EDE Entity’s implementation for ID proofing.</li> <li>– EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3.</li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– EDE Entity’s inclusion of the appropriate Agent and Broker User ID and IDM-Okta token fields in the EDE and Fetch Eligibility and Submit Enrollment API calls.</li> <li>– EDE Entity’s process for ID proofing an Agent or Broker prior to allowing an Agent or Broker to use its EDE environment.</li> <li>– EDE Entity’s process for validating an Agent’s or Broker’s NPN using the National Insurance Producer Registry prior to allowing an Agent or Broker to use its EDE environment.</li> <li>– EDE Entity’s process for systematically providing an Agent and Broker ID proofing approach for all downstream Agents and Brokers of the EDE Entity and, if applicable, any Upstream EDE Entities.</li> <li>– If the Primary EDE Entity has not provided a centralized ID proofing approach to an Upstream EDE Entity, Primary EDE Entity’s process for verifying that an Upstream EDE Entity has conducted appropriate ID proofing, consistent with this requirement, for all of the Upstream EDE Entity’s downstream Agents and Brokers prior to those Agents and Brokers being able to use the Primary EDE Entity’s EDE environment.</li> </ul> </li> </ul>
<b>Phase-dependent Screener Questions (EDE Phase 1 and 2 EDE Entities Only)</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> An EDE Entity that implements either EDE Phase 1 or Phase 2 must implement screening questions to identify Consumers whose eligibility circumstances the EDE Entity is unable to support consistent with the eligibility scenarios supported by the EDE Entity’s selected EDE phase. These phase-dependent screener questions must be located at the beginning of the EDE application, but may follow the QHP plan compare experience. For those Consumers who won’t be able to apply through scenarios covered by the EDE phase that the EDE Entity implements, the EDE Entity must either route the Consumer to the classic DE double-redirect pathway or direct the Consumer to the Exchange by providing the following options: HealthCare.gov or the Exchange Call Center at 1-800-318-2596 [TTY: 1-855-889-4325].</li> <li>▪ <i>Review Standard:</i> The Auditor must verify the following: <ul style="list-style-type: none"> <li>– The EDE Entity has implemented screening questions—consistent with the requirements in the Exchange Application UI Principles document and Application UI Toolkit—to identify Consumers with eligibility scenarios not supported by the EDE Entity’s EDE environment and selected EDE phase.</li> <li>– The EDE Entity’s EDE environment facilitates moving Consumers to one of the alternative enrollment pathways described immediately above.</li> </ul> </li> </ul>

Review Category	Requirement and Audit Standard
<b>Accurate and Streamlined Eligibility Application User Interface (UI)</b>	<p><i>Requirement:</i> EDE Entities using the EDE pathway must support all application scenarios outlined in EDE Entity's selected EDE phase. The EDE Entity must adhere to the guidelines set forth in the FFE Application UI Principles document when implementing the application. EDE Entities can access the FFE Application UI Principles document on CMS zONE (<a href="https://zone.cms.gov/document/eligibility-information">https://zone.cms.gov/document/eligibility-information</a>). Auditors will need to access the FFE Application UI Principles document to conduct the audit.</p> <ul style="list-style-type: none"> <li>– As explained in the FFE Application UI Principles document, the EDE Entity must implement the application in accordance with the Exchange requirements. For each supported eligibility scenario, the EDE Entity must display all appropriate eligibility questions and answers, including all questions designated as optional. (Note: These questions are optional for the Consumer to answer, but are not optional for EDE Entities to implement.) The FFE Application UI Principles document and Application UI Toolkit define appropriate flexibility EDE Entities may implement with respect to question wording, question order or structure, format of answer choices (e.g., drop-down lists, radio buttons), and integrated help information (e.g., tool tips, URLs, help boxes). In most cases, answer choices, question logic (e.g., connections between related questions), and disclaimers (e.g., APTC attestation) must be identical to those of the Exchange. <ul style="list-style-type: none"> <li>Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this exceeds the scope of the test cases in the Eligibility Results Toolkits.</li> </ul> </li> <li>– EDE Entities will also need to plan their application's back-end data structure to ensure that attestations can be successfully submitted to Standalone Eligibility Service (SES) APIs at appropriate intervals within the application process and that the EDE Entity can process responses from SES and integrate them into the UI question flow logic, which is dynamic for an individual Consumer based on his or her responses. The EDE Entity will need to ensure that sufficient, non-contradictory information is collected and stored such that accurate eligibility results will be reached without any validation errors.</li> </ul> <ul style="list-style-type: none"> <li>▪ <i>Review Standard:</i> The Auditor must review and certify the following: <ul style="list-style-type: none"> <li>– The FFE Application UI has been implemented in EDE Entity's environment in accordance with the Exchange Application UI Principles document.</li> <li>– The FFE Application UI displays all appropriate eligibility questions and answers from the Application UI Toolkit, including any questions designated as optional.</li> <li>– The Auditor will review the application for each supported eligibility scenario under the phase the EDE Entity has implemented to confirm that the application has been implemented in accordance with the FFE Application UI Principles document and Application UI Toolkit. The Auditor will document this compliance in the Application UI Toolkit. <ul style="list-style-type: none"> <li>Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this exceeds the scope of the test cases in the Eligibility Results Toolkits.</li> </ul> </li> <li>– If EDE Entity has implemented Phase 1 or Phase 2, the Auditor will confirm that the UI includes a disclaimer stating that the environment does not support all application scenarios, and identifying which scenarios are and are not supported. The disclaimer should direct the Consumer to alternative pathways, such as the classic DE double-redirect pathway or direct the Consumer to the Exchange (HealthCare.gov or the Exchange Call Center at 1-800-318-2596 (TTY: 1-855-889-4325)). This requirement is included in the Communications Toolkit.</li> </ul> </li> </ul>

Review Category	Requirement and Audit Standard
<b>Post-eligibility Application Communications</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> The EDE environment must display high-level eligibility results, next steps for enrollment, and information about each Applicant’s insurance affordability program eligibility (e.g., APTC, CSR, Medicaid, and/or CHIP eligibility), Data Matching Issues (DMIs), special enrollment periods (SEPs), SEP Verification Issues (SVIs), and enrollment steps in a clear, comprehensive and Consumer-friendly way. Generally, CMS’s Communications Toolkit constitutes the minimum post-eligibility application communications requirements that an EDE Entity must provide to users of the EDE environment; CMS does not intend for the Communications Toolkit requirements to imply that EDE Entities are prohibited from providing additional communications or functionality, consistent with applicable requirements. <ul style="list-style-type: none"> <li>– EDE Entity must provide Consumers with required UI messaging tied to API functionality and responses as provided in the EDE API Companion Guide<sup>37</sup>.</li> <li>– EDE Entity must provide Consumers with the CMS-provided Eligibility Determination Notices (EDNs) generated by the Exchange any time it submits or updates an application pursuant to requirements provided by CMS in the Communications Toolkit.</li> </ul> </li> </ul>

<sup>37</sup> The API Companion Guide is available on CMS zONE at the following link: <https://zone.cms.gov/document/api-information>.

Review Category	Requirement and Audit Standard
<b>Post-eligibility Application Communications (continued)</b>	<ul style="list-style-type: none"> <li>– EDE Entity must provide the EDN in a downloadable format at the time the Consumer’s application is submitted or updated and must have a process for providing access to the Consumer’s most recent EDN via the API as well as providing access to the Consumer’s historical notices—accessed via the Notice Retrieval API by the EDE Entity’s EDE environment—within the UI. The UI requirements related to accessibility of a Consumer’s EDN are set forth in the Communications Toolkit.</li> <li>– EDE Entities are not required to store notices downloaded from the Exchange. EDE Entities must use the Metadata Search API and the Notice Retrieval API to generate the most recent Exchange notices when Consumers act to view/download notices consistent with the Communications Toolkit. EDE Entities must also provide access to view/download historical notices in their UIs.</li> <li>– EDE Entity must provide and communicate status updates and access to information for Consumers to manage their applications and coverage. These communications include, but are not limited to, status of DMLs and SVIs, enrollment periods (e.g., SEP eligibility and the OEP), providing and communicating about new notices generated by the Exchange, application and enrollment status, and supporting document upload for DMLs and SVIs. This requirement is detailed in the Communications Toolkit.</li> <li>– EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI (e.g., an account management hub for managing all application- and enrollment-related actions).</li> <li>– For any Consumers enrolled, including via the Agent and Broker pathway, the EDE Entity must provide critical communications to Consumers notifying them of the availability of Exchange-generated EDNs, critical communications that the Consumer will no longer receive from the Exchange (i.e., if the EDE Entity has implemented and been approved by CMS to assume responsibility for those communications), and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer’s application or enrollment status.</li> <li>– All EDE Entities, regardless of phase, must provide Consumers with status updates and document upload capabilities for all DMLs and SVIs. Even if an EDE Entity’s chosen eligibility application phase does not support the questions necessary to reach a certain DMI or SVI, the post-application and post-enrollment functionality must support any Consumer with any DMI or SVI; post-application and post-enrollment DMI and SVI management is not dependent on the EDE Entity’s chosen eligibility application phase.</li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– The EDE Entity’s EDE environment is compliant with the requirements contained in the Communications Toolkit and API Companion Guide.</li> <li>– The EDE Entity’s EDE environment notifies Consumers of their eligibility results prior to QHP enrollment, including when submitting a CiC in the environment. For example, if a Consumer’s APTC or CSR eligibility changes, EDE Entity must notify the Consumer of the change and allow the Consumer to modify his or her QHP selection (if SEP-eligible) or APTC allocation accordingly.</li> <li>– EDE Entity must have a process for providing Consumers with a downloadable EDN in its EDE environment and for providing access to a current EDN via the API. EDE Entity must share required eligibility information that is specified by CMS in the Communications Toolkit.</li> <li>– The Auditor must verify that EDE Entity’s EDE environment is providing status updates and ongoing communications to Consumers according to CMS requirements in the Communications Toolkit as it relates to the status of their application, eligibility, enrollment, notices, and action items the Consumer needs to take.</li> <li>– The EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI.</li> <li>– The EDE Entity must have a means for providing critical communications to the Consumer consistent with the standards above.</li> <li>– The EDE Entity must support all DMLs and SVIs in its post-eligibility application and post-enrollment functionality.</li> </ul> </li> </ul>

Review Category	Requirement and Audit Standard
<b>Accurate Information about the Exchange and Consumer Communications</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must provide Consumers with CMS-provided language informing and educating the Consumers about the Exchanges and HealthCare.gov and Exchange-branded communications Consumers may receive with important action items. CMS defines these requirements in the Communications Toolkit.</li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify that the EDE Entity's EDE environment includes all required language, content, and disclaimers provided by CMS in accordance with the standards stated in guidance and the Communications Toolkit.</li> </ul>
<b>Documentation of Interactions with Consumer Applications or the Exchange</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must implement and maintain tracking functionality on its EDE environment to track Agent, Broker, and Consumer interactions, as applicable, with Consumer applications using a unique identifier for each individual, as well as an individual's interactions with the Exchanges (e.g., application; enrollment; and handling of action items, such as uploading documents to resolve a DMI). This requirement also applies to any actions taken by a downstream Agent or Broker,<sup>38</sup> as well as the Upstream EDE Entity users, of a Primary EDE Entity's EDE environment.</li> <li>▪ <i>Review Standard:</i> The Auditor must verify EDE Entity's process for determining and tracking when an Upstream EDE Entity, downstream Agent or Broker, and Consumer has interacted with a Consumer application or taken actions utilizing the EDE environment or EDE APIs. The Auditor must verify and certify the following:                         <ul style="list-style-type: none"> <li>– The EDE Entity's environment tracks, at a minimum, the interactions of Upstream EDE Entities, downstream Agents or Brokers, and Consumers with a Consumer's account, records, application, or enrollment information utilizing the EDE environment or EDE APIs.</li> <li>– The EDE Entity's environment tracks when an upstream Entity, downstream Agent or Broker, or Consumer views a Consumer's record, enrollment information, or application information utilizing the EDE environment or EDE APIs.</li> <li>– The EDE Entity's environment uses unique identifiers to track and document activities by Consumers, downstream Agents and Brokers, and Upstream EDE Entities using the EDE environment.</li> <li>– The EDE Entity's environment tracks interactions with the EDE suite of APIs by an Upstream EDE Entity, a downstream Agent or Broker, or Consumer.</li> <li>– The EDE Entity's environment stores this information for 10 years.</li> </ul> </li> </ul>

<sup>38</sup> Note: References to downstream Agents and Brokers include downstream Agents and Brokers of either the Primary EDE Entity or an Upstream EDE Entity.

Review Category	Requirement and Audit Standard
<b>Eligibility Results Testing and SES Testing</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must submit accurate applications through its EDE environment that result in accurate and consistent eligibility determinations for the supported eligibility scenarios covered by EDE Entity's chosen EDE phase. <ul style="list-style-type: none"> <li>– The business requirements audit package must include testing results in the designated Exchange EDE testing environment. CMS has provided a set of Eligibility Results Toolkits with the eligibility testing scenarios on CMS zONE <a href="https://zone.cms.gov/document/business-audit">https://zone.cms.gov/document/business-audit</a>.</li> </ul> </li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– The Auditor was able to successfully complete a series of test eligibility scenarios in the EDE Entity's EDE environment implementation using the Eligibility Results Toolkits. For example, these scenarios may include Medicaid and CHIP eligibility determinations, and different combinations of eligibility determinations for APTC and CSRs. Note: These scenarios do not test, and are not expected to test, every possible question in the Application UI flow for an EDE Entity's selected phase. In addition to reviewing the eligibility results test cases, the Auditor must review the Application UI for compliance as defined above.</li> <li>– The Auditor must test each scenario and verify that the eligibility results and the eligibility process were identical to the expected results and process. The Auditor must provide CMS confirmation that each relevant eligibility testing scenario was successful, that the expected results were received, and must submit the required proof, as defined in the Eligibility Results Toolkits. This will include screenshots, EDNs, and the raw JSON from the Get App API response for the application version used to complete the scenario. Note: EDNs and raw JSONs are required for all required toolkit scenarios; however, screenshots are only required for the highest phase an entity is submitting (for example, a Prospective phase 3 EDE Entity must submit screenshots for the Phase 3 Eligibility Results Toolkit only, but must submit EDNs and raw JSONs for applicable Phase 1, Phase 2, and Phase 3 toolkit scenarios).</li> </ul> </li> </ul>
<b>API Functional Integration Requirements</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must implement the EDE API suite and corresponding UI functionality in accordance with the API specifications and EDE API Companion Guide provided by CMS. The EDE API specifications and EDE API Companion Guide are available on CMS zONE (<a href="https://zone.cms.gov/document/api-information">https://zone.cms.gov/document/api-information</a>).</li> <li>▪ <i>Review Standard:</i> The Auditor must complete the set of test scenarios as outlined in the API Functional Integration Toolkit to confirm that the EDE Entity's API and corresponding UI integration performs the appropriate functions when completing the various EDE tasks. For example, the Auditor may have to complete a scenario to verify that a Consumer or Agent and Broker is able to view any SVIs or DMIs that may exist for a Consumer, and confirm that the Consumer or Agent and Broker has the ability to upload documents to resolve any SVIs or DMIs. Some of the test cases require that the Auditor and EDE Entity request CMS to process adjudication actions; the Auditor cannot mark these particular test cases as compliant until evaluating whether the expected outcome occurred after CMS takes the requested action. The Auditor will also need to be aware of the following requirements related to the test scenarios: <ul style="list-style-type: none"> <li>– Test scenarios in the API Functionality Integration Toolkit must be completed for both the Consumer pathway and the Agent and Broker pathway if an EDE Entity is pursuing approval to use both pathways.</li> <li>– The API Functional Integration Toolkit includes a "Required Evidence" column, Column H, on the "Test Cases" tab. Auditors will need to submit the applicable "Required Evidence," including the complete header and body for each required API request and response, as part of the audit submission.</li> </ul> </li> </ul>
<b>Application UI Validation</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must implement CMS-defined validation requirements within the application. The validation requirements prevent EDE Entity from submitting incorrect data to the Exchange.</li> <li>▪ <i>Review Standard:</i> The Auditor must confirm that EDE Entity has implemented the appropriate application field-level validation requirements consistent with CMS requirements. These field-level validation requirements are documented in the FFE Application UI Principles document.</li> </ul>



Review Category	Requirement and Audit Standard
<b>Section 508-compliant UI</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> Pursuant to 45 C.F.R. § 155.220(c)(3)(ii)(D) (citing 45 C.F.R. §§ 155.230 and 155.260(b)) and 45 C.F.R. § 156.265(b)(3)(iii) (citing 45 C.F.R. §§ 155.230 and 155.260(b)), Web-brokers and QHP Issuers participating in DE, including all EDE Entities, must implement an eligibility application UI that is Section 508 compliant. A Section 508-compliant application must meet the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)).</li> <li>▪ <i>Review Standard:</i> The Auditor must confirm that EDE Entity's application UI meets the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)). The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– Within the Business Requirements Audit Report Template, the Auditor must confirm that the EDE Entity's application UI is Section 508 compliant. No specific report or supplemental documentation is required.</li> <li>– The Auditor may review results produced by a 508 compliance testing tool. If an EDE Entity uses a 508 compliance testing tool to verify that its application UI is 508 compliant, its Auditor must, at a minimum, review the results produced by the testing tool and document any non-compliance, as well as any mitigation or remediation to address the non-compliance. It is not sufficient for an Auditor to state that an EDE Entity complies with this requirement by confirming that the EDE Entity utilized a 508 compliance testing tool.</li> </ul> </li> </ul>
<b>Non-English-language Version of the Application UI and Communication Materials</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> In accordance with 45 C.F.R. § 155.205(c)(2)(iv)(B) and (C), QHP Issuers and Web-brokers, including those that are EDE Entities, must translate applicable website content (e.g., the application UI) on Consumer-facing websites into any non-English language that is spoken by a limited English proficient (LEP) population that reaches ten (10) percent or more of the population of the relevant State, as determined in current guidance published by the Secretary of HHS.<sup>39</sup> EDE Entities must also translate communications informing Consumers of the availability of Exchange-generated EDNs; critical communications that the Consumer will no longer receive from the Exchange (i.e., if the EDE Entity has implemented and been approved by CMS to assume responsibility for those communications); and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer's use of its EDE environment into any non-English language that is spoken by an LEP population that reaches ten (10) percent or more of the population of the relevant State, as determined in guidance published by the Secretary of HHS.<sup>40</sup></li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– The Auditor must confirm that the non-English-language version of the application UI and associated critical communications are compliant with the Exchange requirements, including the Application UI Toolkit and Communications Toolkit.</li> <li>– The Auditor must verify that the application UI has the same meaning as its English-language version.</li> <li>– The Auditor must also verify that EDE Entity has met all EDE communications translation requirements released by CMS in the Communications Toolkit.</li> <li>– The Auditor must document compliance with this requirement within the Business Requirements Audit Report Template, the Application UI Toolkit, and the Communications Toolkit. In the toolkits, the Auditor can add additional columns for the Auditor compliance findings fields (yellow-shaded columns) or complete the Spanish audit in a second copy of each of the two toolkits.</li> </ul> </li> </ul>

<sup>39</sup> Guidance and Population Data for Exchanges, Qualified Health Plan Issuers, and Web-Brokers to Ensure Meaningful Access by Limited-English Proficient Speakers Under 45 CFR §155.205(c) and §156.250 (March 30, 2016) <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Language-access-guidance.pdf> and “Appendix A- Top 15 Non-English Languages by State” [https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508\\_update12-20-16.pdf](https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508_update12-20-16.pdf).

<sup>40</sup> Frequently Asked Questions (FAQs) Regarding Spanish Translation and Audit Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with Federally-facilitated Exchanges (FFE) (June 20, 2018) provides further information regarding translation and audit requirements: <https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-Spanish-Translation-and-Audit-Requirements.PDF>.

Review Category	Requirement and Audit Standard
<b>EDE Change Management Process</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must develop and consistently implement processes for managing changes to the EDE environment relevant to the business requirements audit requirements. This requirement does not replace the evaluation necessary for relevant privacy and security controls. At a minimum, the EDE Entity's change management plan must include the following elements: <ul style="list-style-type: none"> <li>– A process that incorporates all elements of the Change Notification SOP as referenced in Section XI.A.i, EDE Entity-initiated Change Request Process;</li> <li>– All application and business audit-related changes are thoroughly defined and evaluated prior to implementation, including the potential effect on other aspects of the EDE end-user experience;</li> <li>– A process for defining regression testing scope and developing or identifying applicable testing scenarios;</li> <li>– A process for conducting regression testing;</li> <li>– A process for identifying and correcting errors discovered through regression testing and re-testing the correction;</li> <li>– A process for maintaining separate testing environments and defining the purposes and releases for each environment;</li> <li>– The change management process must be maintained in writing and relevant individuals must be informed on the change management process and on any updates to the process; and</li> <li>– The change management process must include a process, if applicable, for an EDE Entity to update the non-English-language version of the application UI and communication materials for any changes to the application UI or communication materials in the English-language version of the EDE environment.</li> </ul> </li> <li>▪ <i>Review Standard:</i> The Auditor must evaluate the EDE Entity's change management plan for compliance with the elements and criteria defined above.</li> </ul>
<b>Health Reimbursement Arrangement (HRA) Offer Required UI Messaging</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> Phase 3 EDE Entities, Phase 2 EDE Entities that optionally implement full HRA functionality, and EDE Entities that also offer a classic DE pathway, must implement required UI messaging for qualified individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the qualified individuals consistent with CMS guidance. Required UI messaging for various scenarios are detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.<sup>41</sup></li> <li>▪ <i>Review Standard:</i> The Auditor must review the EDE Entity's HRA offer implementation to confirm that the required UI messaging content is displayed for each of the relevant scenarios detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.</li> </ul>

<sup>41</sup> The document FFEs DE API for Web-brokers/Issuers Technical Specifications (Direct Enrollment API Specs) is available on CMS zONE at the following link: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.



## APPENDIX D: REQUIRED DOCUMENTATION

---

The below table describes the required artifacts that the EDE Entity must complete for approval during Year 6 of EDE.<sup>42</sup> Additional details about the documentation related to the privacy and security audit (i.e., Interconnection Security Agreement (ISA), Security Privacy Assessment Report, Plan of Actions & Milestones (POA&M), Privacy Impact Assessment, Non-Exchange Entity System Security and Privacy Plan (NEE SSP), Incident Response Plan and Incident/Breach Notification Plan, Contingency Plan, Configuration Management Plan, and Information Security and Privacy Continuous Monitoring Strategy Guide (ISCM Guide)<sup>43</sup> are provided in related CMS guidance. All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

---

<sup>42</sup> “Year 6 of EDE” refers to the remainder of PY 2023 and PY 2024, including the PY 2024 OEP. The table in Appendix D is an updated combined version of Exhibits 4 and 7 in the “Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.”

<sup>43</sup> These documents are available on CMS zONE at the following link: <https://zone.cms.gov/document/enhanced-direct-enrollment>.

Document	Description	Submission Requirements	Entity Responsible	Deadline
----------	-------------	-------------------------	--------------------	----------

<p><b>Notice of Intent to Participate and Auditor Confirmation</b></p>	<ul style="list-style-type: none"> <li>▪ Once the Prospective Primary and Prospective Phase Change EDE Entity has a confirmed Auditor(s) who will be completing its audit(s), it must notify CMS that it intends to apply to use the EDE pathway for Year 6 of EDE prior to initiating the audit. The email must include the following:             <ul style="list-style-type: none"> <li>– Prospective EDE Entity Name</li> <li>– Auditor Name(s) and Contact Information (Business Requirements and Privacy and Security, if different)</li> <li>– A copy of the executed contract with the Auditor(s) (pricing and proprietary information may be redacted)</li> <li>– EDE Phase (1, 2, or 3)</li> <li>– Prospective EDE Entity Primary Point of Contact (POC) name, email, and phone number. The Primary POC should be a person who is able to make decisions on behalf of the entity</li> <li>– Prospective EDE Entity Technical POC name, email, and phone number. The Technical POC should be a person</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▪ The Prospective Primary and Prospective Phase Change EDE Entity must email <a href="mailto:directenrollment@cms.hhs.gov">directenrollment@cms.hhs.gov</a></li> <li>▪ Subject line should state: “Enhanced DE: Intent.”</li> </ul>	<p>Prospective Primary and Prospective Phase Change EDE Entities</p> <p>Note: CMS is not collecting notices of intent from prospective Upstream EDE Entities.</p>	<p>March 1</p>
--	---	--	---	----------------

Document	Description	Submission Requirements	Entity Responsible	Deadline
	<ul style="list-style-type: none"> <li>– who manages technical development</li> <li>– Prospective EDE Entity Emergency POC name, email, and phone number. The Emergency POC should be a person who should be contacted in an emergency situation.<sup>44</sup></li> <li>– CMS-issued Hub Partner ID</li> </ul>			
<p><b>DE Entity Documentation Package—Privacy Questionnaire (or attestation, if applicable, see Submission Requirements column)</b></p>	<ul style="list-style-type: none"> <li>▪ CMS has provided the privacy questionnaire as part of the DE Entity Documentation Package available on CMS zONE.</li> <li>▪ EDE Entity must populate the privacy questionnaire and return it to CMS for review.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the DE/EDE Entity PME Site</li> <li>▪ If an EDE Entity's responses to the privacy questionnaire are unchanged from the EDE Entity's last submission of a privacy questionnaire, the Entity may submit an attestation stating that the previously submitted questionnaire remains accurate.</li> <li>– The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents.</li> </ul>	<p>Prospective Primary EDE Entities</p>	<p>Submit with audit submission</p>

<sup>44</sup> CMS will send EDE related communications to the POCs listed in the EDE Entity's Notice of Intent to Participate. EDE Entities can change these POCs at any time by emailing [directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov).

Document	Description	Submission Requirements	Entity Responsible	Deadline
<p><b>DE Entity Documentation Package—Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements column)</b></p>	<ul style="list-style-type: none"> <li>▪ Submit the URL and text of each privacy policy statement displayed on your website and your website's Terms of Service in a Microsoft Word document or a PDF.</li> <li>▪ The privacy policy and terms of service must be submitted for any EDE Entity's website that is collecting Consumer data as part of the EDE end-user experience.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the DE/EDE PME Site</li> <li>▪ If an EDE Entity's privacy policy and Terms of Service remain unchanged from the EDE Entity's last submission of the privacy policy and Terms of Service, the Entity may submit an attestation stating that the previously submitted privacy policy and Terms of Service will remain unchanged.                             <ul style="list-style-type: none"> <li>– The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents</li> </ul> </li> </ul>	<p>Both Prospective Primary and Prospective Upstream EDE Entities</p>	<p>Prospective Primary EDE Entities: Submit with audit submission.</p> <p>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for prospective Upstream EDE Entities, but to be reasonably certain a prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs.</p>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>EDE Business Agreement</b>	<ul style="list-style-type: none"> <li>▪ EDE Entities must execute the EDE Business Agreement to use the EDE pathway. The agreement must identify the Entity's selected Auditor(s) (if applicable).</li> <li>▪ CMS will countersign the EDE Business Agreement after CMS has reviewed and approved the EDE Entity's business requirements audit and the privacy and security audit.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the DE/EDE Entity PME Site</li> </ul>	Both Prospective Primary and Prospective Upstream EDE Entities	<p>Prospective Primary EDE Entities: Submit with audit submission.</p> <p>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for Prospective Upstream EDE Entities, but to be reasonably certain a Prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs.</p>
<b>DE Entity Documentation Package—Operational and Oversight Information</b>	<ul style="list-style-type: none"> <li>▪ EDE Entities must submit the operational and oversight information to CMS to use the EDE pathway. This form must be filled out completely.</li> <li>▪ The form is an Excel file that the EDE Entity will complete and submit to CMS.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the DE/EDE Entity PME Site</li> <li>▪ Prospective Primary EDE Entities will receive an encrypted, pre-populated version of the form from CMS</li> <li>▪ Prospective Upstream EDE Entities will complete a blank version of the form that is available on CMS zONE</li> </ul>	Both Prospective Primary and Prospective Upstream EDE Entities	<p>Prospective Primary EDE Entities: Submit with audit submission.</p> <p>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for Prospective Upstream EDE Entities, but to be reasonably certain a Prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs.</p>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Business Audit Report and Toolkits</b>	<ul style="list-style-type: none"> <li>EDE Entities must submit the Business Requirements Audit Report Template and all applicable toolkits completed by its Auditor(s).</li> <li>See Section VI.B.ii, Business Requirements Audit Resources, Exhibit 5, for more information.</li> </ul>	<ul style="list-style-type: none"> <li>The EDE Entity and its Auditor(s) must submit the different parts of the Auditor resources package via the DE/EDE Entity PME Site</li> </ul>	Prospective Primary EDE Entities, Prospective Phase Change EDE Entities, and their Auditors	April 1 -July 1 (3:00 AM ET)
<b>Training</b>	<ul style="list-style-type: none"> <li>EDE Entities (and their Auditors) must complete the trainings as outlined in Section VIII, Required Auditor and EDE Entity Training.</li> <li>The trainings are located on REGTAP (located at the following link: <a href="https://www.regtap.info/">https://www.regtap.info/</a>).</li> </ul>	<ul style="list-style-type: none"> <li>The person taking the training must complete the course conclusion pages at the end of each module</li> <li>The EDE Entity and Auditor are NOT required to submit anything additional to CMS but must retain a copy of the training confirmation webpage to provide to CMS, if requested</li> </ul>	Prospective Primary EDE Entities, Prospective Phase Change EDE Entities, Prospective Upstream EDE Entities, and Auditors	<p>Trainings must be completed by Prospective Primary and Phase Change EDE Entities and Auditors prior to Audit Submission</p> <p>Prospective Upstream EDE Entities must complete the training prior to approval to use the EDE pathway</p>
<b>HUB Onboarding Form</b>	<ul style="list-style-type: none"> <li>All EDE Entities must submit a new or updated Hub Onboarding Form to request EDE access. If an EDE Entity does not already have a Partner ID, the Hub will create a Partner ID for the EDE Entity upon receiving the Hub Onboarding Form.</li> </ul>	<ul style="list-style-type: none"> <li>Follow instructions on the Hub Onboarding Form (located at the following link: <a href="https://zone.cms.gov/document/hub-onboarding-form">https://zone.cms.gov/document/hub-onboarding-form</a>)</li> <li>Send to <a href="mailto:HubSupport@sparksoftcorp.com">HubSupport@sparksoftcorp.com</a></li> </ul>	Prospective Primary and Prospective Upstream EDE Entities	Prior to accessing the EDE APIs

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Application Technical Assistance and Mini Audit Testing Credentials</b>	<ul style="list-style-type: none"> <li>▪ An EDE Entity must provide application technical assistance and mini audit testing credentials to CMS consistent with the process defined in Sections VI.C, Application Technical Assistance and X.D, Audit Submission Compliance Review for Prospective Primary EDE Entities, below.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Follow instructions on the EDE UI Eligibility Technical Assistance Credentials Form Template on CMS zONE: <a href="https://zone.cms.gov/document/eligibility-information">https://zone.cms.gov/document/eligibility-information</a></li> </ul>	Prospective Primary EDE Entities and Prospective Phase Change EDE Entities	Submit with audit submission date



Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Interconnection Security Agreement (ISA)</b>	<ul style="list-style-type: none"> <li>▪ A Prospective Primary EDE Entity must submit the ISA to use the EDE pathway.</li> <li>▪ CMS will countersign the ISA after CMS has reviewed and approved the EDE Entity's business requirements audit and privacy and security audit.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective Primary EDE Entity must submit the ISA via the DE/EDE Entity PME Site.</li> <li>▪ The ISA contains Appendices that must be completed in full for an EDE Entity to be considered for approval.</li> <li>▪ Appendix B of the ISA must detail:               <ul style="list-style-type: none"> <li>(1) all arrangements with Upstream EDE Entities and any related data connections or exchanges,</li> <li>(2) any arrangements involving Web-brokers, and</li> <li>(3) any arrangements with downstream agents and brokers that involve limited data collections, as described in Section IV.B, Downstream Third-party Agent and Broker Arrangements.</li> </ul> </li> <li>▪ Appendix B of the ISA must be updated and resubmitted as a Primary EDE Entity adds or changes any of the arrangements noted above consistent with the requirements in the ISA.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit with the audit submission</li> </ul>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Security Privacy Controls Assessment Test Plan (SAP)</b>	<ul style="list-style-type: none"> <li>▪ This report is to be completed by the Auditor and submitted to CMS prior to initiating the audit.</li> <li>▪ The SAP describes the Auditor's scope and methodology of the assessment. The SAP includes an attestation of the Auditor's independence.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the SAP completed by its Auditor via the DE/EDE Entity PME Site.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ At least thirty (30) Days before commencing the privacy and security audit; during the planning phase</li> </ul>
<b>Security Privacy Assessment Report (SAR)</b>	<ul style="list-style-type: none"> <li>▪ This report details the Auditor's assessment findings of the Prospective EDE Entity's security and privacy controls implementation.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the SAR completed by its Auditor via the DE/EDE Entity PME Site.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ April 1 – July 1 (3:00 AM ET)</li> </ul>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Plan of Action &amp; Milestones (POA&amp;M)</b>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity must submit a POA&amp;M if its Auditor identifies any privacy and security compliance issues in the SAR.</li> <li>▪ The POA&amp;M details a corrective action plan and the estimated completion date for identified milestones.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the POA&amp;M in conjunction with the SAR via the DE/EDE Entity PME Site.</li> <li>▪ POA&amp;Ms with outstanding findings must be submitted monthly to CMS until all the findings from security controls assessments, security impact analyses, and continuous monitoring activities described in the NEE SSP controls CA-5 and CA-7 are resolved. Prospective EDE Entities can schedule their own time for monthly submissions of the POA&amp;M, but must submit an update monthly to CMS until all significant or major findings are resolved. Thereafter, quarterly POA&amp;M submissions are required as part of the ISCM activities.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Initial: April 1 – July 1 (3:00 AM ET)</li> <li>▪ Monthly submissions, as necessary, if outstanding findings.</li> <li>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit quarterly POA&amp;Ms by the last business Day of March, July, September, and December.</li> </ul>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Risk Acceptance Form</b>	<ul style="list-style-type: none"> <li>▪ The Risk Acceptance Form records the weaknesses that require an official risk acceptance from the organization's Authorizing Official.</li> <li>▪ Before deciding to accept the risks, the relevant NEE's authorities should rigorously explore ways to mitigate the risks.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Once the risk has been identified and deemed acceptable by the NEE's authorized official, the NEE must complete the entire Risk Acceptance Form and submit the completed form to CMS. The NEE will continue to track all accepted risks in the NEE's official POA&amp;M.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ The Risk Acceptance Form should be submitted with the POA&amp;M during the regular POA&amp;M submission schedule.</li> </ul>
<b>Privacy Impact Assessment (PIA)</b>	<ul style="list-style-type: none"> <li>▪ The PIA will detail the Prospective EDE Entity's evaluation of its controls for protecting PII.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity is not required to submit the PIA to CMS. However, per the ISA, CMS may request and review an EDE Entity's PIA at any time, including for audit purposes.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Before commencing the privacy and security audit as part of the NEE SSP</li> </ul>
<b>Non-Exchange Entity System Security and Privacy Plan (NEE SSP)</b>	<ul style="list-style-type: none"> <li>▪ The NEE SSP will include detailed information about the Prospective EDE Entity's implementation of required security and privacy controls.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective Primary EDE Entity must submit the completed NEE SSP via the DE/EDE Entity PME Site before commencing the privacy and security audit.</li> <li>▪ The implementation of security and privacy controls must be completely documented in the NEE SSP before the audit is initiated.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Before commencing the privacy and security audit</li> </ul>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Incident Response Plan and Incident/Breach Notification Plan</b>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity is required to implement Breach and Incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures.</li> <li>▪ A Prospective EDE Entity must incorporate these procedures into its own written policies and procedures.<sup>45</sup></li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity is not required to submit the Incident Response Plan and Incident/Breach Notification Plan to CMS. A Prospective EDE Entity must have procedures in place to meet CMS security and privacy Incident reporting requirements. CMS may request and review an EDE Entity's Incident Response Plan and Incident/Breach Notification Plan at any time, including for audit purposes.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Before commencing the privacy and security audit as part of the NEE SSP</li> </ul>

<sup>45</sup> <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf>.

<p><b>Annual Penetration Testing</b></p>	<ul style="list-style-type: none"> <li>▪ The penetration test must include the EDE environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10.</li> <li>▪ Before conducting the penetration testing, the EDE Entity must execute a Rules of Engagement with their Auditor’s penetration testing team.</li> <li>▪ The EDE Entity must also notify their CMS designated technical counterparts on their annual penetration testing schedule and must provide the following information to CMS, a minimum of five (5) business Days using the CMS-provided form<sup>46</sup>, prior to initiation of the penetration testing:             <ul style="list-style-type: none"> <li>– Period of testing performance (specific times for all penetration testing should be contained in individual test plans);</li> <li>– Target environment resources to be tested (IP addresses, Hostname, URL); and</li> <li>– Any restricted hosts, systems, or subnets that are not to be tested.</li> </ul> </li> <li>▪ During the penetration testing, the Auditor’s testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment.</li> <li>▪ The penetration testing shall be conducted in the lower environment that mirrors the production environment.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the Penetration Test results with the SAR via the DE/EDE Entity PME Site.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Initial: April 1 – July 1 (3:00 AM ET)</li> <li>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities perform penetration testing and submit results to CMS annually, prior to last business Day in July.</li> </ul>
--	---	--	--	---

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Vulnerability Scan</b>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity is required to conduct monthly Vulnerability Scans.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the last three months of their Vulnerability Scan Reports, in conjunction with POA&amp;M and SAR via the DE/EDE Entity PME Site.</li> <li>▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&amp;M.</li> <li>▪ Similar findings can be consolidated.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Initial: April 1 – July 1 (3:00 AM ET)</li> <li>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit Vulnerability Scans annually.</li> </ul>

<sup>46</sup> The Penetration Testing Notification Form is available at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

## APPENDIX E: AUDITOR IDENTIFICATION

---

EDE Entity agrees to identify, in Part I below, all Auditors selected to complete the Operational Readiness Review (ORR) and any subcontractors of the Auditor(s), if applicable. In the case of multiple Auditors, please indicate the role of each Auditor in completing the ORR (i.e., whether the Auditor will conduct the business requirements audit and/or the privacy and security audit, including the completion of an annual assessment of security and privacy controls by an Auditor, as described in the Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide). Include additional sheets, if necessary. EDE Entity must identify the ISCM Auditor that conducted the ISCM immediately preceding this Agreement's submission and execution.

If an Upstream EDE Entity will contract with an Auditor to audit additional functionality or systems added to its Primary EDE Entity's EDE Environment, pursuant to Section VIII.g or VIII.h of this Agreement, complete Part I to indicate the Auditor(s) that will conduct the business requirements audit and/or privacy and security audit of the additional functionality or systems.

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

### **TO BE FILLED OUT BY EDE ENTITY**

Primary EDE Entities, Hybrid Issuer Upstream EDE Entities, and Hybrid Non-Issuer Upstream EDE Entities must complete Part I.

#### **I. Complete These Rows if EDE Entity Is Subject to an Audit (ORR, ISCM, and/or Supplemental Audit)**

Printed Name and Title of Authorized Official of Auditor 1	Shibani Gupta
Auditor 1 Business Name	Absurance
Auditor 1 Address	5300 Ranch Point, Katy, TX 77494
Printed Name and Title of Contact of Auditor 1 (if different from Authorized Official)	
Auditor 1 Contact Phone Number	8322875647
Auditor 1 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	
Printed Name and Title of Authorized Official of Auditor 2	
Auditor 2 Business Name	
Auditor 2 Address	



Printed Name and Title of Contact of Auditor 2 (if different from Authorized Official)	
Auditor 2 Contact Phone Number	
Auditor 2 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	
Printed Name and Title of Authorized Official of Auditor 3	
Auditor 3 Business Name	
Auditor 3 Address	
Printed Name and Title of Contact of Auditor 3 (if different from Authorized Official)	
Auditor 3 Contact Phone Number	
Auditor 3 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	

**APPENDIX F: CONFLICT OF INTEREST DISCLOSURE FORM**

---

**TO BE FILLED OUT BY EDE ENTITY**

EDE Entity must disclose to the Department of Health & Human Services (HHS) any financial relationships between the Auditor(s) identified in Appendix E of this agreement, and individuals who own or are employed by the Auditor(s), and individuals who own or are employed by a Direct Enrollment (DE) Entity for which the Auditor(s) is conducting an Operational Readiness Review pursuant to 45 C.F.R. § 155.221(b)(4) and (f). EDE Entity must disclose any affiliation that may give rise to any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence.

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

Please describe below any relationships, transactions, positions (volunteer or otherwise), or circumstances that you believe could contribute to a conflict of interest:

- Not applicable; EDE Entity is not contracting with an Auditor.
- EDE Entity has no conflict of interest to report for the Auditor(s) identified in Appendix E.
- EDE Entity has the following conflict of interest to report for the Auditor(s) identified in Appendix E:

1. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
2. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
3. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## APPENDIX G: APPLICATION END-STATE PHASES

The below table describes each of the three end-state phases for hosting applications using the EDE Pathway.<sup>47</sup> EDE Entity must indicate the end-state phase it has selected in the “Operational and Oversight Information” form provided by CMS. All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

End State Phases	Description	Benefits
<b>Phase 1: Host Simplified Application + EDE API Suite</b>	<p>EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following:</p> <ul style="list-style-type: none"> <li>▪ Application filer (and others on application, if applicable) resides in the application state and all dependents have the same permanent address, if applicable</li> <li>▪ Application filer plans to file a federal income tax return for the coverage year; if married plans to file a joint federal income tax return with spouse</li> <li>▪ Application filer (and spouse, if applicable) is not responsible for a child 18 or younger who lives with the Application filer but is not on his/her federal income tax return</li> <li>▪ No household members are full-time students aged 18-22</li> <li>▪ No household member is pregnant</li> <li>▪ All Applicants are U.S. citizens</li> <li>▪ All Applicants can enter Social Security Numbers (SSNs)</li> <li>▪ No Applicants are applying under a name different than the one on his/her Social Security cards</li> <li>▪ No Applicants were born outside of the U.S. and became naturalized or derived U.S. citizens</li> <li>▪ No Applicants are currently incarcerated (detained or jailed)</li> <li>▪ No household members are American Indian or Alaska Native</li> <li>▪ No Applicants are offered health coverage through a job or COBRA</li> <li>▪ No Applicants are offered an individual coverage health reimbursement arrangement (HRA) or qualified small employer health reimbursement arrangement (QSEHRA)</li> <li>▪ No Applicants were in foster care at age 18 and are currently 25 or younger</li> <li>▪ All dependents are claimed on the Application filer's federal income tax return for the coverage year</li> <li>▪ All dependents are the Application filer's children who are single (not married) and 25 or younger</li> <li>▪ No dependents are stepchildren or grandchildren</li> <li>▪ No dependents live with a parent who is not on the Application filer's federal income tax return</li> </ul>	<p>Lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.</p>

<sup>47</sup> The table in Appendix G is an updated version of Exhibit 3 in the “Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.”

End State Phases	Description	Benefits
<b>Phase 2: Host Expanded Simplified Application + EDE API Suite</b>	<p>EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following:</p> <ul style="list-style-type: none"> <li>▪ All scenarios covered by Phase 1</li> <li>▪ Full-time student</li> <li>▪ Pregnant application members</li> <li>▪ Non-U.S. citizens</li> <li>▪ Naturalized U.S. citizens</li> <li>▪ Application members who do not provide an SSN</li> <li>▪ Application members with a different name than the one on their SSN cards</li> <li>▪ Incarcerated application members</li> <li>▪ Application members who previously were in foster care</li> <li>▪ Stepchildren</li> </ul>	<p>Second lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.</p>
<b>Phase 3: Host Complete Application + EDE API Suite</b>	<p>EDE Entity hosts an application that supports all application scenarios (equivalent to existing HealthCare.gov):</p> <ul style="list-style-type: none"> <li>▪ All scenarios covered in Phase 2</li> <li>▪ American Indian and Alaskan Native household members</li> <li>▪ Application members with differing home addresses or residing in a State separate from where they are applying for coverage</li> <li>▪ Application members with no home address</li> <li>▪ Application members not planning to file a tax return</li> <li>▪ Married application members not filing jointly</li> <li>▪ Application members responsible for a child age 18 or younger who lives with them, but is not included on the Application filer's federal income tax return (parent/caretaker relative questions)</li> <li>▪ Application members offered coverage through their job, someone else's job, or COBRA</li> <li>▪ Application members with dependent children who are over age 25 or who are married</li> <li>▪ Application members with dependent children living with a parent not on their federal income tax return</li> <li>▪ Dependents who are not sons/daughters</li> <li>▪ Applicants who are offered an individual coverage HRA or QSEHRA</li> </ul>	<p>Highest level of effort to implement and audit. EDE Entity would provide and service the full range of Consumer scenarios. Additionally, the EDE Entity would no longer need to redirect Consumers to alternative pathways for complex eligibility scenarios. Please note that the implementation of Phase 3 is comparatively more complex than the other phases and may require more time to implement, audit, and approve.</p>

**APPENDIX H: TECHNICAL AND TESTING STANDARDS  
FOR USING THE EDE PATHWAY**

---

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions the meaning provided in 45 C.F.R. § 155.20.

- (1) EDE Entity must possess a unique Partner ID assigned by the Centers for Medicare & Medicare Services (CMS). EDE Entity must use its Partner ID when interacting with the CMS Data Services Hub (Hub) and the EDE Application Program Interfaces (APIs) for EDE Entity's own line of business.

If EDE Entity uses a Primary EDE Entity's EDE Environment, EDE Entity must use its own Partner ID when interacting with the Hub and the EDE APIs. If EDE Entity is a Primary EDE Entity and provides an EDE Environment to another EDE Entity, as permitted under Section VIII.f, VIII.g, and VIII.h of this Agreement, the Primary EDE Entity must use the Partner ID assigned to the EDE Entity using its EDE Environment for any Hub or EDE API interactions for the other EDE Entity. If EDE Entity is a Primary EDE Entity, it must provide to CMS the Partner IDs of all entities that will implement and use Primary EDE Entity's EDE Environment.

- (2) CMS will provide EDE Entity with information outlining EDE API Specifications and with EDE-related Companion Guides, including the EDE Companion Guide, the Federally-facilitated Exchange (FFE) User Interface (UI) Application Principles for Integration with FFE APIs, and the UI Question Companion Guide, which is embedded within the FFE UI Application Principles for Integration with FFE APIs. The terms of these documents are specifically incorporated herein. EDE Entity's use of the EDE Environment must comply with any standards detailed in the EDE API Specifications guidance and the EDE-related Companion Guides.
- (3) EDE Entity must complete testing for each Hub-related transaction it will implement, and it shall not be allowed to exchange data with CMS in production mode until testing is satisfactorily passed, as determined by CMS in its sole discretion. Successful testing generally means the ability to pass approved standards, and to process data transmitted by EDE Entity to the Hub. The capability to submit these test transactions must be maintained by EDE Entity throughout the term of this Agreement.
- (4) EDE Entity agrees to submit test transactions to the Hub prior to the submission of any transactions to the FFE production system, and to determine that the transactions and responses comply with all requirements and specifications approved by CMS and/or the CMS contractor.
- (5) EDE Entity agrees that prior to the submission of any additional transaction types to the FFE production system, or as a result of making changes to an existing transaction type or system, it will submit test transactions to the Hub in accordance with paragraph (3) and (4) above.

- (6) EDE Entity acknowledges that CMS requires successful completion of an Operational Readiness Review (ORR) to the satisfaction of CMS, which must occur before EDE Entity is able to execute an ISA with CMS or submit any transactions using its EDE Environment to the FFE production system. The ORR will assess EDE Entity's compliance with CMS' regulatory requirements, this Agreement, and the Interconnection Security Agreement (ISA), including the required privacy and security controls. This Agreement may be terminated or access to CMS systems may be denied for a failure to comply with CMS requirements in connection to an ORR.
- (7) Upon approval for a significant change in the EDE Environment, including, but not limited to, initial approval to go-live with an EDE Environment, approval to go-live with an end-state phase change, or approval to proceed with a significant change to EDE Environment functionality, EDE Entity will limit enrollment volume in its production environment in accordance with the scale and schedule set by CMS, in its sole discretion, until CMS has verified the successful implementation of the EDE Entity's EDE Environment in production.
- (8) CMS, in its sole discretion, may restrict, delay, or deny an EDE Entity's ability to implement a significant change in the EDE Environment, consistent with paragraph (7) of this Appendix, if an EDE Entity has not maintained compliance with program requirements or the EDE Entity has triggered the conditions for Inactive, Approved Primary EDE Entities (Section IX.v of this Agreement). Failure to maintain compliance with program requirements includes, but is not limited to, an inability to meet CMS-issued deadlines for CMS-initiated Change Requests (Section IX.d of this Agreement) or failure to maintain an EDE Environment that complies with the standards detailed in the EDE API Specifications guidance and the EDE-related Companion Guides.
- (9) All compliance testing (Operational, Management and Technical) of EDE Entity will occur at a FIPS 199 MODERATE level due to the Personally Identifiable Information (PII) data that will be contained within EDE Entity's systems.

# **Exhibit F**

**ENHANCED DIRECT ENROLLMENT AGREEMENT BETWEEN ENHANCED  
DIRECT ENROLLMENT ENTITY AND THE CENTERS FOR MEDICARE &  
MEDICAID SERVICES FOR THE INDIVIDUAL MARKET FEDERALLY-  
FACILITATED EXCHANGES AND STATE-BASED EXCHANGES ON THE FEDERAL  
PLATFORM**

---

**THIS ENHANCED DIRECT ENROLLMENT AGREEMENT** (“Agreement”) is entered into by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES (“CMS”), as the Party (as defined below) responsible for the management and oversight of the Federally-facilitated Exchanges (“FFE”), also referred to as “Federally-facilitated Marketplaces” or “FFMs” and the operation of the federal eligibility and enrollment platform, which includes the CMS Data Services Hub (“Hub”), relied upon by certain State-based Exchanges (SBEs) for their eligibility and enrollment functions (including State-based Exchanges on the Federal Platform (SBE-FPs)), and Benefitalign LLC (hereinafter referred to as “Enhanced Direct Enrollment [EDE] Entity”), which uses a non-FFE Internet website in accordance with 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or 156.1230 to assist Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives in applying for Advance Payments of the Premium Tax Credit (“APTC”) and Cost-sharing Reductions (“CSRs”); applying for enrollment in Qualified Health Plans (“QHPs”); completing enrollment in QHPs; and providing related Customer Service. CMS and EDE Entity are hereinafter referred to as the “Party” or, collectively, as the “Parties.”

**WHEREAS:**

Section 1312(e) of the Affordable Care Act (“ACA”) provides that the Secretary of the U.S. Department of Health & Human Services (“HHS”) shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals in QHPs through an Exchange, and to assist individuals in applying for APTC and CSRs, to the extent allowed by States. To participate in the FFEs or SBE-FPs, Agents and Brokers, including Web-brokers, must complete all applicable registration and training requirements under 45 C.F.R. § 155.220.

Section 1301(a) of the ACA provides that QHPs are health plans that are certified by an Exchange and, among other things, comply with the regulations developed by the HHS under Section 1321(a) of the ACA and other requirements that an applicable Exchange may establish.

To facilitate the eligibility determination and enrollment processes, CMS will provide centralized and standardized business and technical services (“Hub Web Services”) through application programming interfaces (“APIs”) to EDE Entity that will enable EDE Entity to host application, enrollment, and post-enrollment services on EDE Entity’s own website. The APIs will enable the secure transmission of key eligibility and enrollment information between CMS and EDE Entity.

To facilitate the operation of the FFEs and SBE-FPs, CMS desires to: (a) allow EDE Entity to create, collect, disclose, access, maintain, store, and use Personally Identifiable



Information (“PII”) it receives directly from CMS and from Consumers, Applicants, Qualified Individuals, and Enrollees through EDE Entity’s website—or from these individuals’ legal representatives or Authorized Representatives—for the sole purpose of performing activities that are necessary to carry out functions that the ACA and its implementing regulations permit EDE Entity to perform; and (b) allow EDE Entity to provide such PII and other Consumer, Applicant, Qualified Individual, and Enrollee information to the FFEs and SBE-FPs through specific APIs to be provided by CMS.

EDE Entity desires to use an EDE Environment to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—to perform the Authorized Functions described in Section III.a of this Agreement.

45 C.F.R. § 155.260(b) provides that an Exchange must, among other things, require as a condition of contract or agreement that Non-Exchange Entities comply with privacy and security standards that are consistent with the standards in 45 C.F.R. §§ 155.260(a)(1) through (a)(6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 C.F.R. § 155.260(a)(3). 45 C.F.R. § 155.280 requires HHS to oversee and monitor Non-Exchange Entities for compliance with Exchange-established privacy and security requirements.

CMS has adopted privacy and security standards with which EDE Entity must comply, as specified in the Non-Exchange Entity System Security and Privacy Plan (“NEE SSP”)<sup>1</sup> and referenced in Appendix A (“Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities”), which are specifically incorporated herein. The security and privacy controls and implementation standards documented in the NEE SSP are established in accordance with Section 1411(g) of the ACA (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 (“FISMA”) (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the standards in 45 C.F.R. §§ 155.260(a)(1) through (a)(6).

Now, therefore, in consideration of the promises and covenants herein contained, the adequacy of which the Parties acknowledge, the Parties agree as follows:

I. Definitions.

Capitalized terms not otherwise specifically defined herein shall have the meaning set forth in the attached Appendix B (“Definitions”). Any capitalized term that is not defined herein or in Appendix B has the meaning provided in 45 C.F.R. § 155.20.

---

<sup>1</sup> The NEE SSP template is located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

II. Interconnection Security Agreement (ISA) Between Centers for Medicare & Medicaid Services (CMS) and Enhanced Direct Enrollment (EDE) Entity (“ISA”).

If EDE Entity is a Primary EDE Entity, it must enter into an ISA with CMS. EDE Entity must comply with all terms of the ISA,<sup>2</sup> including the privacy and security compliance requirements set forth in the ISA. The ISA shall be in effect for the full duration of this Agreement. If an Upstream EDE Entity is using a Primary EDE Entity’s EDE Environment, the Primary EDE Entity must supply an NEE SSP to each Upstream EDE Entity using the Primary EDE Entity’s EDE Environment that identifies all Common Controls and Hybrid Controls implemented in the EDE Environment. All Common Controls and Hybrid Controls must be documented between each applicable Upstream EDE Entity and its Primary EDE Entity as required by the NEE SSP section “Common and Hybrid Controls.” Furthermore, Appendix B of the ISA requires a Primary EDE Entity to attest that it has documented and shared the NEE SSP inheritable Common Controls and Hybrid Controls with applicable Upstream EDE Entities.

III. Acceptance of Standard Rules of Conduct.

EDE Entity and CMS are entering into this Agreement to satisfy the requirements under 45 C.F.R. §§ 155.260(b)(2) and 155.221(b)(4)(v). EDE Entity hereby acknowledges and agrees to accept and abide by the standard rules of conduct set forth below and in the Appendices, which are incorporated by reference in this Agreement, while and as engaging in any activity as EDE Entity for purposes of the ACA. EDE Entity shall strictly adhere to the privacy and security standards—and ensure that its employees, officers, directors, contractors, subcontractors, agents, Auditors, and representatives strictly adhere to the same—to gain and maintain access to the Hub Web Services and to create, collect, disclose, access, maintain, store, and use PII for the efficient operation of the FFEs and SBE-FPs. To the extent the privacy and security standards set forth in this Agreement are different than privacy and security standards applied to EDE Entity through any existing agreements with CMS, the more stringent privacy and security standards shall control.

- a. Authorized Functions. EDE Entity may create, collect, disclose, access, maintain, store, and use PII for the following, if applicable:
1. Assisting with completing applications for QHP eligibility;
  2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons;
  3. Assisting with completing applications for the receipt of APTC or CSRs and with selecting an APTC amount;
  4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR determination, if applicable;
  5. Assisting with the application for and determination of certificates of exemption;

---

<sup>2</sup> Unless specifically indicated otherwise, references to the ISA refer to the current, legally enforceable version of the agreement. The ISA is available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

6. Assisting with filing appeals of eligibility determinations in connection with the FFEs and SBE-FPs;
7. Transmitting information about the Consumer's, Applicant's, Qualified Individual's, or Enrollee's decisions regarding QHP enrollment and/or CSR and APTC information to the FFEs and SBE-FPs;
8. Facilitating payment of the initial premium amount to the appropriate QHP Issuer;
9. Facilitating an Enrollee's ability to disenroll from a QHP;
10. Educating Consumers, Applicants, Qualified Individuals or Enrollees—or these individuals' legal representatives or Authorized Representatives—on Insurance Affordability Programs and, if applicable, informing such individuals of eligibility for Medicaid or the Children's Health Insurance Program (CHIP);
11. Assisting an Enrollee in reporting changes in eligibility status to the FFEs and SBE-FPs throughout the coverage year, including changes that may affect eligibility (e.g., adding a dependent);
12. Correcting errors in the application for QHP enrollment;
13. Informing or reminding Enrollees when QHP coverage should be renewed, when Enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform Enrollees of QHP coverage options at renewal;
14. Providing appropriate information, materials, and programs to Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to inform and educate them about the use and management of their health information, as well as medical services and benefit options offered through the selected QHP or among the available QHP options;
15. Contacting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to assess their satisfaction or resolve complaints with services provided by EDE Entity in connection with the FFEs, SBE-FPs, EDE Entity, or QHPs;
16. Providing assistance in communicating with QHP Issuers;
17. Fulfilling the legal responsibilities related to the efficient functions of QHP Issuers in the FFEs and SBE-FPs, as permitted or required by a Web-broker EDE Entity's contractual relationships with QHP Issuers; and
18. Performing other functions substantially similar to those enumerated above and such other functions that CMS may approve in writing from time to time.

b. Collection of PII. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, EDE Entity may create, collect, disclose, access, maintain, store, and use the following PII from Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives— including, but not limited to:

- APTC percentage and amount applied
- Auto disenrollment information
- Applicant name
- Applicant address
- Applicant birthdate
- Applicant telephone number
- Applicant email
- Applicant Social Security Number
- Applicant spoken and written language preference
- Applicant Medicaid Eligibility indicator, start and end dates
- Applicant CHIP eligibility indicator, start and end dates
- Applicant QHP eligibility indicator, start and end dates
- Applicant APTC percentage and amount applied eligibility indicator, start and end dates
- Applicant household income
- Applicant maximum APTC amount
- Applicant CSR eligibility indicator, start and end dates
- Applicant CSR level
- Applicant QHP eligibility status change
- Applicant APTC eligibility status change
- Applicant CSR eligibility status change
- Applicant Initial or Annual Open Enrollment Indicator, start and end dates
- Applicant Special Enrollment Period (“SEP”) eligibility indicator and reason code
- Contact name
- Contact address
- Contact birthdate
- Contact telephone number
- Contact email
- Contact spoken and written language preference
- Enrollment group history (past six months)
- Enrollment type period
- FFE Applicant ID
- FFE Member ID
- Issuer Member ID
- Net premium amount
- Premium amount, start and end dates

- Credit or Debit Card Number, name on card
  - Checking account and routing number
  - SEP reason
  - Subscriber indicator and relationship to subscriber
  - Tobacco use indicator and last date of tobacco use
  - Custodial parent
  - Health coverage
  - American Indian/Alaska Native status and name of tribe
  - Marital status
  - Race/ethnicity
  - Requesting financial assistance
  - Responsible person
  - Dependent name
  - Applicant/dependent sex
  - Student status
  - Subscriber indicator and relationship to subscriber
  - Total individual responsibility amount
  - Immigration status
  - Immigration document number
  - Naturalization document number
- c. Security and Privacy Controls. EDE Entity agrees to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including the NEE SSP. Furthermore, EDE Entity agrees to timely inform the Exchange of any material change in its administrative, technical, or operational environments, or any material change that would require an alteration of the privacy and security standards within this Agreement through the EDE Entity-initiated Change Request process (Section IX.c of this Agreement).
- d. Use of PII. PII collected from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—in the context of completing an application for QHP, APTC, or CSR eligibility, if applicable, or enrolling in a QHP, or any data transmitted from or through the Hub, if applicable, may be used only for Authorized Functions specified in Section III.a of this Agreement. Such PII may not be used for purposes other than authorized by this Agreement or as consented to by a Consumer, Applicant, Qualified Individual, and Enrollee—or these individuals’ legal representatives or Authorized Representatives.
- e. Collection and Use of PII Provided Under Other Authorities. This Agreement does not preclude EDE Entity from collecting PII from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—for a non-FFE/non-SBE-FP/non-Hub purpose, and using, reusing, and disclosing PII obtained as permitted by applicable law and/or other applicable

authorities. Such PII must be stored separately from any PII collected in accordance with Section III.b of this Agreement.

- f. Ability of Individuals to Limit Collection and Use of PII. EDE Entity agrees to provide the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—the opportunity to opt in to have EDE Entity collect, create, disclose, access, maintain, store, and use their PII. EDE Entity agrees to provide a mechanism through which the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—can limit the collection, creation, disclosure, access, maintenance, storage and use of his or her PII for the sole purpose of obtaining EDE Entity’s assistance in performing Authorized Functions specified in Section III.a of this Agreement.
- g. Downstream and Delegated Entities. EDE Entity will satisfy the requirement in 45 C.F.R. § 155.260(b)(2)(v) to require Downstream and Delegated Entities to adhere to the same privacy and security standards that apply to Non-Exchange Entities by entering into written agreements with any Downstream and Delegated Entities that will have access to PII collected in accordance with this Agreement. EDE Entity must require in writing all Downstream and Delegated Entities adhere to the terms of this Agreement.

Upon request, EDE Entity must provide CMS with information about its downstream Agents/Brokers, EDE Entity’s oversight of its downstream Agents/Brokers, and the EDE Environment(s) it provides to each of its downstream Agents/Brokers.

- h. Commitment to Protect PII. EDE Entity shall not release, publish, or disclose Consumer, Applicant, Qualified Individual, or Enrollee PII to unauthorized personnel, and shall protect such information in accordance with provisions of any laws and regulations governing the adequate safeguarding of Consumer, Applicant, Qualified Individual, or Enrollee PII, the misuse of which carries with it the potential to cause financial, reputational, and other types of harm.
  - 1. Technical leads must be designated to facilitate direct contacts between the Parties to support the management and operation of the interconnection.
  - 2. The overall sensitivity level of data or information that will be made available or exchanged across the interconnection will be designated as MODERATE as determined by Federal Information Processing Standards (FIPS) Publication 199.
  - 3. EDE Entity agrees to comply with all federal laws and regulations regarding the handling of PII—regardless of where the organization is located or where the data are stored and accessed.
  - 4. EDE Entity’s Rules of Behavior must be at least as stringent as the HHS Rules of Behavior.<sup>3</sup>

---

<sup>3</sup> The HHS Rules of Behavior are available at the following link: <https://www.hhs.gov/ocio/policy/hhs-rob.html>.

5. EDE Entity understands and agrees that all financial and legal liabilities arising from inappropriate disclosure or Breach of Consumer, Applicant, Qualified Individual, or Enrollee PII while such information is in the possession of EDE Entity shall be borne exclusively by EDE Entity.
6. EDE Entity shall train and monitor staff on the requirements related to the authorized use and sharing of PII with third parties and the consequences of unauthorized use or sharing of PII, and periodically audit their actual use and disclosure of PII.

IV. Effective Date and Term; Renewal.

- a. Effective Date and Term. This Agreement becomes effective on the date the last of the two Parties executes this Agreement and ends the Day before the first Day of the open enrollment period (“OEP”) under 45 C.F.R. § 155.410(e)(3) for the benefit year beginning January 1, 2025.
- b. Renewal. This Agreement may be renewed upon the mutual agreement of the Parties for subsequent and consecutive one (1) year periods upon thirty (30) Days’ advance written notice to EDE Entity.

V. Termination.

- a. Termination without Cause. Either Party may terminate this Agreement without cause and for its convenience upon thirty (30) Days’ prior written notice to the other Party.  
  
EDE Entity must reference and complete the NEE Decommissioning Plan and NEE Decommissioning Close Out Letter in situations where EDE Entity will retire or decommission its EDE Environment.<sup>4</sup>
- b. Termination of Agreement with Notice by CMS. The termination of this Agreement and the reconsideration of any such termination shall be governed by the termination and reconsideration standards adopted by the FFEs or SBE-FPs under 45 C.F.R. § 155.220. Notwithstanding the foregoing, EDE Entity shall be considered in “Habitual Default” of this Agreement in the event that it has been served with a non-compliance notice under 45 C.F.R. § 155.220(g) or an immediate suspension notice under Section V.c of this Agreement more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately terminate this Agreement upon notice to EDE Entity without any further opportunity to resolve the Breach and/or non-compliance.
- c. Termination of Interconnection for Non-compliance. Instances of non-compliance with the privacy and security standards and operational requirements under this Agreement by EDE Entity, which may or may not rise to the level of a material Breach of this Agreement, may lead to termination of the interconnection between the Parties. CMS may block EDE Entity’s access to CMS systems if EDE Entity does not

---

<sup>4</sup> The Non-Exchange Entity (NEE) Decommissioning Plan and NEE Decommissioning Close Out Letter are available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.



- implement reasonable precautions to prevent the risk of Security Incidents spreading to CMS' network or based on the existence of unmitigated privacy or security risks, or the misuse of the PII of Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives. In accordance with Section X.m of this Agreement, CMS is authorized to audit the security of EDE Entity's network and systems periodically by requesting that EDE Entity provide documentation of compliance with the privacy and security requirements in this Agreement and in the ISA. EDE Entity shall provide CMS access to its information technology resources impacted by this Agreement for the purposes of audits. CMS may suspend or terminate the interconnection if EDE Entity does not comply with such a compliance review request within seven (7) business days, or within such longer time period as determined by CMS. Further, notwithstanding Section V.b of this Agreement, CMS may immediately suspend EDE Entity's ability to transact information with the FFEs or SBE-FPs via use of its EDE Environment if CMS discovers circumstances that pose unacceptable or unmitigated risk to FFE operations or CMS information technology systems. If EDE Entity's ability to transact information with the FFEs or SBE-FPs is suspended, CMS will provide EDE Entity with written notice within two (2) business days.
- d. Effect of Termination. Termination of this Agreement will result in termination of the functionality and electronic interconnection(s) covered by this Agreement, but will not affect obligations under EDE Entity's other respective agreement(s) with CMS, including the QHP Issuer Agreement, the Web-broker Agreement, or the Agent Broker General Agreement for Individual Market Federally-Facilitated Exchanges and State-Based Exchanges on the Federal Platform (Agent/Broker Agreement). However, the termination of EDE Entity's ISA, QHP Issuer Agreement, or Web-broker Agreement will result in termination of this Agreement and termination of EDE Entity's connection to CMS systems, including its connection to the Hub and ability to access the EDE suite of APIs as allowed by this Agreement. CMS may terminate this Agreement and EDE Entity's connection to CMS systems, consistent with this clause, if a Designated Representative, who is associated with the EDE Entity, has their Agent/Broker Agreement terminated by CMS.
- e. Notice to Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—of Termination of the Interconnection/Agreement, Suspension of Interconnection, and Nonrenewal of Agreement. EDE Entity must provide Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—with written notice of termination of this Agreement without cause, as permitted under Section V.a of this Agreement, no less than ten (10) Days prior to the date of termination. Within ten (10) Days after termination or expiration of this Agreement or termination or suspension of the interconnection, EDE Entity must provide Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—with written notice of termination of this Agreement with cause under Section V.b of this Agreement; termination or suspension of the interconnection for non-compliance under Section V.c of this Agreement; termination resulting from termination of EDE Entity's ISA,



QHP Issuer Agreement, or Web-broker Agreement under Section V.d of this Agreement; or non-renewal of this Agreement.

The written notice required by this Section shall notify each Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—of the date the termination or suspension of the interconnection will or did occur and direct the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—to access his or her application through the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]) after that date. The written notice shall also provide sufficient details to the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—, including, but not limited to the Consumer's, Applicant's, Qualified Individual's, or Enrollee's Application ID, pending actions, and enrollment status, to allow the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—to update his or her application and provide the next steps necessary to update the Consumer's, Applicant's, Qualified Individual's, or Enrollee's application through the FFE. If EDE Entity's interconnection has been suspended, the written notice must also state that EDE Entity will provide updates to the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—regarding the Consumer's, Applicant's, Qualified Individual's, or Enrollee's—or these individuals' legal representatives or Authorized Representatives—ability to access his or her application through EDE Entity's website in the future.

In addition to providing written notice to Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—EDE Entity must also prominently display notice of the termination or suspension of the interconnection on EDE Entity's website, including language directing Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—to access their applications through the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]).

This clause will survive the expiration or termination of this Agreement.

- f. Destruction of PII. EDE Entity covenants and agrees to destroy all PII in its possession at the end of the record retention period required under the NEE SSP. EDE Entity's duty to protect and maintain the privacy and security of PII, as provided for in the NEE SSP, shall continue in full force and effect until such PII is destroyed and shall survive the termination or expiration of this Agreement.

This clause will survive expiration or termination of this Agreement.

VI. Use of EDE Entity's EDE Environment by Agents, Brokers, or DE Entity Application Assisters.

- a. General. EDE Entity may allow third-party Agents, Brokers, or DE Entity Application Assisters that are not or will not be a party to their own EDE Agreement with CMS to enroll Qualified Individuals in QHPs and to assist individuals in applying for APTC and CSRs through EDE Entity's EDE Environment. EDE Entity, or an Upstream EDE Entity<sup>5</sup> for which EDE Entity provides an EDE Environment, must have a contractual and legally binding relationship with its third-party Agents, Brokers, or DE Entity Application Assisters reflected in a signed, written agreement between the third-party Agents, Brokers, or DE Entity Application Assisters and EDE Entity.

Except as provided in this Section, or as documented for CMS review and approval consistent with Section IX.c of this Agreement as a data connection in the ISA, EDE Entity may not establish a data connection between a third-party Agent's or Broker's website and the EDE Entity's EDE Environment that transmits any data.

The use of embedding tools and programming techniques, such as iframe technical implementations, which may enable the distortion, manipulation, or modification of the audited and approved EDE Environment and the overall EDE End-User Experience developed by a Primary EDE Entity, are prohibited unless explicitly approved through the EDE Entity-initiated Change Request process consistent with Section IX.c of this Agreement.

The EDE Entity environment must limit the number of concurrent sessions to one (1) session per a single set of credentials/FFE user ID. However, multiple sessions associated with a single set of credentials/FFE user ID that is traceable to a single device/browser is permitted.

- b. Downstream White-Label Third-Party User Arrangement Requirements. Downstream third-party Agent and Broker arrangements may be Downstream White-Label Third-Party User Arrangements for which a Primary EDE Entity enables the third-party Agent or Broker to only make minor branding changes to the Primary EDE Entity's EDE Environment (i.e., adding an Agent's or Broker's logo or name to an EDE Environment). The use of embedding tools and programming techniques, such as iframe technical implementations, which may enable the distortion, manipulation, or modification of the audited and approved EDE Environment and the overall EDE End-User Experience developed by a Primary EDE Entity, are prohibited unless explicitly approved through the EDE Entity-initiated Change Request process consistent with Section IX.c of this Agreement.
- c. Downstream White-Label Third-Party User Arrangement Data Exchange Limited Flexibility. With prior written approval from CMS, Downstream White-Label Third-Party User Arrangements may allow limited data collection from the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal

---

<sup>5</sup> Permissible Upstream EDE Entity arrangements are defined in Sections VIII.f, VIII.g, and VIII.h of this Agreement.

representatives or Authorized Representatives—on the Downstream third-party Agent’s or Broker’s website that can be used in the EDE End-User Experience via a one-way limited data connection to the Primary EDE Entity’s EDE Environment. The following types of limited data collection by the third-party Agent’s or Broker’s website are permissible under this clause: 1) data to determine if a Consumer, Applicant, Qualified Individual, or Enrollee is (or should be) shopping for QHPs, such as basic information to assess potential eligibility for financial assistance, as well as to estimate premiums (e.g., household income, ages of household members, number of household members, and tobacco use status); and 2) data related to the Consumer’s, Applicant’s, Qualified Individual’s, or Enrollee’s service area (e.g., zip code, county, and State).

As part of the EDE-facilitated application and QHP enrollment processes, EDE Entity must not enable or allow the selection of QHPs by a Consumer or Agent/Broker on a third-party website that exists outside of the EDE Entity’s approved DE Environment. This includes pre-populating or pre-selecting a QHP for a Consumer that was selected on a downstream Agent’s/Broker’s website or a lead generator’s website. This prohibition does not extend to websites that are provided, owned, and maintained by entities subject to CMS regulations for QHP display (i.e., Web-brokers and QHP Issuers).

In any limited data collection arrangement, the data must be transmitted securely and in one direction only (i.e., from the downstream Agent or Broker to the Primary EDE Entity’s EDE Environment). EDE Entity must not provide access to Consumer, Applicant, Qualified Individual, or Enrollee data to the third-party Agent or Broker outside of the EDE End-User Experience unless otherwise specified in Sections III.d, III.e, and III.f of this Agreement. Additionally, the Downstream White-Label Third-Party User Arrangement must not involve additional data exchanges beyond what is outlined above as permissible, which takes place in conjunction with the initial redirect prior to the beginning of the EDE End-User Experience on the Primary EDE Entity’s EDE Environment.

- d. Oversight Responsibilities. EDE Entity may only allow third-party Agents, Brokers, and DE Entity Application Assisters who are validly registered with the FFE for the applicable plan year to use its approved EDE Environment. EDE Entity must not provide access to its approved EDE Environment, the EDE End-User Experience or any data obtained via the EDE End-User Experience to an Agent or Broker until the Agent or Broker has completed the process for Agent or Broker Identity Proofing consistent with the requirements in Section IX.r of this Agreement.

## VII. QHP Issuer Use of an EDE Environment.

QHP Issuer EDE Entities, operating as Primary EDE Entities or Upstream EDE Entities, must bind all affiliated Issuer organizations (i.e., HIOS IDs) that use its EDE Environment or EDE End-User Experience—either for Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—use or Agent or Broker use—to the terms and provisions of this Agreement. QHP Issuer EDE Entities must identify all applicable affiliated Issuer organizations that will use its EDE Environment during the

onboarding process in the “Operational and Oversight Information” form provided by CMS<sup>6</sup>. The signatory of this Agreement on behalf of the QHP Issuer EDE Entity must have sufficient authority to execute an agreement with CMS on behalf of the QHP Issuer EDE Entity and all affiliated QHP Issuer organizations that use the QHP Issuer EDE Entity’s EDE Environment or EDE End-User Experience. QHP Issuer EDE Entities must identify all applicable affiliated QHP Issuer organizations in the “Operational and Oversight Information” form provided by CMS.

#### VIII. Audit Requirements.

- a. Operational Readiness Review (“ORR”). In order to receive approval to participate in EDE and utilize an integrated EDE Environment, EDE Entity must contract with one or more independent Auditor(s) consistent with this Agreement’s provisions and applicable regulatory requirements to conduct an ORR, composed of a business requirements audit and a privacy and security audit.<sup>7</sup> EDE Entity must follow the detailed guidance CMS provided in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.<sup>8</sup>

The Auditor must document and attest in the ORR report that EDE Entity’s EDE Environment, including its website and operations, complies with the terms of this Agreement, the ISA, EDE Entity’s respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement), the Framework for the Independent Assessment of Security and Privacy Controls for Enhanced Direct Enrollment Entities,<sup>9</sup> and applicable program requirements. If an EDE Entity will offer its EDE Environment in a State in which a non-English language is spoken by a Limited English Proficient (LEP) population that reaches ten (10) percent or more of the State’s population, as determined in guidance published by the Secretary of HHS,<sup>10</sup> the Auditor conducting EDE Entity’s business requirements audit must also audit the non-English language version of the application user interface (UI) and any critical communications EDE Entity sends Consumers, Applicants, Qualified Individuals, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—in relation to their use of its EDE Environment for compliance with

<sup>6</sup> The Operational and Oversight Information form is available in the PY 2023 DE Documentation Package zip file on CMS zONE at the following link: <https://zone.cms.gov/document/business-audit>.

<sup>7</sup> The Auditor must use NIST SP 800-53A, which describes the appropriate assessment procedure (examine, interview, and test) for each control to evaluate that the control is effectively implemented and operating as intended.

<sup>8</sup> This document is available at the following link: <https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf>.

<sup>9</sup> This document is available at the following link within the Privacy and Security Templates Resources: <https://zone.cms.gov/document/privacy-and-security-audit>.

<sup>10</sup> Guidance and Population Data for Exchanges, Qualified Health Plan Issuers, and Web-Brokers to Ensure Meaningful Access by Limited-English Proficient Speakers Under 45 CFR §155.205(c) and §156.250 (March 30, 2016) <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Language-access-guidance.pdf> and “Appendix A- Top 15 Non-English Languages by State” [https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508\\_update12-20-16.pdf](https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508_update12-20-16.pdf). HHS may release revised guidance. DE Entity should refer to the most current HHS guidance.

applicable CMS requirements. EDE Entity must submit the resulting business requirements and privacy and security audit packages to CMS.

The ORR must detail EDE Entity's compliance with the requirements set forth in Appendix C, including any requirements set forth in CMS guidance referenced in Appendix C.<sup>11</sup> The business requirements and privacy and security audit packages EDE Entity submits to CMS must demonstrate that EDE Entity's Auditor(s) conducted its review in accordance with the review standards set forth in Appendix C and in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.

CMS will approve EDE Entity's EDE Environment only once it has reviewed and approved the business requirements audit and privacy and security audit findings reports. Final approval of EDE Entity's EDE Environment will be evidenced by CMS countersigning the ISA with EDE Entity. Upon receipt of the counter-signed ISA, EDE Entity will be approved to use its approved EDE Environment consistent with applicable regulations, this Agreement, and the ISA.

- b. Identification of Auditor(s) and Subcontractors of Auditor(s). All Auditor(s), including any Auditor(s) that has subcontracted with EDE Entity's Auditor(s), will be considered Downstream or Delegated Entities of EDE Entity pursuant to EDE Entity's respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement) and applicable program requirements. EDE Entity must identify each Auditor it selects, and any subcontractor(s) of the Auditor(s), in Appendix E of this Agreement. EDE Entity must also submit a copy of the signed agreement or contract between the Auditor(s) and EDE Entity to CMS.
- c. Conflict of Interest. For any arrangement between EDE Entity and an Auditor for audit purposes covered by this Agreement, EDE Entity must select an Auditor that is free from any real or perceived conflict(s) of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. EDE Entity must disclose to HHS any financial relationships between the Auditor, and individuals who own or are employed by the Auditor, and individuals who own or are employed by an EDE Entity for which the Auditor is conducting an ORR pursuant to 45 C.F.R. §§ 155.221(b)(4) and (f). EDE Entity must document and disclose any conflict(s) of interest in the form in Appendix F, if applicable.
- d. Auditor Independence and Objectivity. EDE Entity's Auditor(s) must remain independent and objective throughout the audit process for both audits. An Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the EDE Environment and the determination of security and privacy control effectiveness or business requirement compliance. EDE Entity must not take any actions that impair

---

<sup>11</sup> The table in Appendix C is an updated version of Exhibit 2 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

the independence and objectivity of EDE Entity's Auditor. EDE Entity's Auditor must attest to their independence and objectivity in completing the EDE audit(s).

- e. Required Documentation. EDE Entity must maintain and/or submit the required documentation detailed in Appendix D, including templates provided by CMS, to CMS in the manner specified in Appendix D.<sup>12</sup> Documentation that EDE Entity must submit to CMS (as set forth in Appendix D) will constitute EDE Entity's EDE Application.
- f. Use of an EDE Environment by a QHP Issuer with Minor Branding Deviations (White-Label Issuer Upstream EDE Entity).

A QHP Issuer EDE Entity may use an approved EDE Environment provided by a Primary EDE Entity. If a QHP Issuer EDE Entity implements and uses an EDE Environment that is identical to its Primary EDE Entity's EDE Environment, except for minor deviations for branding or QHP display changes relevant to the Issuer's QHPs, the QHP Issuer EDE Entity is not required to submit a business requirements audit package and privacy and security audit package. CMS refers to a QHP Issuer EDE Entity operating consistent with this Section as a White-Label Issuer Upstream EDE Entity. In all arrangements permitted under this Section, all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions specified in Section III.a of this Agreement must be conducted within the confines of the Primary EDE Entity's approved EDE Environment.

In all arrangements permitted under this Section, the White-Label Issuer Upstream EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265 and 156.1230, operational requirements, this Agreement, and the ISA. Any Primary EDE Entity supplying an EDE Environment to a White-Label Issuer Upstream EDE Entity will be considered a Downstream or Delegated Entity of the White-Label Issuer Upstream EDE Entity. A White-Label Issuer Upstream EDE Entity must identify its Primary EDE Entity in the "Operational and Oversight Information" form provided by CMS. A White-Label Issuer Upstream EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the White-Label Issuer Upstream EDE Entity and the Primary EDE Entity.

- g. Use of an EDE Environment by a QHP Issuer with Additional Functionality or Systems (Hybrid Issuer Upstream EDE Entity).

If a QHP Issuer EDE Entity will implement its own EDE Environment composed, in part, of an approved EDE Environment provided by a Primary EDE Entity and, in

---

<sup>12</sup> The table in Appendix D is a combined version of Exhibits 4 and 7 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."



part, of additional functionality or systems implemented by or on behalf of the QHP Issuer EDE Entity, the QHP Issuer EDE Entity may be required to retain an Auditor to conduct part(s) of the ORR relevant to functionalities and systems implemented by the QHP Issuer EDE Entity outside of the Primary EDE Entity's EDE Environment, or in addition to the Primary EDE Entity's approved EDE Environment, and to analyze the effect, if any, of those functionalities and systems on the operations and compliance of the Primary EDE Entity's approved EDE Environment. CMS refers to a QHP Issuer EDE Entity operating consistent with this Section as a Hybrid Issuer Upstream EDE Entity. In this scenario, the Hybrid Issuer Upstream EDE Entity may be required to submit to CMS an ORR audit package that contains the results of the supplemental business requirements audit and/or privacy and security audit, as appropriate, in which the Auditor reviewed the additional functionality or systems implemented by or on behalf of the Hybrid Issuer Upstream EDE Entity. The Hybrid Issuer Upstream EDE Entity may be required to submit to CMS an ORR consisting of the results of its Auditor's review of its implementation of non-inheritable, Hybrid and inheritable but not inherited EDE privacy and security controls. The ORR audit package that contains the results of the business requirements audit and/or privacy and security audit covering additional functionality or systems implemented by or on behalf of the Hybrid Issuer Upstream EDE Entity must demonstrate the Hybrid Issuer Upstream EDE Entity's compliance with applicable regulations, operational requirements, this Agreement, and the ISA. The Hybrid Issuer Upstream EDE Entity does not need to submit the Primary EDE Entity's ORR.

CMS considers any changes to the Primary EDE Entity's approved EDE Environment or the overall EDE End-User Experience—beyond minor deviations for branding or QHP display changes relevant to the Issuer's QHPs—to be the addition of functionality or systems to an approved EDE Environment subject to the requirements of this Section.

CMS has identified the following non-exclusive list as additional functionality that requires a supplemental audit submission:

1. Hybrid Issuer Upstream EDE Entities implementing a single sign-on (SSO) solution must retain an Auditor to conduct a supplemental security and privacy audit and submit the results to CMS consistent with the EDE Guidelines.<sup>13</sup>

In all arrangements permitted under this paragraph, the Hybrid Issuer Upstream EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265, and 156.1230, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265 and 156.1230, operational requirements, this Agreement, and the ISA. Any

---

<sup>13</sup> A Hybrid Issuer Upstream EDE Entity implementing a SSO solution may leverage prior audit results that assessed some or all control requirements listed in Exhibit 14 of the EDE Guidelines, available at the following link: <https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf> if the prior audit was conducted within one year of the date of submission of the audit documentation to CMS.

Primary EDE Entity supplying an EDE Environment to the Hybrid Issuer Upstream EDE Entity will be considered a Downstream or Delegated Entity of the Hybrid Issuer Upstream EDE Entity. A Hybrid Issuer Upstream EDE Entity must identify its Primary EDE Entity in the “Operational and Oversight Information” form provided by CMS . The Hybrid Issuer Upstream EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the Hybrid Issuer Upstream EDE Entity and the Primary EDE Entity. The Primary EDE Entity must identify inheritable Common Controls and Hybrid Controls that the Hybrid Issuer Upstream EDE Entity should leverage. The inherited Common Controls and Hybrid Controls must be documented in the NEE SSP Template and must also be documented as part of the written contract between the Primary EDE Entity and the Hybrid Issuer Upstream EDE Entity.

A Hybrid Issuer Upstream EDE Entity operating under this provision cannot provide access to its EDE Environment to another Issuer or a Hybrid Non-Issuer Upstream EDE Entity.

h. Use of an EDE Environment by a Non-Issuer Entity with Additional Functionality or Systems (Hybrid Non-Issuer Upstream EDE Entity).

If a Hybrid Non-Issuer Upstream EDE Entity will implement its own EDE Environment composed, in part, of an approved EDE Environment provided by a Primary EDE Entity and, in part, of additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer Upstream EDE Entity, the Hybrid Non-Issuer EDE Entity must retain an Auditor to conduct part(s) of the ORR relevant to functionalities and systems implemented by the Hybrid Non-Issuer EDE Entity outside of the Primary EDE Entity’s EDE Environment, or in addition to the Primary EDE Entity’s approved EDE Environment, and to analyze the effect, if any, of those functionalities and systems on the operations and compliance of the Primary EDE Entity’s approved EDE Environment.<sup>14</sup> In this scenario, the Hybrid Non-Issuer EDE Entity must submit an ORR consisting of the results of its Auditor’s review of its implementation of non-inheritable, Hybrid and inheritable but not inherited EDE privacy and security controls. The Hybrid Non-Issuer EDE Entity may also be required to submit to CMS a supplemental ORR audit package that contains the results of any supplemental business requirements and/or privacy and security audits, as appropriate, in which the Auditor reviewed the additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer EDE Entity.<sup>15</sup> The ORR, and

---

<sup>14</sup> With respect to Agents and Brokers regulated by this section as Hybrid Non-Issuer Upstream EDE Entities, these arrangements are distinct and independent from those arrangements regulated under Section VI of this Agreement. An Agent or Broker in a limited data-sharing arrangement consistent with Section VI.c of this Agreement would not necessarily also be subject to the requirements for Hybrid Non-Issuer Upstream EDE Entities under Section VIII.h of this Agreement. The determination of what requirements apply to a particular arrangement will be a fact heavy analysis that takes into account the specific details of the arrangement.

<sup>15</sup> A Hybrid Non-Issuer Upstream EDE Entity may leverage prior audit results that assessed some or all control requirements listed in Exhibit 12 and Exhibit 13 of Appendix A of the EDE Guidelines, if the prior audit was conducted within one year of the date of submission of the audit documentation to CMS. The EDE Guidelines are available at the following link:

<https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf>.



supplemental ORR audit package that contains the results of the supplemental business requirements audit and/or privacy and security audit covering additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer EDE Entity (when required), must demonstrate the Hybrid Non-Issuer EDE Entity's compliance with applicable regulations, operational requirements, this Agreement, and the ISA. The Hybrid Non-Issuer EDE Entity does not need to submit the Primary EDE Entity's ORR.

CMS considers any changes to the Primary EDE Entity's approved EDE Environment or the overall EDE End-User Experience beyond minor deviations for branding to be the addition of functionality or systems to an approved EDE Environment subject to the requirements of this Section. In all arrangements permitted under this paragraph, the Hybrid Non-Issuer EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements as defined in 45 C.F.R. §§ 155.220(c) and 155.221, operational requirements, this Agreement, and the ISA. Any Primary EDE Entity supplying an EDE Environment to the Hybrid Non-Issuer EDE Entity will be considered a Downstream or Delegated Entity of the Hybrid Non-Issuer EDE Entity. A Hybrid Non-Issuer EDE Entity must identify its Primary EDE Entity in the "Operational and Oversight Information" form provided by CMS. The Hybrid Non-Issuer EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the Hybrid Non-Issuer EDE Entity and the Primary EDE Entity. The Primary EDE Entity must identify inheritable Common Controls and Hybrid Controls that the Hybrid Non-Issuer EDE Entity should leverage. The inherited Common Controls and Hybrid Controls must be documented in the NEE SSP Template and must also be documented as part of the written contract between the Primary EDE Entity and the Hybrid Non-Issuer EDE Entity.

Depending on the additional functionality and systems added, the Hybrid Non-Issuer EDE Entity may also need to onboard and register with CMS as a Web-broker. For example, a Hybrid Non-Issuer EDE Entity that hosts its own QHP display or plan shopping experience as part of the EDE End-User Experience must be registered with CMS as a Web-broker.

The QHP display or plan shopping experience displayed in the EDE End-User Experience provided to or operated by a Hybrid Non-Issuer EDE Entity must comply with the requirements of 45 C.F.R. §§ 155.220 and 155.221.

When onboarding, annually during agreement renewal, and upon request, the Hybrid Non-Issuer EDE Entity must provide CMS operational information, including, but not limited to, its Designated Representative's National Producer Number (NPN), State licensure information, and information about its downstream agents/brokers, if applicable. The Designated Representative designated by the Hybrid Non-Issuer EDE

Entity must have completed registration and, if applicable, training with the FFE consistent with 45 C.F.R. § 155.220(d).

A Hybrid Non-Issuer EDE Entity operating under this provision cannot provide access to its EDE Environment to an Issuer or another Hybrid Non-Issuer Upstream EDE Entity.

IX. FFE Eligibility Application and Enrollment Requirements.

- a. FFE Eligibility Application End-State Phases and Phase-Dependent Screener Questions. Appendix G describes each of the three end-state phases for hosting applications using the EDE Pathway (Phase 1, Phase 2, and Phase 3).<sup>16</sup> EDE Entity must select and implement an end-state phase. If EDE Entity has selected application end-state Phase 1 or Phase 2, it must implement the requirements related to phase-dependent screener questions set forth in Appendix C. In addition, EDE Entity must meet any end-state phase-related communications requirements established by CMS. EDE Entity must indicate the phase it has selected in the “Operational and Oversight Information” form provided by CMS.

The business requirements audit package EDE Entity submits to CMS must demonstrate that EDE Entity’s EDE Environment meets all requirements associated with EDE Entity’s selected phase, as set forth in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements,<sup>17</sup> Enhanced Direct Enrollment API Companion Guide,<sup>18</sup> and FFE UI Application Principles for Integration with FFE APIs.<sup>19</sup> EDE Entity must consult CMS prior to switching phases. If EDE Entity decides to switch to a different phase after its Auditor has completed the business requirements audit, EDE Entity’s Auditor must conduct portions of a revised business requirements audit to account for the changes to the EDE Environment necessary to implement the new end-state phase selected by EDE Entity to confirm compliance with all applicable requirements.

- b. EDE Entity Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—Support for Term of Agreement. EDE Entity’s EDE Environment must support Consumer-, Applicant-, Qualified Individual-, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—reported Changes in Circumstances (CiCs), inclusive of SEP CiCs and non-SEP CiCs, and SEPs within EDE Entity’s chosen end-state phase for the full term of this Agreement, as well as supporting re-enrollment application activities. Furthermore, all EDE Entities, regardless of the phase chosen, must support households that wish to enroll in more than one enrollment group. Consistent with the general expectations for EDE requirements—that the EDE requirements are

<sup>16</sup> The table in Appendix G is an updated version of Exhibit 3 in the “Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.”

<sup>17</sup> See supra note 8.

<sup>18</sup> The document Enhanced Direct Enrollment API Companion *Guide* is available at the following link: <https://zone.cms.gov/document/api-information>.

<sup>19</sup> The document FFE UI Application Principles for Integration with FFE APIs is available at the following link: <https://zone.cms.gov/document/eligibility-information>.

implemented for and provided to all users of an EDE Environment—Primary EDE Entities must provide the functionalities described in this paragraph for all users of the Primary EDE Entity’s EDE Environment, including any Upstream EDE Entities and their users (e.g., Downstream Agents and Brokers).

If EDE Entity is no longer operating an EDE Environment, EDE Entity must direct the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals’ legal representatives or Authorized Representatives—to the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]). EDE Entity should take reasonable steps to continue supporting households that have used their EDE Environment in the past to transfer to the new EDE Pathway. CMS suggests that reasonable steps would include: send written notices to Consumers of the steps to create an account/transfer their account to the different Primary EDE Entity, provide the requisite information for them to create an account on that other site or carry their information to a different pathway, and provide a notice on the site that EDE Entity has transitioned its EDE Pathway to a different environment. EDE Entity can go beyond these limited, minimum requirements in easing the Consumer transition to [New Entity] and should follow the EDE Entity-initiated Change Request process as described in Section IX.c of this Agreement for this functionality as appropriate

This provision survives the termination of the Agreement.

- c. EDE Entity-initiated Modifications to EDE Environment (EDE Entity-initiated Change Requests and EDE Entity-initiated Phase Change Requests). EDE Entity must notify CMS immediately if it intends to make any change to its audited or approved EDE Environment, including when EDE Entity opts to change to a different EDE application phase (from its approved or audited EDE phase), consistent with the processes and standards defined by CMS in the Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems.<sup>20</sup> CMS excludes changes made in response to an Auditor’s documented findings (if the findings were submitted to CMS), to CMS technical assistance, or to resolve compliance findings from being subject to the procedures detailed in the Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems.
- d. CMS-initiated Modifications to EDE Program Requirements (CMS-initiated Change Requests). CMS will periodically release updates to EDE program requirements in the form of CMS-initiated Change Requests (CRs); these CMS-initiated CRs are documented in the EDE Change Request Tracker.<sup>21</sup> EDE Entity must provide specified documentation to CMS demonstrating its implementation of applicable CMS-initiated CRs by the CMS-established deadline. EDE Entity must make any CMS-mandated changes within the timeline established by CMS to make such changes. If an EDE Entity does not timely submit documentation of its

<sup>20</sup> The document Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems is available at the following link: <https://zone.cms.gov/document/business-audit>.

<sup>21</sup> The EDE Change Request Tracker is located on CMS zONE: <https://zone.cms.gov/document/business-audit>.

implementation of such CRs, CMS may suspend the non-compliant EDE Entity's access to the EDE Pathway.

- e. Maintenance of an Accurate Testing Environment. EDE Entity must maintain a testing environment that accurately represents the EDE Entity's production environment and integration with the EDE Pathway, including functional use of all EDE APIs. Approved and Prospective Phase Change EDE Entities must maintain at least one testing environment that reflects their current production EDE environments when developing and testing any prospective changes to their production EDE environments. This will require Approved and Prospective Phase Change EDE Entities to develop one or more separate environments (other than production and the testing environment that reflects production) for developing and testing prospective changes to their production environments. Network traffic into and out of all non-production environments is only permitted to facilitate system testing and must be restricted by source and destination access control lists, as well as ports and protocols, as documented in the NEE SSP, SA-11 implementation standard. The EDE Entity shall not submit actual PII to the FFE Testing Environments. The EDE Entity shall not submit test data to the FFE Production Environments. The EDE Entity's testing environments shall be readily accessible to applicable CMS staff and contractors via the Internet to complete CMS audits.

EDE Entity must provide CMS, via the DE Help Desk, with a set of credentials and any additional instructions necessary so that CMS can access the testing environment that reflects the EDE Entity's production environment to complete audits of the EDE Entity's EDE Environment. EDE Entity must ensure that the testing credentials are valid and that all APIs and components of the EDE Environment in the testing environment, including the remote identity proofing (RIDP) services, are accessible for CMS to audit EDE Entity's EDE Environment as determined necessary by CMS.

- f. Penetration Testing. The EDE Entity must conduct penetration testing which examines the network, application, device, and physical security of its EDE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Before conducting the penetration testing, the EDE Entity must execute a Rules of Engagement with their Auditor's penetration testing team. The EDE Entity must also notify their CMS designated technical counterparts on their annual penetration testing schedule a minimum of five (5) business days prior to initiation of the penetration testing using the CMS-provided form.<sup>22</sup> During the penetration testing, the Auditor's testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment. The penetration testing shall be conducted in the lower environment that reflects the EDE Entity's current production environment, consistent with Section IX.e.

---

<sup>22</sup> The Penetration Testing Notification Form is available at the following links:  
<https://zone.cms.gov/document/privacy-and-security-audit>.

- g. Identity Proofing. EDE Entity must meet the identity proofing implementation requirements set forth in Appendix C.
- h. Accurate and Streamlined Eligibility Application UI. EDE Entity must meet the accurate and streamlined eligibility application UI requirements set forth in Appendix C.
- i. Post-Eligibility Application Communications. EDE Entity must provide account management functions for Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—and timely communicate with Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—regarding their application and coverage status. EDE Entity must meet all requirements related to post-eligibility application communications and account management functions set forth in Appendix C. In addition to those requirements, EDE Entity must update and report changes to the Consumer’s, Applicant’s, Qualified Individual’s, or Enrollee’s application and enrollment information to the FFE and must comply with future CMS guidance that elaborates upon EDE Entity’s duties under this Agreement and applicable regulations.
- j. Accurate Information About Exchanges and Consumer, Applicant, Qualified Individual, or Enrollee Communications. EDE Entity must meet the requirements related to providing to Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—accurate information about Exchanges and the Consumer, Applicant, Qualified Individual, or Enrollee communications requirements set forth in Appendix C. In addition, EDE Entity must meet the marketing-related communications requirements defined by CMS in the Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements and the Communications Toolkit.<sup>23</sup>
- k. Documentation of Interactions with Consumer, Applicant, Qualified Individual, or Enrollee Applications or the Exchange. EDE Entity must meet the requirements related to documentation of interactions with Consumer, Applicant, Qualified Individual, or Enrollee applications or the Exchange set forth in Appendix C.
- l. Eligibility Results Testing and Standalone Eligibility Service (SES) Testing. EDE Entity must meet the requirements related to eligibility results testing and SES testing set forth in Appendix C.
- m. API Functional Integration Requirements. EDE Entity must meet the API functional integration requirements set forth in Appendix C.
- n. Application UI Validation. EDE Entity must meet the application UI validation requirements set forth in Appendix C.

---

<sup>23</sup> The Communications Toolkit is stored within the Business Report Template and Toolkits file available at the following link: <https://zone.cms.gov/document/business-audit>.

- o. Section 508-compliant UI. EDE Entity must meet the 508-compliant UI requirements set forth in Appendix C.
- p. Non-English-Language Version of the Application UI and Communication Materials. EDE Entity must translate the Application UI and any critical communications EDE Entity sends Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—in relation to their use of its EDE Environment into any non-English language that is spoken by an LEP population that reaches ten percent or more of the population of the relevant State as set forth in Appendix C.
- q. Correction of Consumer, Applicant, Qualified Individual, or Enrollee Application Information. If EDE Entity identifies issues in its EDE Environment constituting noncompliance with the EDE program requirements as documented in Section IX of this Agreement that may affect the accuracy of a Consumer’s, Applicant’s, Qualified Individual’s, or Enrollee’s Application Information—including the Exchange’s eligibility determination or enrollment status—EDE Entity must notify CMS immediately by email to [directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov). For any such issues identified by EDE Entity or CMS, EDE Entity must provide CMS-requested data on a timeline established by CMS. CMS-requested data includes all data that CMS deems necessary to determine the scope of the issues and identify potentially affected Consumers, Applicants, Qualified Individuals, or Enrollees, including records maintained by EDE Entity consistent with Section IX.k of this Agreement. EDE Entity must provide assistance to CMS to identify the population of Consumers, Applicants, Qualified Individuals, or Enrollees potentially affected by the identified issues. EDE Entity must remedy CMS- or EDE Entity-identified issues in EDE Entity’s EDE Environment in a manner and timeline subject to CMS’ approval. CMS may require that EDE Entity submit updated application information within thirty (30) Days to correct inaccuracies in previously submitted applications. CMS may require that EDE Entity conduct necessary CMS-approved outreach to notify the potentially affected Consumers, Applicants, Qualified Individuals, or Enrollees of any action required by the Consumers, Applicants, Qualified Individuals, or Enrollees, if applicable, and of any changes in eligibility or enrollment status as a result of the issues.
- r. Agent/Broker Identity Proofing Requirements. EDE Entity must implement Agent and Broker identity verification procedures that consist of the following requirements:
  - 1. EDE Entity must provide the User ID of the requester in each EDE API call. For Agents and Brokers, the User ID must exactly match the FFE-assigned User-ID for the Agent or Broker using the EDE Environment or the request will fail FFE User ID validation.<sup>24</sup> As a reminder, for Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals’ legal representatives or Authorized Representatives—the User ID should be the account User ID for the

---

<sup>24</sup> In order for an Agent or Broker to obtain and maintain an FFE User ID, the Agent or Broker must complete registration and training with the Exchange annually.



Consumer, Applicant, Qualified Individual, or Enrollee or a distinct identifier for the Consumer, Applicant, Qualified Individual, or Enrollee.

2. EDE Entity must identity proof all Agents and Brokers prior to allowing the Agents and Brokers to use the EDE Environment. EDE Entity may conduct identity proofing in one of the following ways:
  - a. Use the FFE-provided Remote Identity Proofing/Fraud Solutions Archive Reporting Service (RIDP/FARS) or a Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS)-approved service to remotely identity-proof Agents and Brokers; OR
  - b. Manually identity-proof Agents and Brokers following the guidelines outlined in the document “Acceptable Documentation for Identity Proofing.”<sup>25</sup>
3. EDE Entity must validate an Agent’s or Broker’s National Producer number (NPN) using the National Insurance Producer Registry (<https://www.nipr.com>) prior to allowing the Agent or Broker to use the EDE Environment.
4. EDE Entity must review the Agent/Broker Suspension and Termination list prior to allowing the Agent or Broker to initially use the EDE Environment.<sup>26</sup>
5. If EDE Entity does not provide Agent or Broker identity proofing functionality consistent with the requirements above, EDE Entity cannot provide access to its EDE Environment to third-party Agents or Brokers. Furthermore, if a Primary EDE Entity does not provide Agent or Broker identity proofing functionality consistent with the requirements above, any Upstream EDE Entities that wish to use the Agent or Broker EDE Pathway must implement an Agent or Broker identity proofing approach consistent with these requirements prior to offering Agents or Brokers access to their EDE Environments. In such cases, the Upstream EDE Entities must contract with an independent Auditor to conduct an audit to evaluate the Agent or Broker identity proofing requirements consistent with this Section, and submit the audit to CMS for approval.
6. EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3.
7. EDE Entity must not permit Agents and Brokers using the EDE Environment to share access control credentials.
- s. Implement Full EDE API Suite of Required Services. EDE Entity must implement the full EDE API suite of required services, regardless of EDE Entity’s chosen application end-state phase. The suite of required services consists of the following APIs: Store ID Proofing, Person Search, Create App, Create App from Prior Year

---

<sup>25</sup> The document Acceptable Documentation for Identity Proofing is available on CMS zONE at the following link: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>.

<sup>26</sup> The Agent/Broker Suspension and Termination List is available at: <https://data.healthcare.gov/ab-suspension-and-termination-list>.

- App, Store Permission, Revoke Permission, Get App, Add Member, Remove Member, Update App, Submit App, Get Data Matching Issue (DMI), Get Special Enrollment Period Verification Issue (SVI), Metadata Search, Notice Retrieval, Submit Enrollment, Document Upload, System and State Reference Data, Get Enrollment, Payment Redirect<sup>27</sup>, Update Policy, and Event-Based Processing (EBP). CMS may release additional required or optional APIs during the term of this Agreement. If CMS releases a required API, the change will be considered a CMS-initiated Change Request consistent with Section IX.d of this Agreement.
- t. Maintain Full EDE API Suite of Required Services. In addition to any CMS-initiated Change Requests, CMS may make technical updates to Exchange systems or APIs that may affect EDE Entity's use of the EDE APIs. In order to maintain a functional EDE Environment and avoid errors or discrepancies when submitting data to and receiving data from the Exchange, EDE Entity must maintain an EDE Environment that implements changes as needed and documented in EDE technical documentation provided by CMS.<sup>28</sup>
- u. Health Reimbursement Arrangement (HRA) Offer Disclaimer. EDE Entity must implement disclaimers for Qualified Individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the Qualified Individuals consistent with CMS guidance. Disclaimers for various scenarios are detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.<sup>29</sup>
- v. Inactive, Approved Primary EDE Entities to Demonstrate Operational Readiness and Compliance. In order for an approved Primary EDE Entity to maintain status as an approved Primary EDE Entity during the annual renewal process for this Agreement, EDE Entity must demonstrate a history of enrollments completed via EDE during the term of the prior year's Agreement if the approved Primary EDE Entity has been approved for at least one year as determined by the date of the initial approval of the Primary EDE Entity and initial execution of the ISA. If the EDE Entity has been approved for at least one year and does not have a history of enrollments completed via EDE during the term of the prior year's Agreement, EDE Entity must demonstrate operational readiness and compliance with applicable requirements as documented in the EDE Guidelines in order to continue to participate as an approved Primary EDE Entity. Under this section, CMS may withhold execution of the subsequent plan year's Agreement and ISA or delay approval of an Upstream EDE Entity until EDE Entity has demonstrated operational readiness and compliance with applicable requirements to CMS's satisfaction.

---

<sup>27</sup> For information on exceptions to the requirement for EDE Entities to integrate with the Payment Redirect API, see Section 13.3, Payment Redirect Integration Requirements, of the EDE API Companion Guide, available at the following link: <https://zone.cms.gov/document/api-information>.

<sup>28</sup> EDE APIs technical documentation is available on CMS zONE at the following link: <https://zone.cms.gov/document/api-information>.

<sup>29</sup> The document Direct Enrollment API Specs is available on CMS zONE at the following link: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.



X. Miscellaneous.

- a. Notice. All notices to Parties specifically required under this Agreement shall be given in writing and shall be delivered as follows:

If to CMS:

By email:

[directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov)

By mail:

Centers for Medicare & Medicaid Services (CMS)

Center for Consumer Information and Insurance Oversight (CCIIO)

Attn: Office of the Director

Room 739H

200 Independence Avenue, SW

Washington, DC 20201

If to EDE Entity, to EDE Entity's primary contact's email address on record.

Notices sent by hand or overnight courier service, or mailed by certified or registered mail, shall be deemed to have been given when received; notices sent by email shall be deemed to have been given when the appropriate confirmation of receipt has been received; provided that notices not given on a business day (i.e., Monday-Friday excluding federal holidays) between 9:00 a.m. and 5:00 p.m. local time where the recipient is located shall be deemed to have been given at 9:00 a.m. on the next business day for the recipient. A Party to this Agreement may change its contact information for notices and other communications by providing written notice of such changes in accordance with this provision. Such notice should be provided thirty (30) Days in advance of such change, unless circumstances warrant a shorter timeframe.

- b. Assignment and Subcontracting. Except as otherwise provided in this Section, EDE Entity shall not assign this Agreement in whole or in part, whether by merger, acquisition, consolidated, reorganization, or otherwise any portion of the services to be provided by EDE Entity under this Agreement without the express, prior written consent of CMS, which consent may be withheld, conditioned, granted, or denied in CMS' sole discretion. EDE Entity must provide written notice at least thirty (30) Days prior to any such proposed assignment, including any change in ownership of EDE Entity or any change in management or ownership of the EDE Environment. Notwithstanding the foregoing, CMS does not require prior written consent for subcontracting arrangements that do not involve the operation, management, or control of the EDE Environment. EDE Entity must report all subcontracting arrangements on its annual Operational and Oversight Information form during the annual EDE Agreement Renewal process and submit revisions annually thereafter. EDE Entity shall assume ultimate responsibility for all services and functions described under this Agreement, including those that are subcontracted to other entities, and must ensure that subcontractors will perform all functions in accordance with all applicable requirements. EDE Entity shall further be subject to such oversight and enforcement actions for functions or activities performed by subcontractors as may otherwise be provided for under applicable law and program requirements,

including EDE Entity's respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement). Notwithstanding any subcontracting of any responsibility under this Agreement, EDE Entity shall not be released from any of its performance or compliance obligations hereunder, and shall remain fully bound to the terms and conditions of this Agreement as unaltered and unaffected by such subcontracting.

If EDE Entity attempts to make an assignment, subcontracting arrangement or otherwise delegate its obligations hereunder in violation of this provision, such assignment, subcontract, or delegation shall be deemed void *ab initio* and of no force or effect, and EDE Entity shall remain legally bound hereto and responsible for all obligations under this Agreement.

- c. Use of the FFE Web Services. EDE Entity will only use a CMS-approved EDE Environment when accessing the APIs and web services that facilitate EDE functionality to enroll Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix H.
- d. Incident Reporting Procedures: EDE Entity must implement Incident and Breach Handling procedures as required by the NEE SSP and that are consistent with CMS's Incident and Breach Notification Procedures. Such policies and procedures must identify EDE Entity's Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents or Breaches and provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes. EDE Entity agrees to report any Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at [cms\\_it\\_service\\_desk@cms.hhs.gov](mailto:cms_it_service_desk@cms.hhs.gov) within 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.
- e. Survival. EDE Entity's obligation under this Agreement to protect and maintain the privacy and security of PII and any other obligation of EDE Entity in this Agreement which, by its express terms or nature and context is intended to survive expiration or termination of this Agreement, shall survive the expiration or termination of this Agreement.
- f. Severability. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement. In the event that any provision of this Agreement is determined to be invalid, unenforceable or otherwise illegal, such provision shall be deemed restated, in accordance with applicable law, to reflect as nearly as possible the original intention of the Parties, and the remainder of the Agreement shall be in full force and effect.

- g. Disclaimer of Joint Venture. Neither this Agreement nor the activities of EDE Entity contemplated by and under this Agreement shall be deemed or construed to create in any way any partnership, joint venture, or agency relationship between CMS and EDE Entity. Neither Party is, nor shall either Party hold itself out to be, vested with any power or right to bind the other Party contractually or to act on behalf of the other Party, except to the extent expressly set forth in the ACA and the regulations codified thereunder, including as codified at 45 C.F.R. part 155.
- h. Remedies Cumulative. No remedy herein conferred upon or reserved to CMS under this Agreement is intended to be exclusive of any other remedy or remedies available to CMS under operative law and regulation, and each and every such remedy, to the extent permitted by law, shall be cumulative and in addition to any other remedy now or hereafter existing at law or in equity or otherwise.
- i. Records. EDE Entity shall maintain all records that it creates in the normal course of its business in connection with activity under this Agreement for the term of this Agreement in accordance with 45 C.F.R. §§ 155.220(c)(3)(i)(E) or 156.705(c), as applicable. Subject to applicable legal requirements and reasonable policies, such records shall be made available to CMS to ensure compliance with the terms and conditions of this Agreement. The records shall be made available during regular business hours at EDE Entity's offices, and CMS's review shall not interfere unreasonably with EDE Entity's business activities. This clause survives the expiration or termination of this Agreement.
- j. Compliance with Law. EDE Entity covenants and agrees to comply with any and all applicable laws, statutes, regulations, or ordinances of the United States of America and any Federal Government agency, board, or court that are applicable to the conduct of the activities that are the subject of this Agreement, including, but not necessarily limited to, any additional and applicable standards required by statute, and any regulations or policies implementing or interpreting such statutory provisions hereafter issued by CMS. In the event of a conflict between the terms of this Agreement and any statutory, regulatory, or sub-regulatory guidance released by CMS, the requirement that constitutes the stricter, higher, or more stringent level of compliance shall control.
- k. Governing Law and Consent to Jurisdiction. This Agreement will be governed by the laws and common law of the United States of America, including without limitation such regulations as may be promulgated by HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. EDE Entity further agrees and consents to the jurisdiction of the Federal Courts located within the District of Columbia and the courts of appeal therefrom, and waives any claim of lack of jurisdiction or *forum non conveniens*.
- l. Amendment. CMS may amend this Agreement for purposes of reflecting changes in applicable law or regulations, with such amendments taking effect upon thirty (30) Days' written notice to EDE Entity ("CMS notice period"), unless circumstances warrant an earlier effective date. Any amendments made under this provision will only have prospective effect and will not be applied retrospectively. EDE Entity may reject such amendment by providing to CMS, during the CMS notice period, written

notice of its intent to reject the amendment (“rejection notice period”). Any such rejection of an amendment made by CMS shall result in the termination of this Agreement upon expiration of the rejection notice period.

- m. Audit and Compliance Review. EDE Entity agrees that CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees may conduct compliance reviews or audits, which includes the right to interview employees, contractors, and business partners of EDE Entity and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of EDE Entity’s compliance with the requirements of this Agreement and applicable program requirements upon reasonable notice to EDE Entity, during EDE Entity’s regular business hours, and at EDE Entity’s regular business location. These audit and review rights include the right to audit EDE Entity’s compliance with and implementation of the privacy and security requirements under this Agreement, the ISA, EDE Entity’s respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement), and applicable program requirements. EDE Entity further agrees to allow reasonable access to the information and facilities, including, but not limited to, EDE Entity website testing environments, requested by CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees for the purpose of such a compliance review or audit. EDE Entity is also responsible for ensuring cooperation by its Downstream and Delegated Entities, including EDE Entity’s subcontractors and assignees, as well as the Auditor(s) and any of its subcontractors, with audits and reviews. CMS may suspend or terminate this Agreement if EDE Entity does not comply with such a compliance review request within seven (7) business days. If any of EDE Entity’s obligations under this Agreement are delegated to other parties, the EDE Entity’s agreement with any Downstream and Delegated Entities must incorporate this Agreement provision.

This clause survives the expiration or termination of this Agreement.

- n. Access to the FFEs and SBE-FPs. EDE Entity; its Downstream and Delegated Entities, including downstream Agents/Brokers; and its assignees or subcontractors—including, employees, developers, agents, representatives, or contractors—cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to EDE Entity’s systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through virtual private networks (VPNs).

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

This “Agreement between EDE Entity and the Centers for Medicare & Medicaid Services for the Individual Market Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform” has been signed and executed by:

**TO BE FILLED OUT BY EDE ENTITY**

The undersigned is an authorized official of EDE Entity who is authorized to represent and bind EDE Entity for purposes of this Agreement. The undersigned attests to the accuracy and completeness of all information provided in this Agreement.

*Manal Mehta*

10-19-2023

Signature of Authorized Official of EDE Entity

Date

Manal Mehta, CEO

Printed Name and Title of Authorized Official of EDE Entity

Benefitalign LLC

EDE Entity Name

04.BFT.MD\*.450.850

EDE Entity Partner IDs

*T White*

Signature of Privacy Officer

Tamara White

Printed Name and Title of Privacy Officer

2400 Louisiana Blvd NE,

Building 3, Albuquerque,

NM 87110

EDE Entity Address

**REDACTED**

EDE Entity Contact Number

Centers for Medicare & Medicaid Services

---

**FOR CMS**

The undersigned are officials of CMS who are authorized to represent and bind CMS for purposes of this Agreement.

**Jeffrey Grant -S** Digitally signed by Jeffrey Grant -S  
Date: 2023.10.19 15:50:03 -04'00'

---

**Jeffrey D. Grant**

**Date**

Deputy Director for Operations

Center for Consumer Information and Insurance Oversight

Centers for Medicare & Medicaid Services

**George C. Hoffmann -S** Digitally signed by George C. Hoffmann -S  
Date: 2023.10.30 07:12:02 -04'00'

---

**George C. Hoffmann**

**Date**

CMS Deputy CIO

Deputy Director, Office of Information Technology (OIT)

Centers for Medicare & Medicaid Services (CMS)

## **APPENDIX A: PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS FOR NON-EXCHANGE ENTITIES**

---

Federally-facilitated Exchanges (“FFE”) will enter into contractual agreements with all Non-Exchange Entities, including EDE Entities, that gain access to Personally Identifiable Information (“PII”) exchanged with the FFEs (including FF-SHOPs) and State-based Exchanges on the Federal Platform (“SBE-FPs”) (including SBE-FP-SHOPs), or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals’ legal representatives or Authorized Representatives. This Agreement and its appendices govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by EDE Entities in the context of the FFEs and SBE-FPs. In signing this contractual Agreement, in which this Appendix A has been incorporated, EDE Entities agree to comply with the security and privacy standards and implementation specifications outlined in the Non-Exchange Entity System Security and Privacy Plan (“NEE SSP”)<sup>30</sup> and Section A<sup>31</sup> below while performing the Authorized Functions outlined in their respective Agreement(s) with CMS.

The standards documented in the NEE SSP and Section A below are established in accordance with Section 1411(g) of the Affordable Care Act (“ACA”) (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 (“FISMA”) (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the principles in 45 C.F.R. §§ 155.260(a)(1) through (a)(6). All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

### **A. NON-EXCHANGE ENTITY PRIVACY AND SECURITY IMPLEMENTATION SPECIFICATIONS**

Non-Exchange Entities must meet privacy and security implementation specifications that are consistent with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 P.L. 104-191 and the Privacy Act of 1974, 5 U.S.C. § 552a, including:

- (1) Openness and Transparency. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, and Enrollees and their PII.
  - a. Standard: Privacy Notice Statement. Prior to collecting PII, the Non-Exchange Entity must provide a notice that is prominently and conspicuously displayed on a public-facing website, if applicable, or on the electronic and/or paper form the

---

<sup>30</sup> The NEE SSP template is located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

<sup>31</sup> Section A contains excerpts from the NEE SSP of two requirements for ease of reference. This does not alter the need to comply with other applicable EDE Entity requirements, including those outlined within 45 C.F.R. § 155.260(a)(1) through (a)(6) or the NEE SSP.



Non-Exchange Entity will use to gather and/or request PII. The EDE Entity must comply with any additional standards and implementation specifications described in NEE SSP TR-1: Privacy Notice.

i. Implementation Specifications.

1. The statement must be written in plain language and provided in a manner that is timely and accessible to people living with disabilities and with limited English proficiency.
2. The statement must contain at a minimum the following information:
  - a. Legal authority to collect PII;
  - b. Purpose of the information collection;
  - c. To whom PII might be disclosed, and for what purposes;
  - d. Authorized uses and disclosures of any collected information;
  - e. Whether the request to collect PII is voluntary or mandatory under the applicable law; and
  - f. Effects of non-disclosure if an individual chooses not to provide the requested information.
3. The Non-Exchange Entity shall maintain its Privacy Notice Statement content by reviewing and revising as necessary on an annual basis, at a minimum, and before or as soon as possible after any change to its privacy policies and procedures.
4. If the Non-Exchange Entity operates a website, it shall ensure that descriptions of its privacy and security practices, and information on how to file complaints with CMS and the Non-Exchange Entity, are publicly available through its website.<sup>32</sup>

(2) Individual Choice. In keeping with the standards and implementation specifications used by the FFEs, the Non-Exchange Entity should ensure that Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—are provided a reasonable opportunity and capability to make informed decisions about the creation, collection, disclosure, access, maintenance, storage, and use of their PII.

- a. Standard: Informed Consent. The Non-Exchange Entity may create, collect, disclose, access, maintain, store, and use PII from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—only for the functions and purposes listed in the

---

<sup>32</sup> CMS recommends that EDE Entities direct consumers, who are seeking to file a complaint, to the Secretary of the U.S. Department of Health and Human Services, 200 Independence Ave, S.W., Washington, D.C. 20201. Call (202) 619-0257 (or toll free (877) 696-6775) or go to the website of the Office for Civil Rights, [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa).



Privacy Notice Statement and any relevant agreements in effect as of the time the information is collected, unless the FFE, SBE-FP, or Non-Exchange Entity obtains informed consent from such individuals. The EDE Entity must comply with any additional standards and implementation specifications described in NEE SSP IP-1: Consent.

i. Implementation Specifications.

1. The Non-Exchange Entity must obtain informed consent from individuals for any use or disclosure of information that is not permissible within the scope of the Privacy Notice Statement and any relevant agreements that were in effect as of the time the PII was collected. Such consent must be subject to a right of revocation.
2. Any such consent that serves as the basis of a use or disclosure must:
  - a. Be provided in specific terms and in plain language,
  - b. Identify the entity collecting or using the PII, and/or making the disclosure,
  - c. Identify the specific collections, use(s), and disclosure(s) of specified PII with respect to a specific recipient(s), and
  - d. Provide notice of an individual's ability to revoke the consent at any time.
3. Consent documents must be appropriately secured and retained for ten (10) Years.

## APPENDIX B: DEFINITIONS

---

This Appendix defines terms that are used in the Agreement and other Appendices. Any capitalized term used in the Agreement that is not defined therein or in this Appendix has the meaning provided in 45 C.F.R. § 155.20.

- (1) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 C.F.R. § 155.20.
- (2) **Affordable Care Act (ACA)** means the Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), which are referred to collectively as the Affordable Care Act or ACA.
- (3) **Agent** or **Broker** has the meaning set forth in 45 C.F.R. § 155.20.
- (4) **Agent or Broker Direct Enrollment (DE) Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.
- (5) **Applicant** has the meaning set forth in 45 C.F.R. § 155.20.
- (6) **Auditor** means a person or organization that meets the requirements set forth in this Agreement and contracts with a Direct Enrollment (DE) Entity for the purposes of conducting an Operational Readiness Review (ORR) in accordance with 45 C.F.R. §§ 155.221(b)(4) and (f), this Agreement and CMS-issued guidance.
- (7) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in the Agreement that incorporates this Appendix B.
- (8) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 C.F.R. § 155.227.
- (9) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information for anything other than an authorized purpose.
- (10) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (CMS).
- (11) **Classic Direct Enrollment (Classic DE)** means, for purposes of this Agreement, the original version of Direct Enrollment, which utilizes a double redirect from a Direct Enrollment (DE) Entity's website to HealthCare.gov where the eligibility application is submitted and an eligibility determination is received, and back to the DE Entity's

website for QHP shopping and plan selection consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(i), 155.221, 156.265 and/or 156.1230(b).

- (12) **Classic Direct Enrollment Pathway (Classic DE Pathway)** means, for the purposes of this Agreement, the application and enrollment process used by Direct Enrollment (DE) Entities for Classic DE.
- (13) **CMS** means the Centers for Medicare & Medicaid Services.
- (14) **CMS Companion Guides** means a CMS-authored guide, available on the CMS website, which is meant to be used in conjunction with and supplement relevant implementation guides published by the Accredited Standards Committee.
- (15) **CMS Data Services Hub (Hub)** is the CMS Federally-managed service to interface data among connecting entities, including HHS, certain other Federal agencies, and State Medicaid agencies.
- (16) **CMS Data Services Hub Web Services (Hub Web Services)** means business and technical services made available by CMS to enable the determination of certain eligibility and enrollment or federal financial payment data through the Federally-facilitated Exchange (FFE) website, including the collection of personal and financial information necessary for Consumer, Applicant, Qualified Individual, or Enrollee account creations; Qualified Health Plan (QHP) application submissions; and Insurance Affordability Program eligibility determinations.
- (17) **Common Control** means a security or privacy control whose implementation results in a security or privacy capability that is inheritable by multiple information systems being served by the Primary EDE Entity.
- (18) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (QHP) offered through an Exchange or Insurance Affordability Program, or whom an Agent or Broker (including Web-brokers) registered with the FFE, Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a QHP, applying for APTC and CSRs, and/or completing enrollment in a QHP through the FFEs or State-based Exchanges on the Federal Platform (SBE-FPs) for individual market coverage.
- (19) **Cost-sharing Reductions (CSRs)** has the meaning set forth in 45 C.F.R. § 155.20.
- (20) **Customer Service** means assistance regarding eligibility and Health Insurance Coverage provided to a Consumer, Applicant, Qualified Individual, and Enrollee, including, but not limited to, responding to questions and complaints; providing information about eligibility; applying for APTC and/or CSRs, and Health Insurance Coverage; and explaining enrollment processes in connection with the FFEs or SBE-FPs.
- (21) **Day or Days** means calendar days, unless otherwise expressly indicated in the relevant provision of the Agreement that incorporates this Appendix B.

- (22) **Delegated Entity** means, for purposes of this Agreement, any party, including an Agent or Broker, that enters into an agreement with an Enhanced Direct Enrollment (EDE Entity) to provide administrative or other services to or on behalf of the EDE Entity or to provide administrative or other services to Consumers and their dependents.
- (23) **Designated Privacy Official** means a contact person or office responsible for receiving complaints related to Breaches or Incidents, able to provide further information about matters covered by the Privacy Notice statement, responsible for the development and implementation of the privacy policies and procedures of the Non-Exchange Entity, and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy of Personally Identifiable Information (PII).
- (24) **Designated Representative** means an Agent or Broker that has the legal authority to act on behalf of the Web-broker.
- (25) **Designated Security Official** means a contact person or office responsible for the development and implementation of the security policies and procedures of the Non-Exchange Entity and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the security of Personally Identifiable Information (PII).
- (26) **Direct Enrollment (DE)** means, for the purposes of this Agreement, the process by which a Direct Enrollment (DE) Entity may assist an Applicant or Enrollee with enrolling in a QHP in a manner that is considered through the Exchange consistent with applicable requirements in 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or 156.1230. Direct Enrollment is the collective term used when referring to both Classic Direct Enrollment and Enhanced Direct Enrollment.
- (27) **Direct Enrollment (DE) Entity** has the meaning set forth in 45 C.F.R. § 155.20.
- (28) **Direct Enrollment Entity Application Assister** has the meaning set forth in 45 C.F.R. § 155.20.
- (29) **Direct Enrollment (DE) Environment** means an information technology application or platform provided, owned, and maintained by a DE Entity through which a DE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.
- (30) **Downstream Entity** means, for purposes of this Agreement, any party, including an Agent or Broker, that enters into an agreement with a Delegated Entity or with another Downstream Entity for purposes of providing administrative or other services related to the agreement between the Delegated Entity and the Enhanced Direct Enrollment (EDE) Entity. The term “Downstream Entity” is intended to refer to the

entity that directly provides administrative services or other services to or on behalf of the EDE Entity or that provides administrative or other services to Consumers and their dependents.

- (31) **Downstream White-Label Third-Party User Arrangements** means an arrangement between an Agent or Broker and a Primary EDE Entity to use the Primary EDE Entity's EDE Environment. In this arrangement, a Primary EDE Entity enables the Downstream White-Label Agent or Broker to only make minor branding changes to the Primary EDE Entity's EDE Environment.
- (32) **Enhanced Direct Enrollment (EDE)** means, for purposes of this Agreement, the version of Direct Enrollment which allows Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—to complete all steps in the application, eligibility and enrollment processes on an EDE Entity's website consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(ii), 155.221, 156.265 and/or 156.1230(b) using application programming interfaces (APIs) as provided, owned, and maintained by CMS to transfer data between the Exchange and the EDE Entity's website.
- (33) **Enhanced Direct Enrollment (EDE) End-User Experience** means all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions under this Agreement.
- (34) **Enhanced Direct Enrollment (EDE) Entity** means a DE Entity that has been approved by CMS to use the EDE Pathway. This term includes both Primary EDE Entities and Upstream EDE Entities.
- (35) **Enhanced Direct Enrollment (EDE) Environment** means an information technology application or platform provided, owned, and maintained by an EDE Entity through which an EDE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.
- (36) **Enhanced Direct Enrollment (EDE) Pathway** means the APIs and functionality comprising the systems that enable EDE as provided, owned, and maintained by CMS.
- (37) **Enrollee** has the meaning set forth in 45 C.F.R. § 155.20.
- (38) **Exchange** has the meaning set forth in 45 C.F.R. § 155.20.
- (39) **Federally-facilitated Exchange (FFE)** means an **Exchange (or Marketplace)** established by the Department of Health and Human Services (HHS) and operated by

CMS under Section 1321(c)(1) of the ACA for individual market coverage.  
**Federally-facilitated Marketplaces (FFMs)** has the same meaning as FFEs.

- (40) **Health Insurance Coverage** has the meaning set forth in 45 C.F.R. § 155.20.
- (41) **Health Insurance Portability and Accountability Act (HIPAA)** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and its implementing regulations.
- (42) **Health Reimbursement Arrangement (HRA)** has the meaning set forth in 45 C.F.R. § 146.123(c).
- (43) **HHS** means the United States Department of Health & Human Services.
- (44) **Hybrid Control** means those controls for which both a Primary EDE Entity and its Upstream EDE Entity share the responsibility of implementing the full control objectives and implementation standards. Hybrid Controls refer to arrangements in which an Upstream EDE Entity information system inherits part of a control from a Primary EDE Entity, with the remainder of the control provided by the Upstream EDE Entity leveraging the Primary EDE Entity's EDE Environment.
- (45) **Hybrid Issuer Upstream EDE Entity** means a QHP Issuer EDE Entity that uses the EDE Environment of a Primary EDE Entity and adds functionality or systems to the Primary EDE Entity's EDE Environment such that the Primary EDE Entity's EDE Environment or overall EDE End-User Experience is modified beyond minor deviations for branding or QHP display changes relevant to the Issuer's QHPs.
- (46) **Hybrid Non-Issuer Upstream EDE Entity** means an Agent, Broker, or Web-broker under 45 C.F.R. §§ 155.220(c)(3) and 155.221 that uses the EDE Environment of a Primary EDE Entity and adds functionality or systems to the Primary EDE Entity's EDE Environment such that the Primary EDE Entity's EDE Environment or overall EDE End-User Experience is modified beyond minor branding changes.
- (47) **Incident, or Security Incident**, has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and means an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- (48) **Insurance Affordability Program** means a program that is one of the following:
  - (1) A State Medicaid program under title XIX of the Social Security Act.
  - (2) A State Children's Health Insurance Program (CHIP) under title XXI of the Social Security Act.
  - (3) A State basic health program established under section 1331 of the Care Act.

- (4) A program that makes coverage in a Qualified Health Plan (QHP) through the Exchange with APTC established under section 36B of the Internal Revenue Code available to Qualified Individuals.
- (5) A program that makes available coverage in a QHP through the Exchange with CSRs established under section 1402 of the ACA.
- (49) **Interconnection Security Agreement** means a distinct agreement that outlines the technical solution and security requirements for an interconnection between CMS and EDE Entity.
- (50) **Issuer** has the meaning set forth in 45 C.F.R. § 144.103.
- (51) **Non-Exchange Entity** has the meaning at 45 C.F.R. § 155.260(b)(1), including, but not limited to, Qualified Health Plan (QHP) Issuers, Navigators, Agents, Brokers, and Web-brokers.
- (52) **OMB** means the Office of Management and Budget.
- (53) **Operational Readiness Review (ORR)** means an audit conducted under 45 C.F.R. §§ 155.221(b)(4) and (f) and includes the reports submitted by an EDE Entity detailing its compliance with CMS requirements and readiness to implement and use the EDE Environment.
- (54) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- (55) **Primary EDE Entity** means an entity that has developed and maintains an EDE Environment. A Primary EDE Entity may provide its EDE Environment to an Upstream EDE Entity and the Primary EDE Entity may provide an EDE Environment for use by Consumers, Applicants, Qualified Individuals, Enrollees—or these individuals' legal representatives or Authorized Representatives—, Agents, Brokers, or DE Entity Application Assisters.
- (56) **Prospective EDE Entity** means an entity that has not yet been approved by CMS to use the EDE Pathway.
- (57) **Prospective Phase Change EDE Entity** means a Primary EDE Entity already approved to use the EDE Pathway that is seeking to implement a new eligibility application phase using the EDE Entity-initiated Change Request process.
- (58) **Qualified Health Plan (QHP)** has the meaning set forth in 45 C.F.R. § 155.20.
- (59) **Qualified Health Plan (QHP) Issuer** has the meaning set forth in 45 C.F.R. § 155.20.
- (60) **Qualified Health Plan (QHP) Issuer Agreement** means the QHP Certification Agreement and Privacy and Security Agreement Between QHP Issuer and CMS.



- (61) **Qualified Health Plan (QHP) Direct Enrollment (DE) Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.
- (62) **Qualified Individual** has the meaning set forth in 45 C.F.R. § 155.20.
- (63) **Rules of Engagement (ROE)** means the detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test and gives the test team authority to conduct defined activities without the need for additional permissions.
- (64) **Special Enrollment Period (SEP)** has the meaning set forth in 45 C.F.R. § 155.20.
- (65) **Standalone Eligibility Service (SES)** means a suite of application program interfaces (APIs) that will allow an EDE Entity to create, update, submit, and ultimately retrieve eligibility results for an application.
- (66) **State** means the State that has licensed the Agent, Broker, Web-broker, or Issuer that is a party to this Agreement and in which the Agent, Broker, Web-broker, or Issuer is operating.
- (67) **State-based Exchange (SBE)** means an Exchange established by a State that receives approval to operate under 45 C.F.R. § 155.105. **State-based Marketplace (“SBM”)** has the same meaning as SBE.
- (68) **State-based Exchange on the Federal Platform (SBE-FP)** means an Exchange established by a State that receives approval under 45 C.F.R. § 155.106(c) to utilize the Federal platform to support select eligibility and enrollment functions. **State-based Marketplace on the Federal Platform (“SBM-FP”)** has the same meaning as SBE-FP.
- (69) **Streamlined Eligibility Application User Interface (UI)** means the application UI on HealthCare.gov available for Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—with non-complex eligibility application responses determined by an initial set of eligibility questions for determining the complexity of an Applicant’s eligibility profile.
- (70) **Upstream EDE Entity** means an EDE Entity that uses the EDE Environment of a Primary EDE Entity and meets the definition of a Hybrid Issuer Upstream EDE Entity; a Hybrid Non-Issuer Upstream EDE Entity; or a White-Label Issuer Upstream EDE Entity.
- (71) **Web-broker** has the meaning set forth in 45 C.F.R. § 155.20.
- (72) **Web-broker Agreement** means the Agreement between a Web-broker and CMS for the FFEs and SBE-FPs.
- (73) **White-Label Issuer Upstream EDE Entity** means a QHP Issuer that uses the EDE Environment of a Primary EDE Entity without modifications beyond minor branding changes or QHP display changes.



- (74) **Workforce** means a Non-Exchange Entity's employees, contractors, subcontractors, officers, directors, agents, representatives, and any other individual who may create, collect, disclose, access, maintain, store, or use PII in the performance of his or her duties.



## APPENDIX C: EDE BUSINESS REQUIREMENTS<sup>33</sup>

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

Review Category	Requirement and Audit Standard
<b>Consumer Identity Proofing Implementation</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> The EDE Entity must conduct identity proofing (ID proofing) for Consumers entering the EDE pathway for enrollments through both Consumer and in-person Agent and Broker pathways.<sup>34</sup> The EDE Entity must conduct ID proofing prior to submitting a Consumer's application to the Exchange. If an EDE Entity is unable to complete ID proofing of the Consumer, the EDE Entity may either direct the Consumer to the classic DE (i.e., double-redirect) pathway or direct the Consumer to the Exchange (HealthCare.gov or the Exchange Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]).               <ul style="list-style-type: none"> <li>– <u>Remote ID Proofing/Fraud Solutions Archive Reporting Services (RIDP/FARS) or Third-Party ID Proofing Service:</u> CMS will make the Exchange RIDP and FARS services available for the EDE Entity to use when remote ID proofing Consumers for the Consumer pathway (i.e., when a Consumer is interacting directly with the EDE environment without the assistance of an individual Agent or Broker). If an EDE Entity uses the Exchange RIDP service, it must use the RIDP service only after confirming the Consumer is seeking coverage in a State supported by the Exchange/Federal Platform, and only after confirming the Consumer is eligible for the EDE Entity's chosen phase. However, CMS does not require that EDE Entities use the Exchange RIDP and FARS services, specifically, to complete ID proofing. An EDE Entity may instead opt to use a third-party ID proofing service for ID proofing in the Consumer pathway. If an EDE Entity uses a third-party identity proofing service, the service must be Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS)-approved, and the EDE Entity must be able to produce documentary evidence that each Applicant has been successfully ID proofed. Documentation related to a third-party service could be requested in an audit or investigation by CMS (or its designee), pursuant to the EDE Business Agreement. Applicants do not need to be ID proofed on subsequent interactions with the EDE Entity if the Applicant creates an account (i.e., username and password) on the EDE Entity's website, and the EDE Entity tracks that ID proofing has occurred when the Applicant's account was created.</li> <li>– <u>Manual ID Proofing in the In-Person Agent and Broker Pathway:</u> EDE Entities may also offer a manual ID proofing process. Consumers being ID proofed in the in-person Agent and Broker pathway (i.e., when an Agent or Broker is working with a Consumer and conducting ID proofing in-person, rather than remotely) must be ID proofed following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE (<a href="https://zone.cms.gov/document/api-information">https://zone.cms.gov/document/api-information</a>).</li> </ul> </li> </ul>

<sup>33</sup> The table in Appendix C is an updated version of Exhibit 2 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

<sup>34</sup> Consumer pathway means the workflow, UI, and accompanying APIs for an EDE environment that is intended for use by a Consumer to complete an eligibility application and enrollment. Agent and Broker pathway means the workflow, UI, and accompanying APIs for an EDE environment that is intended for use by an Agent or Broker to assist a Consumer with completing an eligibility application and enrollment.

Review Category	Requirement and Audit Standard
<b>Consumer Identity Proofing Implementation (continued)</b>	<ul style="list-style-type: none"> <li>– For the Consumer pathway, the EDE Entity must provide the User ID of the requester in the header for each EDE API call. For the Consumer pathway, the User ID should be the User ID for the Consumer’s account on the EDE Entity’s site, or some other distinct identifier the EDE Entity assigns to the Consumer.</li> <li>– Additionally, if an EDE Entity is using the Fetch Eligibility API, the same User ID requirements apply. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID.</li> <li>▪ Review Standard: <ul style="list-style-type: none"> <li>– If an EDE Entity uses the Exchange RIDP service, the Auditor must verify that the EDE Entity has successfully passed testing with the Hub.<sup>35</sup></li> <li>– If an EDE Entity uses a third-party ID proofing service, the Auditor must evaluate and certify the following: <ul style="list-style-type: none"> <li>The ID proofing service is FICAM TFS-approved, and</li> <li>The EDE Entity has implemented the service correctly.</li> </ul> </li> <li>– If an EDE Entity offers a Manual ID proofing option for an in-person Agent and Broker pathway, the Auditor must verify that the EDE Entity requires Agents and Brokers to ID proof Consumers as described in the “Acceptable Documentation for Identity Proofing” document.</li> <li>– EDE Entity’s inclusion of the appropriate Consumer User ID fields in the EDE and Fetch Eligibility API calls.</li> </ul> </li> </ul>

<sup>35</sup> RIDP/FARS testing requirements for the Hub can be found at the following link on CMS zONE:  
<https://zone.cms.gov/document/api-information>.

Review Category	Requirement and Audit Standard
<b>Agent and Broker Identity Proofing Verification</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> If an EDE Entity is implementing an Agent and Broker pathway for its EDE environment, the EDE Entity must implement Agent and Broker ID proofing verification procedures that consist of the following requirements: <ul style="list-style-type: none"> <li>– EDE Entity must integrate with IDM-Okta<sup>36</sup> and provide the User ID of the requester and IDM-Okta token in the header for each EDE API call. For Agents and Brokers, the User ID must exactly match the Exchange User ID (i.e. the Agent’s or Broker’s portal.cms.gov User ID) for the Agent or Broker, or the request will fail Exchange User ID validation. The same User ID requirements apply to the Fetch Eligibility and Submit Enrollment APIs. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID.</li> <li>– EDE Entity must ID proof all Agents and Brokers prior to allowing the Agents and Brokers to use its EDE environment. EDE Entity may conduct ID proofing in one of the following ways: <ul style="list-style-type: none"> <li>Use the Exchange-provided RIDP/FARS APIs to remotely ID proof Agents and Brokers; OR</li> <li>Manually ID proof Agents and Brokers following the guidelines outlined in the document “Acceptable Documentation for Identity Proofing” available on CMS zONE EDE webpage (<a href="https://zone.cms.gov/document/api-information">https://zone.cms.gov/document/api-information</a>). EDE Entities are permitted to use manual ID proofing as an alternative for Agents and Brokers that cannot be ID proofed via the RIDP/FARS services.</li> </ul> </li> <li>– EDE Entity must validate an Agent’s or Broker’s National Producer Number (NPN) using the National Insurance Producer Registry (<a href="https://www.nipr.com">https://www.nipr.com</a>) prior to allowing the Agent or Broker to use its EDE environment.</li> <li>– EDE Entity must systematically provide an Agent and Broker ID proofing process—that meets all of the requirements defined here—that applies to all downstream Agents and Brokers of the Primary EDE Entity.</li> <li>– Additionally, all Agent and Broker users of an Upstream EDE Entity’s EDE website (hosted by a Primary EDE Entity) must be ID proofed consistent with these requirements. The Primary EDE Entity may provide one centralized ID proofing approach for any Agents and Brokers that will use the Primary EDE Entity’s EDE environment (including when utilized by Upstream EDE Entities and their downstream Agents and Brokers).</li> </ul> </li> </ul>

<sup>36</sup> For instructions on how to integrate with IDM-Okta, see the Change Request #55 Integration Manual (IDM Integration), available at: <https://zone.cms.gov/document/business-audit> and *Hub Onboarding Form*, available at: <https://zone.cms.gov/document/hub-onboarding-form>.

Review Category	Requirement and Audit Standard
<b>Agent and Broker Identity Proofing Verification (continued)</b>	<p>Alternatively, the Upstream EDE Entity may conduct its own ID proofing process of its downstream Agents and Brokers consistent with these requirements. The Upstream EDE Entity must provide the information for Agents and Brokers that have passed and failed ID proofing to the Primary EDE Entity using a secure data transfer. If an Upstream EDE Entity wants to pursue this flexibility, its ID proofing process must be audited by an Auditor consistent with these standards and the arrangement will be considered a hybrid arrangement.</p> <ul style="list-style-type: none"> <li>– Note: If a Primary EDE Entity does not provide a centralized process for ID proofing an Upstream EDE Entity’s downstream Agent and Broker and if the Primary EDE Entity intends to provide the EDE environment to Upstream EDE Entities, the Upstream EDE Entities will be required to provide documentation of an Auditor’s evaluation of its ID proofing approach consistent with these standards. This process must be categorized as an EDE Entity-initiated Change Request (Section XI.A, EDE Entity-initiated Change Requests) if it occurs after the Primary EDE Entity’s initial audit submission and the arrangement with the Upstream EDE Entity will be considered a hybrid arrangement.</li> <li>– All Agents and Brokers that will use EDE must be ID proofed consistent with these standards. This includes downstream Agents and Brokers of Primary EDE Entities and Upstream EDE Entities. If applicable, the Auditor must evaluate the Primary EDE Entity’s centralized implementation for ID proofing or the Upstream EDE Entity’s implementation for ID proofing.</li> <li>– EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3.</li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– EDE Entity’s inclusion of the appropriate Agent and Broker User ID and IDM-Okta token fields in the EDE and Fetch Eligibility and Submit Enrollment API calls.</li> <li>– EDE Entity’s process for ID proofing an Agent or Broker prior to allowing an Agent or Broker to use its EDE environment.</li> <li>– EDE Entity’s process for validating an Agent’s or Broker’s NPN using the National Insurance Producer Registry prior to allowing an Agent or Broker to use its EDE environment.</li> <li>– EDE Entity’s process for systematically providing an Agent and Broker ID proofing approach for all downstream Agents and Brokers of the EDE Entity and, if applicable, any Upstream EDE Entities.</li> <li>– If the Primary EDE Entity has not provided a centralized ID proofing approach to an Upstream EDE Entity, Primary EDE Entity’s process for verifying that an Upstream EDE Entity has conducted appropriate ID proofing, consistent with this requirement, for all of the Upstream EDE Entity’s downstream Agents and Brokers prior to those Agents and Brokers being able to use the Primary EDE Entity’s EDE environment.</li> </ul> </li> </ul>
<b>Phase-dependent Screener Questions (EDE Phase 1 and 2 EDE Entities Only)</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> An EDE Entity that implements either EDE Phase 1 or Phase 2 must implement screening questions to identify Consumers whose eligibility circumstances the EDE Entity is unable to support consistent with the eligibility scenarios supported by the EDE Entity’s selected EDE phase. These phase-dependent screener questions must be located at the beginning of the EDE application, but may follow the QHP plan compare experience. For those Consumers who won’t be able to apply through scenarios covered by the EDE phase that the EDE Entity implements, the EDE Entity must either route the Consumer to the classic DE double-redirect pathway or direct the Consumer to the Exchange by providing the following options: HealthCare.gov or the Exchange Call Center at 1-800-318-2596 [TTY: 1-855-889-4325].</li> <li>▪ <i>Review Standard:</i> The Auditor must verify the following: <ul style="list-style-type: none"> <li>– The EDE Entity has implemented screening questions—consistent with the requirements in the Exchange Application UI Principles document and Application UI Toolkit—to identify Consumers with eligibility scenarios not supported by the EDE Entity’s EDE environment and selected EDE phase.</li> <li>– The EDE Entity’s EDE environment facilitates moving Consumers to one of the alternative enrollment pathways described immediately above.</li> </ul> </li> </ul>

Review Category	Requirement and Audit Standard
<b>Accurate and Streamlined Eligibility Application User Interface (UI)</b>	<p><i>Requirement:</i> EDE Entities using the EDE pathway must support all application scenarios outlined in EDE Entity's selected EDE phase. The EDE Entity must adhere to the guidelines set forth in the FFE Application UI Principles document when implementing the application. EDE Entities can access the FFE Application UI Principles document on CMS zONE (<a href="https://zone.cms.gov/document/eligibility-information">https://zone.cms.gov/document/eligibility-information</a>). Auditors will need to access the FFE Application UI Principles document to conduct the audit.</p> <ul style="list-style-type: none"> <li>– As explained in the FFE Application UI Principles document, the EDE Entity must implement the application in accordance with the Exchange requirements. For each supported eligibility scenario, the EDE Entity must display all appropriate eligibility questions and answers, including all questions designated as optional. (Note: These questions are optional for the Consumer to answer, but are not optional for EDE Entities to implement.) The FFE Application UI Principles document and Application UI Toolkit define appropriate flexibility EDE Entities may implement with respect to question wording, question order or structure, format of answer choices (e.g., drop-down lists, radio buttons), and integrated help information (e.g., tool tips, URLs, help boxes). In most cases, answer choices, question logic (e.g., connections between related questions), and disclaimers (e.g., APTC attestation) must be identical to those of the Exchange. <ul style="list-style-type: none"> <li>Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this exceeds the scope of the test cases in the Eligibility Results Toolkits.</li> </ul> </li> <li>– EDE Entities will also need to plan their application's back-end data structure to ensure that attestations can be successfully submitted to Standalone Eligibility Service (SES) APIs at appropriate intervals within the application process and that the EDE Entity can process responses from SES and integrate them into the UI question flow logic, which is dynamic for an individual Consumer based on his or her responses. The EDE Entity will need to ensure that sufficient, non-contradictory information is collected and stored such that accurate eligibility results will be reached without any validation errors.</li> </ul> <ul style="list-style-type: none"> <li>▪ <i>Review Standard:</i> The Auditor must review and certify the following: <ul style="list-style-type: none"> <li>– The FFE Application UI has been implemented in EDE Entity's environment in accordance with the Exchange Application UI Principles document.</li> <li>– The FFE Application UI displays all appropriate eligibility questions and answers from the Application UI Toolkit, including any questions designated as optional.</li> <li>– The Auditor will review the application for each supported eligibility scenario under the phase the EDE Entity has implemented to confirm that the application has been implemented in accordance with the FFE Application UI Principles document and Application UI Toolkit. The Auditor will document this compliance in the Application UI Toolkit. <ul style="list-style-type: none"> <li>Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this exceeds the scope of the test cases in the Eligibility Results Toolkits.</li> </ul> </li> <li>– If EDE Entity has implemented Phase 1 or Phase 2, the Auditor will confirm that the UI includes a disclaimer stating that the environment does not support all application scenarios, and identifying which scenarios are and are not supported. The disclaimer should direct the Consumer to alternative pathways, such as the classic DE double-redirect pathway or direct the Consumer to the Exchange (HealthCare.gov or the Exchange Call Center at 1-800-318-2596 (TTY: 1-855-889-4325)). This requirement is included in the Communications Toolkit.</li> </ul> </li> </ul>

Review Category	Requirement and Audit Standard
<b>Post-eligibility Application Communications</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> The EDE environment must display high-level eligibility results, next steps for enrollment, and information about each Applicant’s insurance affordability program eligibility (e.g., APTC, CSR, Medicaid, and/or CHIP eligibility), Data Matching Issues (DMIs), special enrollment periods (SEPs), SEP Verification Issues (SVIs), and enrollment steps in a clear, comprehensive and Consumer-friendly way. Generally, CMS’s Communications Toolkit constitutes the minimum post-eligibility application communications requirements that an EDE Entity must provide to users of the EDE environment; CMS does not intend for the Communications Toolkit requirements to imply that EDE Entities are prohibited from providing additional communications or functionality, consistent with applicable requirements. <ul style="list-style-type: none"> <li>– EDE Entity must provide Consumers with required UI messaging tied to API functionality and responses as provided in the EDE API Companion Guide<sup>37</sup>.</li> <li>– EDE Entity must provide Consumers with the CMS-provided Eligibility Determination Notices (EDNs) generated by the Exchange any time it submits or updates an application pursuant to requirements provided by CMS in the Communications Toolkit.</li> </ul> </li> </ul>

<sup>37</sup> The API Companion Guide is available on CMS zONE at the following link: <https://zone.cms.gov/document/api-information>.



Review Category	Requirement and Audit Standard
<b>Post-eligibility Application Communications (continued)</b>	<ul style="list-style-type: none"> <li>– EDE Entity must provide the EDN in a downloadable format at the time the Consumer’s application is submitted or updated and must have a process for providing access to the Consumer’s most recent EDN via the API as well as providing access to the Consumer’s historical notices—accessed via the Notice Retrieval API by the EDE Entity’s EDE environment—within the UI. The UI requirements related to accessibility of a Consumer’s EDN are set forth in the Communications Toolkit.</li> <li>– EDE Entities are not required to store notices downloaded from the Exchange. EDE Entities must use the Metadata Search API and the Notice Retrieval API to generate the most recent Exchange notices when Consumers act to view/download notices consistent with the Communications Toolkit. EDE Entities must also provide access to view/download historical notices in their UIs.</li> <li>– EDE Entity must provide and communicate status updates and access to information for Consumers to manage their applications and coverage. These communications include, but are not limited to, status of DMLs and SVIs, enrollment periods (e.g., SEP eligibility and the OEP), providing and communicating about new notices generated by the Exchange, application and enrollment status, and supporting document upload for DMLs and SVIs. This requirement is detailed in the Communications Toolkit.</li> <li>– EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI (e.g., an account management hub for managing all application- and enrollment-related actions).</li> <li>– For any Consumers enrolled, including via the Agent and Broker pathway, the EDE Entity must provide critical communications to Consumers notifying them of the availability of Exchange-generated EDNs, critical communications that the Consumer will no longer receive from the Exchange (i.e., if the EDE Entity has implemented and been approved by CMS to assume responsibility for those communications), and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer’s application or enrollment status.</li> <li>– All EDE Entities, regardless of phase, must provide Consumers with status updates and document upload capabilities for all DMLs and SVIs. Even if an EDE Entity’s chosen eligibility application phase does not support the questions necessary to reach a certain DMI or SVI, the post-application and post-enrollment functionality must support any Consumer with any DMI or SVI; post-application and post-enrollment DMI and SVI management is not dependent on the EDE Entity’s chosen eligibility application phase.</li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– The EDE Entity’s EDE environment is compliant with the requirements contained in the Communications Toolkit and API Companion Guide.</li> <li>– The EDE Entity’s EDE environment notifies Consumers of their eligibility results prior to QHP enrollment, including when submitting a CiC in the environment. For example, if a Consumer’s APTC or CSR eligibility changes, EDE Entity must notify the Consumer of the change and allow the Consumer to modify his or her QHP selection (if SEP-eligible) or APTC allocation accordingly.</li> <li>– EDE Entity must have a process for providing Consumers with a downloadable EDN in its EDE environment and for providing access to a current EDN via the API. EDE Entity must share required eligibility information that is specified by CMS in the Communications Toolkit.</li> <li>– The Auditor must verify that EDE Entity’s EDE environment is providing status updates and ongoing communications to Consumers according to CMS requirements in the Communications Toolkit as it relates to the status of their application, eligibility, enrollment, notices, and action items the Consumer needs to take.</li> <li>– The EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI.</li> <li>– The EDE Entity must have a means for providing critical communications to the Consumer consistent with the standards above.</li> <li>– The EDE Entity must support all DMLs and SVIs in its post-eligibility application and post-enrollment functionality.</li> </ul> </li> </ul>

Review Category	Requirement and Audit Standard
<b>Accurate Information about the Exchange and Consumer Communications</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must provide Consumers with CMS-provided language informing and educating the Consumers about the Exchanges and HealthCare.gov and Exchange-branded communications Consumers may receive with important action items. CMS defines these requirements in the Communications Toolkit.</li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify that the EDE Entity's EDE environment includes all required language, content, and disclaimers provided by CMS in accordance with the standards stated in guidance and the Communications Toolkit.</li> </ul>
<b>Documentation of Interactions with Consumer Applications or the Exchange</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must implement and maintain tracking functionality on its EDE environment to track Agent, Broker, and Consumer interactions, as applicable, with Consumer applications using a unique identifier for each individual, as well as an individual's interactions with the Exchanges (e.g., application; enrollment; and handling of action items, such as uploading documents to resolve a DMI). This requirement also applies to any actions taken by a downstream Agent or Broker,<sup>38</sup> as well as the Upstream EDE Entity users, of a Primary EDE Entity's EDE environment.</li> <li>▪ <i>Review Standard:</i> The Auditor must verify EDE Entity's process for determining and tracking when an Upstream EDE Entity, downstream Agent or Broker, and Consumer has interacted with a Consumer application or taken actions utilizing the EDE environment or EDE APIs. The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– The EDE Entity's environment tracks, at a minimum, the interactions of Upstream EDE Entities, downstream Agents or Brokers, and Consumers with a Consumer's account, records, application, or enrollment information utilizing the EDE environment or EDE APIs.</li> <li>– The EDE Entity's environment tracks when an upstream Entity, downstream Agent or Broker, or Consumer views a Consumer's record, enrollment information, or application information utilizing the EDE environment or EDE APIs.</li> <li>– The EDE Entity's environment uses unique identifiers to track and document activities by Consumers, downstream Agents and Brokers, and Upstream EDE Entities using the EDE environment.</li> <li>– The EDE Entity's environment tracks interactions with the EDE suite of APIs by an Upstream EDE Entity, a downstream Agent or Broker, or Consumer.</li> <li>– The EDE Entity's environment stores this information for 10 years.</li> </ul> </li> </ul>

<sup>38</sup> Note: References to downstream Agents and Brokers include downstream Agents and Brokers of either the Primary EDE Entity or an Upstream EDE Entity.

Review Category	Requirement and Audit Standard
<b>Eligibility Results Testing and SES Testing</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must submit accurate applications through its EDE environment that result in accurate and consistent eligibility determinations for the supported eligibility scenarios covered by EDE Entity's chosen EDE phase. <ul style="list-style-type: none"> <li>– The business requirements audit package must include testing results in the designated Exchange EDE testing environment. CMS has provided a set of Eligibility Results Toolkits with the eligibility testing scenarios on CMS zONE <a href="https://zone.cms.gov/document/business-audit">https://zone.cms.gov/document/business-audit</a>.</li> </ul> </li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– The Auditor was able to successfully complete a series of test eligibility scenarios in the EDE Entity's EDE environment implementation using the Eligibility Results Toolkits. For example, these scenarios may include Medicaid and CHIP eligibility determinations, and different combinations of eligibility determinations for APTC and CSRs. Note: These scenarios do not test, and are not expected to test, every possible question in the Application UI flow for an EDE Entity's selected phase. In addition to reviewing the eligibility results test cases, the Auditor must review the Application UI for compliance as defined above.</li> <li>– The Auditor must test each scenario and verify that the eligibility results and the eligibility process were identical to the expected results and process. The Auditor must provide CMS confirmation that each relevant eligibility testing scenario was successful, that the expected results were received, and must submit the required proof, as defined in the Eligibility Results Toolkits. This will include screenshots, EDNs, and the raw JSON from the Get App API response for the application version used to complete the scenario. Note: EDNs and raw JSONs are required for all required toolkit scenarios; however, screenshots are only required for the highest phase an entity is submitting (for example, a Prospective phase 3 EDE Entity must submit screenshots for the Phase 3 Eligibility Results Toolkit only, but must submit EDNs and raw JSONs for applicable Phase 1, Phase 2, and Phase 3 toolkit scenarios).</li> </ul> </li> </ul>
<b>API Functional Integration Requirements</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must implement the EDE API suite and corresponding UI functionality in accordance with the API specifications and EDE API Companion Guide provided by CMS. The EDE API specifications and EDE API Companion Guide are available on CMS zONE (<a href="https://zone.cms.gov/document/api-information">https://zone.cms.gov/document/api-information</a>).</li> <li>▪ <i>Review Standard:</i> The Auditor must complete the set of test scenarios as outlined in the API Functional Integration Toolkit to confirm that the EDE Entity's API and corresponding UI integration performs the appropriate functions when completing the various EDE tasks. For example, the Auditor may have to complete a scenario to verify that a Consumer or Agent and Broker is able to view any SVIs or DMIs that may exist for a Consumer, and confirm that the Consumer or Agent and Broker has the ability to upload documents to resolve any SVIs or DMIs. Some of the test cases require that the Auditor and EDE Entity request CMS to process adjudication actions; the Auditor cannot mark these particular test cases as compliant until evaluating whether the expected outcome occurred after CMS takes the requested action. The Auditor will also need to be aware of the following requirements related to the test scenarios: <ul style="list-style-type: none"> <li>– Test scenarios in the API Functionality Integration Toolkit must be completed for both the Consumer pathway and the Agent and Broker pathway if an EDE Entity is pursuing approval to use both pathways.</li> <li>– The API Functional Integration Toolkit includes a "Required Evidence" column, Column H, on the "Test Cases" tab. Auditors will need to submit the applicable "Required Evidence," including the complete header and body for each required API request and response, as part of the audit submission.</li> </ul> </li> </ul>
<b>Application UI Validation</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must implement CMS-defined validation requirements within the application. The validation requirements prevent EDE Entity from submitting incorrect data to the Exchange.</li> <li>▪ <i>Review Standard:</i> The Auditor must confirm that EDE Entity has implemented the appropriate application field-level validation requirements consistent with CMS requirements. These field-level validation requirements are documented in the FFE Application UI Principles document.</li> </ul>

Review Category	Requirement and Audit Standard
<b>Section 508-compliant UI</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> Pursuant to 45 C.F.R. § 155.220(c)(3)(ii)(D) (citing 45 C.F.R. §§ 155.230 and 155.260(b)) and 45 C.F.R. § 156.265(b)(3)(iii) (citing 45 C.F.R. §§ 155.230 and 155.260(b)), Web-brokers and QHP Issuers participating in DE, including all EDE Entities, must implement an eligibility application UI that is Section 508 compliant. A Section 508-compliant application must meet the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)).</li> <li>▪ <i>Review Standard:</i> The Auditor must confirm that EDE Entity's application UI meets the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)). The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– Within the Business Requirements Audit Report Template, the Auditor must confirm that the EDE Entity's application UI is Section 508 compliant. No specific report or supplemental documentation is required.</li> <li>– The Auditor may review results produced by a 508 compliance testing tool. If an EDE Entity uses a 508 compliance testing tool to verify that its application UI is 508 compliant, its Auditor must, at a minimum, review the results produced by the testing tool and document any non-compliance, as well as any mitigation or remediation to address the non-compliance. It is not sufficient for an Auditor to state that an EDE Entity complies with this requirement by confirming that the EDE Entity utilized a 508 compliance testing tool.</li> </ul> </li> </ul>
<b>Non-English-language Version of the Application UI and Communication Materials</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> In accordance with 45 C.F.R. § 155.205(c)(2)(iv)(B) and (C), QHP Issuers and Web-brokers, including those that are EDE Entities, must translate applicable website content (e.g., the application UI) on Consumer-facing websites into any non-English language that is spoken by a limited English proficient (LEP) population that reaches ten (10) percent or more of the population of the relevant State, as determined in current guidance published by the Secretary of HHS.<sup>39</sup> EDE Entities must also translate communications informing Consumers of the availability of Exchange-generated EDNs; critical communications that the Consumer will no longer receive from the Exchange (i.e., if the EDE Entity has implemented and been approved by CMS to assume responsibility for those communications); and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer's use of its EDE environment into any non-English language that is spoken by an LEP population that reaches ten (10) percent or more of the population of the relevant State, as determined in guidance published by the Secretary of HHS.<sup>40</sup></li> <li>▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> <li>– The Auditor must confirm that the non-English-language version of the application UI and associated critical communications are compliant with the Exchange requirements, including the Application UI Toolkit and Communications Toolkit.</li> <li>– The Auditor must verify that the application UI has the same meaning as its English-language version.</li> <li>– The Auditor must also verify that EDE Entity has met all EDE communications translation requirements released by CMS in the Communications Toolkit.</li> <li>– The Auditor must document compliance with this requirement within the Business Requirements Audit Report Template, the Application UI Toolkit, and the Communications Toolkit. In the toolkits, the Auditor can add additional columns for the Auditor compliance findings fields (yellow-shaded columns) or complete the Spanish audit in a second copy of each of the two toolkits.</li> </ul> </li> </ul>

<sup>39</sup> Guidance and Population Data for Exchanges, Qualified Health Plan Issuers, and Web-Brokers to Ensure Meaningful Access by Limited-English Proficient Speakers Under 45 CFR §155.205(c) and §156.250 (March 30, 2016) <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Language-access-guidance.pdf> and “Appendix A- Top 15 Non-English Languages by State” [https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508\\_update12-20-16.pdf](https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508_update12-20-16.pdf).

<sup>40</sup> Frequently Asked Questions (FAQs) Regarding Spanish Translation and Audit Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with Federally-facilitated Exchanges (FFE) (June 20, 2018) provides further information regarding translation and audit requirements: <https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-Spanish-Translation-and-Audit-Requirements.PDF>.

Review Category	Requirement and Audit Standard
<b>EDE Change Management Process</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> EDE Entity must develop and consistently implement processes for managing changes to the EDE environment relevant to the business requirements audit requirements. This requirement does not replace the evaluation necessary for relevant privacy and security controls. At a minimum, the EDE Entity's change management plan must include the following elements: <ul style="list-style-type: none"> <li>– A process that incorporates all elements of the Change Notification SOP as referenced in Section XI.A.i, EDE Entity-initiated Change Request Process;</li> <li>– All application and business audit-related changes are thoroughly defined and evaluated prior to implementation, including the potential effect on other aspects of the EDE end-user experience;</li> <li>– A process for defining regression testing scope and developing or identifying applicable testing scenarios;</li> <li>– A process for conducting regression testing;</li> <li>– A process for identifying and correcting errors discovered through regression testing and re-testing the correction;</li> <li>– A process for maintaining separate testing environments and defining the purposes and releases for each environment;</li> <li>– The change management process must be maintained in writing and relevant individuals must be informed on the change management process and on any updates to the process; and</li> <li>– The change management process must include a process, if applicable, for an EDE Entity to update the non-English-language version of the application UI and communication materials for any changes to the application UI or communication materials in the English-language version of the EDE environment.</li> </ul> </li> <li>▪ <i>Review Standard:</i> The Auditor must evaluate the EDE Entity's change management plan for compliance with the elements and criteria defined above.</li> </ul>
<b>Health Reimbursement Arrangement (HRA) Offer Required UI Messaging</b>	<ul style="list-style-type: none"> <li>▪ <i>Requirement:</i> Phase 3 EDE Entities, Phase 2 EDE Entities that optionally implement full HRA functionality, and EDE Entities that also offer a classic DE pathway, must implement required UI messaging for qualified individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the qualified individuals consistent with CMS guidance. Required UI messaging for various scenarios are detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.<sup>41</sup></li> <li>▪ <i>Review Standard:</i> The Auditor must review the EDE Entity's HRA offer implementation to confirm that the required UI messaging content is displayed for each of the relevant scenarios detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.</li> </ul>

<sup>41</sup> The document FFEs DE API for Web-brokers/Issuers Technical Specifications (Direct Enrollment API Specs) is available on CMS zONE at the following link: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.

## APPENDIX D: REQUIRED DOCUMENTATION

---

The below table describes the required artifacts that the EDE Entity must complete for approval during Year 6 of EDE.<sup>42</sup> Additional details about the documentation related to the privacy and security audit (i.e., Interconnection Security Agreement (ISA), Security Privacy Assessment Report, Plan of Actions & Milestones (POA&M), Privacy Impact Assessment, Non-Exchange Entity System Security and Privacy Plan (NEE SSP), Incident Response Plan and Incident/Breach Notification Plan, Contingency Plan, Configuration Management Plan, and Information Security and Privacy Continuous Monitoring Strategy Guide (ISCM Guide)<sup>43</sup> are provided in related CMS guidance. All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

---

<sup>42</sup> “Year 6 of EDE” refers to the remainder of PY 2023 and PY 2024, including the PY 2024 OEP. The table in Appendix D is an updated combined version of Exhibits 4 and 7 in the “Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.”

<sup>43</sup> These documents are available on CMS zONE at the following link: <https://zone.cms.gov/document/enhanced-direct-enrollment>.

Document	Description	Submission Requirements	Entity Responsible	Deadline
----------	-------------	-------------------------	--------------------	----------

<p><b>Notice of Intent to Participate and Auditor Confirmation</b></p>	<ul style="list-style-type: none"> <li>▪ Once the Prospective Primary and Prospective Phase Change EDE Entity has a confirmed Auditor(s) who will be completing its audit(s), it must notify CMS that it intends to apply to use the EDE pathway for Year 6 of EDE prior to initiating the audit. The email must include the following:             <ul style="list-style-type: none"> <li>– Prospective EDE Entity Name</li> <li>– Auditor Name(s) and Contact Information (Business Requirements and Privacy and Security, if different)</li> <li>– A copy of the executed contract with the Auditor(s) (pricing and proprietary information may be redacted)</li> <li>– EDE Phase (1, 2, or 3)</li> <li>– Prospective EDE Entity Primary Point of Contact (POC) name, email, and phone number. The Primary POC should be a person who is able to make decisions on behalf of the entity</li> <li>– Prospective EDE Entity Technical POC name, email, and phone number. The Technical POC should be a person</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▪ The Prospective Primary and Prospective Phase Change EDE Entity must email <a href="mailto:directenrollment@cms.hhs.gov">directenrollment@cms.hhs.gov</a></li> <li>▪ Subject line should state: “Enhanced DE: Intent.”</li> </ul>	<p>Prospective Primary and Prospective Phase Change EDE Entities</p> <p>Note: CMS is not collecting notices of intent from prospective Upstream EDE Entities.</p>	<p>March 1</p>
--	---	--	---	----------------



Document	Description	Submission Requirements	Entity Responsible	Deadline
	<ul style="list-style-type: none"> <li>– who manages technical development</li> <li>– Prospective EDE Entity Emergency POC name, email, and phone number. The Emergency POC should be a person who should be contacted in an emergency situation.<sup>44</sup></li> <li>– CMS-issued Hub Partner ID</li> </ul>			
<p><b>DE Entity Documentation Package—Privacy Questionnaire (or attestation, if applicable, see Submission Requirements column)</b></p>	<ul style="list-style-type: none"> <li>▪ CMS has provided the privacy questionnaire as part of the DE Entity Documentation Package available on CMS zONE.</li> <li>▪ EDE Entity must populate the privacy questionnaire and return it to CMS for review.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the DE/EDE Entity PME Site</li> <li>▪ If an EDE Entity's responses to the privacy questionnaire are unchanged from the EDE Entity's last submission of a privacy questionnaire, the Entity may submit an attestation stating that the previously submitted questionnaire remains accurate.</li> <li>– The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents.</li> </ul>	<p>Prospective Primary EDE Entities</p>	<p>Submit with audit submission</p>

<sup>44</sup> CMS will send EDE related communications to the POCs listed in the EDE Entity's Notice of Intent to Participate. EDE Entities can change these POCs at any time by emailing [directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov).

Document	Description	Submission Requirements	Entity Responsible	Deadline
<p><b>DE Entity Documentation Package—Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements column)</b></p>	<ul style="list-style-type: none"> <li>▪ Submit the URL and text of each privacy policy statement displayed on your website and your website's Terms of Service in a Microsoft Word document or a PDF.</li> <li>▪ The privacy policy and terms of service must be submitted for any EDE Entity's website that is collecting Consumer data as part of the EDE end-user experience.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the DE/EDE PME Site</li> <li>▪ If an EDE Entity's privacy policy and Terms of Service remain unchanged from the EDE Entity's last submission of the privacy policy and Terms of Service, the Entity may submit an attestation stating that the previously submitted privacy policy and Terms of Service will remain unchanged. <ul style="list-style-type: none"> <li>– The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents</li> </ul> </li> </ul>	<p>Both Prospective Primary and Prospective Upstream EDE Entities</p>	<p>Prospective Primary EDE Entities: Submit with audit submission.</p> <p>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for prospective Upstream EDE Entities, but to be reasonably certain a prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs.</p>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>EDE Business Agreement</b>	<ul style="list-style-type: none"> <li>▪ EDE Entities must execute the EDE Business Agreement to use the EDE pathway. The agreement must identify the Entity's selected Auditor(s) (if applicable).</li> <li>▪ CMS will countersign the EDE Business Agreement after CMS has reviewed and approved the EDE Entity's business requirements audit and the privacy and security audit.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the DE/EDE Entity PME Site</li> </ul>	Both Prospective Primary and Prospective Upstream EDE Entities	<p>Prospective Primary EDE Entities: Submit with audit submission.</p> <p>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for Prospective Upstream EDE Entities, but to be reasonably certain a Prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs.</p>
<b>DE Entity Documentation Package—Operational and Oversight Information</b>	<ul style="list-style-type: none"> <li>▪ EDE Entities must submit the operational and oversight information to CMS to use the EDE pathway. This form must be filled out completely.</li> <li>▪ The form is an Excel file that the EDE Entity will complete and submit to CMS.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the DE/EDE Entity PME Site</li> <li>▪ Prospective Primary EDE Entities will receive an encrypted, pre-populated version of the form from CMS</li> <li>▪ Prospective Upstream EDE Entities will complete a blank version of the form that is available on CMS zONE</li> </ul>	Both Prospective Primary and Prospective Upstream EDE Entities	<p>Prospective Primary EDE Entities: Submit with audit submission.</p> <p>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for Prospective Upstream EDE Entities, but to be reasonably certain a Prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs.</p>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Business Audit Report and Toolkits</b>	<ul style="list-style-type: none"> <li>EDE Entities must submit the Business Requirements Audit Report Template and all applicable toolkits completed by its Auditor(s).</li> <li>See Section VI.B.ii, Business Requirements Audit Resources, Exhibit 5, for more information.</li> </ul>	<ul style="list-style-type: none"> <li>The EDE Entity and its Auditor(s) must submit the different parts of the Auditor resources package via the DE/EDE Entity PME Site</li> </ul>	Prospective Primary EDE Entities, Prospective Phase Change EDE Entities, and their Auditors	April 1 -July 1 (3:00 AM ET)
<b>Training</b>	<ul style="list-style-type: none"> <li>EDE Entities (and their Auditors) must complete the trainings as outlined in Section VIII, Required Auditor and EDE Entity Training.</li> <li>The trainings are located on REGTAP (located at the following link: <a href="https://www.regtap.info/">https://www.regtap.info/</a>).</li> </ul>	<ul style="list-style-type: none"> <li>The person taking the training must complete the course conclusion pages at the end of each module</li> <li>The EDE Entity and Auditor are NOT required to submit anything additional to CMS but must retain a copy of the training confirmation webpage to provide to CMS, if requested</li> </ul>	Prospective Primary EDE Entities, Prospective Phase Change EDE Entities, Prospective Upstream EDE Entities, and Auditors	<p>Trainings must be completed by Prospective Primary and Phase Change EDE Entities and Auditors prior to Audit Submission</p> <p>Prospective Upstream EDE Entities must complete the training prior to approval to use the EDE pathway</p>
<b>HUB Onboarding Form</b>	<ul style="list-style-type: none"> <li>All EDE Entities must submit a new or updated Hub Onboarding Form to request EDE access. If an EDE Entity does not already have a Partner ID, the Hub will create a Partner ID for the EDE Entity upon receiving the Hub Onboarding Form.</li> </ul>	<ul style="list-style-type: none"> <li>Follow instructions on the Hub Onboarding Form (located at the following link: <a href="https://zone.cms.gov/document/hub-onboarding-form">https://zone.cms.gov/document/hub-onboarding-form</a>)</li> <li>Send to <a href="mailto:HubSupport@sparksoftcorp.com">HubSupport@sparksoftcorp.com</a></li> </ul>	Prospective Primary and Prospective Upstream EDE Entities	Prior to accessing the EDE APIs

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Application Technical Assistance and Mini Audit Testing Credentials</b>	<ul style="list-style-type: none"> <li>▪ An EDE Entity must provide application technical assistance and mini audit testing credentials to CMS consistent with the process defined in Sections VI.C, Application Technical Assistance and X.D, Audit Submission Compliance Review for Prospective Primary EDE Entities, below.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Follow instructions on the EDE UI Eligibility Technical Assistance Credentials Form Template on CMS zONE: <a href="https://zone.cms.gov/document/eligibility-information">https://zone.cms.gov/document/eligibility-information</a></li> </ul>	Prospective Primary EDE Entities and Prospective Phase Change EDE Entities	Submit with audit submission date

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Interconnection Security Agreement (ISA)</b>	<ul style="list-style-type: none"> <li>▪ A Prospective Primary EDE Entity must submit the ISA to use the EDE pathway.</li> <li>▪ CMS will countersign the ISA after CMS has reviewed and approved the EDE Entity's business requirements audit and privacy and security audit.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective Primary EDE Entity must submit the ISA via the DE/EDE Entity PME Site.</li> <li>▪ The ISA contains Appendices that must be completed in full for an EDE Entity to be considered for approval.</li> <li>▪ Appendix B of the ISA must detail:               <ol style="list-style-type: none"> <li>(1) all arrangements with Upstream EDE Entities and any related data connections or exchanges,</li> <li>(2) any arrangements involving Web-brokers, and</li> <li>(3) any arrangements with downstream agents and brokers that involve limited data collections, as described in Section IV.B, Downstream Third-party Agent and Broker Arrangements.</li> </ol> </li> <li>▪ Appendix B of the ISA must be updated and resubmitted as a Primary EDE Entity adds or changes any of the arrangements noted above consistent with the requirements in the ISA.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit with the audit submission</li> </ul>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Security Privacy Controls Assessment Test Plan (SAP)</b>	<ul style="list-style-type: none"> <li>▪ This report is to be completed by the Auditor and submitted to CMS prior to initiating the audit.</li> <li>▪ The SAP describes the Auditor's scope and methodology of the assessment. The SAP includes an attestation of the Auditor's independence.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the SAP completed by its Auditor via the DE/EDE Entity PME Site.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ At least thirty (30) Days before commencing the privacy and security audit; during the planning phase</li> </ul>
<b>Security Privacy Assessment Report (SAR)</b>	<ul style="list-style-type: none"> <li>▪ This report details the Auditor's assessment findings of the Prospective EDE Entity's security and privacy controls implementation.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the SAR completed by its Auditor via the DE/EDE Entity PME Site.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ April 1 – July 1 (3:00 AM ET)</li> </ul>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Plan of Action &amp; Milestones (POA&amp;M)</b>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity must submit a POA&amp;M if its Auditor identifies any privacy and security compliance issues in the SAR.</li> <li>▪ The POA&amp;M details a corrective action plan and the estimated completion date for identified milestones.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the POA&amp;M in conjunction with the SAR via the DE/EDE Entity PME Site.</li> <li>▪ POA&amp;Ms with outstanding findings must be submitted monthly to CMS until all the findings from security controls assessments, security impact analyses, and continuous monitoring activities described in the NEE SSP controls CA-5 and CA-7 are resolved. Prospective EDE Entities can schedule their own time for monthly submissions of the POA&amp;M, but must submit an update monthly to CMS until all significant or major findings are resolved. Thereafter, quarterly POA&amp;M submissions are required as part of the ISCM activities.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Initial: April 1 – July 1 (3:00 AM ET)</li> <li>▪ Monthly submissions, as necessary, if outstanding findings.</li> <li>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit quarterly POA&amp;Ms by the last business Day of March, July, September, and December.</li> </ul>



Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Risk Acceptance Form</b>	<ul style="list-style-type: none"> <li>▪ The Risk Acceptance Form records the weaknesses that require an official risk acceptance from the organization's Authorizing Official.</li> <li>▪ Before deciding to accept the risks, the relevant NEE's authorities should rigorously explore ways to mitigate the risks.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Once the risk has been identified and deemed acceptable by the NEE's authorized official, the NEE must complete the entire Risk Acceptance Form and submit the completed form to CMS. The NEE will continue to track all accepted risks in the NEE's official POA&amp;M.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ The Risk Acceptance Form should be submitted with the POA&amp;M during the regular POA&amp;M submission schedule.</li> </ul>
<b>Privacy Impact Assessment (PIA)</b>	<ul style="list-style-type: none"> <li>▪ The PIA will detail the Prospective EDE Entity's evaluation of its controls for protecting PII.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity is not required to submit the PIA to CMS. However, per the ISA, CMS may request and review an EDE Entity's PIA at any time, including for audit purposes.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Before commencing the privacy and security audit as part of the NEE SSP</li> </ul>
<b>Non-Exchange Entity System Security and Privacy Plan (NEE SSP)</b>	<ul style="list-style-type: none"> <li>▪ The NEE SSP will include detailed information about the Prospective EDE Entity's implementation of required security and privacy controls.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective Primary EDE Entity must submit the completed NEE SSP via the DE/EDE Entity PME Site before commencing the privacy and security audit.</li> <li>▪ The implementation of security and privacy controls must be completely documented in the NEE SSP before the audit is initiated.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Before commencing the privacy and security audit</li> </ul>

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Incident Response Plan and Incident/Breach Notification Plan</b>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity is required to implement Breach and Incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures.</li> <li>▪ A Prospective EDE Entity must incorporate these procedures into its own written policies and procedures.<sup>45</sup></li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity is not required to submit the Incident Response Plan and Incident/Breach Notification Plan to CMS. A Prospective EDE Entity must have procedures in place to meet CMS security and privacy Incident reporting requirements. CMS may request and review an EDE Entity's Incident Response Plan and Incident/Breach Notification Plan at any time, including for audit purposes.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Before commencing the privacy and security audit as part of the NEE SSP</li> </ul>

<sup>45</sup> <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf>.

<p><b>Annual Penetration Testing</b></p>	<ul style="list-style-type: none"> <li>▪ The penetration test must include the EDE environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10.</li> <li>▪ Before conducting the penetration testing, the EDE Entity must execute a Rules of Engagement with their Auditor’s penetration testing team.</li> <li>▪ The EDE Entity must also notify their CMS designated technical counterparts on their annual penetration testing schedule and must provide the following information to CMS, a minimum of five (5) business Days using the CMS-provided form<sup>46</sup>, prior to initiation of the penetration testing:             <ul style="list-style-type: none"> <li>– Period of testing performance (specific times for all penetration testing should be contained in individual test plans);</li> <li>– Target environment resources to be tested (IP addresses, Hostname, URL); and</li> <li>– Any restricted hosts, systems, or subnets that are not to be tested.</li> </ul> </li> <li>▪ During the penetration testing, the Auditor’s testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment.</li> <li>▪ The penetration testing shall be conducted in the lower environment that mirrors the production environment.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the Penetration Test results with the SAR via the DE/EDE Entity PME Site.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Initial: April 1 – July 1 (3:00 AM ET)</li> <li>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities perform penetration testing and submit results to CMS annually, prior to last business Day in July.</li> </ul>
--	---	--	--	---

Document	Description	Submission Requirements	Entity Responsible	Deadline
<b>Vulnerability Scan</b>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity is required to conduct monthly Vulnerability Scans.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A Prospective EDE Entity and its Auditor must submit the last three months of their Vulnerability Scan Reports, in conjunction with POA&amp;M and SAR via the DE/EDE Entity PME Site.</li> <li>▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&amp;M.</li> <li>▪ Similar findings can be consolidated.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Initial: April 1 – July 1 (3:00 AM ET)</li> <li>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit Vulnerability Scans annually.</li> </ul>

<sup>46</sup> The Penetration Testing Notification Form is available at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

## APPENDIX E: AUDITOR IDENTIFICATION

---

EDE Entity agrees to identify, in Part I below, all Auditors selected to complete the Operational Readiness Review (ORR) and any subcontractors of the Auditor(s), if applicable. In the case of multiple Auditors, please indicate the role of each Auditor in completing the ORR (i.e., whether the Auditor will conduct the business requirements audit and/or the privacy and security audit, including the completion of an annual assessment of security and privacy controls by an Auditor, as described in the Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide). Include additional sheets, if necessary. EDE Entity must identify the ISCM Auditor that conducted the ISCM immediately preceding this Agreement's submission and execution.

If an Upstream EDE Entity will contract with an Auditor to audit additional functionality or systems added to its Primary EDE Entity's EDE Environment, pursuant to Section VIII.g or VIII.h of this Agreement, complete Part I to indicate the Auditor(s) that will conduct the business requirements audit and/or privacy and security audit of the additional functionality or systems.

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

### **TO BE FILLED OUT BY EDE ENTITY**

Primary EDE Entities, Hybrid Issuer Upstream EDE Entities, and Hybrid Non-Issuer Upstream EDE Entities must complete Part I.

#### **I. Complete These Rows if EDE Entity Is Subject to an Audit (ORR, ISCM, and/or Supplemental Audit)**

Printed Name and Title of Authorized Official of Auditor 1	Shibani Gupta
Auditor 1 Business Name	Absurance
Auditor 1 Address	5300 Ranch Point, Katy, TX 77494
Printed Name and Title of Contact of Auditor 1 (if different from Authorized Official)	
Auditor 1 Contact Phone Number	REDACTED
Auditor 1 Contact Email Address	REDACTED
Subcontractor Name & Information (if applicable)	
Audit Role	Auditor - Business and Privacy & Security Audits
Printed Name and Title of Authorized Official of Auditor 2	
Auditor 2 Business Name	
Auditor 2 Address	

Printed Name and Title of Contact of Auditor 2 (if different from Authorized Official)	
Auditor 2 Contact Phone Number	
Auditor 2 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	
Printed Name and Title of Authorized Official of Auditor 3	
Auditor 3 Business Name	
Auditor 3 Address	
Printed Name and Title of Contact of Auditor 3 (if different from Authorized Official)	
Auditor 3 Contact Phone Number	
Auditor 3 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	

**APPENDIX F: CONFLICT OF INTEREST DISCLOSURE FORM**

---

**TO BE FILLED OUT BY EDE ENTITY**

EDE Entity must disclose to the Department of Health & Human Services (HHS) any financial relationships between the Auditor(s) identified in Appendix E of this agreement, and individuals who own or are employed by the Auditor(s), and individuals who own or are employed by a Direct Enrollment (DE) Entity for which the Auditor(s) is conducting an Operational Readiness Review pursuant to 45 C.F.R. § 155.221(b)(4) and (f). EDE Entity must disclose any affiliation that may give rise to any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence.

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

Please describe below any relationships, transactions, positions (volunteer or otherwise), or circumstances that you believe could contribute to a conflict of interest:

- Not applicable; EDE Entity is not contracting with an Auditor.
- EDE Entity has no conflict of interest to report for the Auditor(s) identified in Appendix E.
- EDE Entity has the following conflict of interest to report for the Auditor(s) identified in Appendix E:

1. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
2. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
3. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## APPENDIX G: APPLICATION END-STATE PHASES

The below table describes each of the three end-state phases for hosting applications using the EDE Pathway.<sup>47</sup> EDE Entity must indicate the end-state phase it has selected in the “Operational and Oversight Information” form provided by CMS. All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

End State Phases	Description	Benefits
<b>Phase 1: Host Simplified Application + EDE API Suite</b>	<p>EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following:</p> <ul style="list-style-type: none"> <li>▪ Application filer (and others on application, if applicable) resides in the application state and all dependents have the same permanent address, if applicable</li> <li>▪ Application filer plans to file a federal income tax return for the coverage year; if married plans to file a joint federal income tax return with spouse</li> <li>▪ Application filer (and spouse, if applicable) is not responsible for a child 18 or younger who lives with the Application filer but is not on his/her federal income tax return</li> <li>▪ No household members are full-time students aged 18-22</li> <li>▪ No household member is pregnant</li> <li>▪ All Applicants are U.S. citizens</li> <li>▪ All Applicants can enter Social Security Numbers (SSNs)</li> <li>▪ No Applicants are applying under a name different than the one on his/her Social Security cards</li> <li>▪ No Applicants were born outside of the U.S. and became naturalized or derived U.S. citizens</li> <li>▪ No Applicants are currently incarcerated (detained or jailed)</li> <li>▪ No household members are American Indian or Alaska Native</li> <li>▪ No Applicants are offered health coverage through a job or COBRA</li> <li>▪ No Applicants are offered an individual coverage health reimbursement arrangement (HRA) or qualified small employer health reimbursement arrangement (QSEHRA)</li> <li>▪ No Applicants were in foster care at age 18 and are currently 25 or younger</li> <li>▪ All dependents are claimed on the Application filer's federal income tax return for the coverage year</li> <li>▪ All dependents are the Application filer's children who are single (not married) and 25 or younger</li> <li>▪ No dependents are stepchildren or grandchildren</li> <li>▪ No dependents live with a parent who is not on the Application filer's federal income tax return</li> </ul>	<p>Lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.</p>

<sup>47</sup> The table in Appendix G is an updated version of Exhibit 3 in the “Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.”



End State Phases	Description	Benefits
<b>Phase 2: Host Expanded Simplified Application + EDE API Suite</b>	<p>EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following:</p> <ul style="list-style-type: none"> <li>▪ All scenarios covered by Phase 1</li> <li>▪ Full-time student</li> <li>▪ Pregnant application members</li> <li>▪ Non-U.S. citizens</li> <li>▪ Naturalized U.S. citizens</li> <li>▪ Application members who do not provide an SSN</li> <li>▪ Application members with a different name than the one on their SSN cards</li> <li>▪ Incarcerated application members</li> <li>▪ Application members who previously were in foster care</li> <li>▪ Stepchildren</li> </ul>	<p>Second lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.</p>
<b>Phase 3: Host Complete Application + EDE API Suite</b>	<p>EDE Entity hosts an application that supports all application scenarios (equivalent to existing HealthCare.gov):</p> <ul style="list-style-type: none"> <li>▪ All scenarios covered in Phase 2</li> <li>▪ American Indian and Alaskan Native household members</li> <li>▪ Application members with differing home addresses or residing in a State separate from where they are applying for coverage</li> <li>▪ Application members with no home address</li> <li>▪ Application members not planning to file a tax return</li> <li>▪ Married application members not filing jointly</li> <li>▪ Application members responsible for a child age 18 or younger who lives with them, but is not included on the Application filer's federal income tax return (parent/caretaker relative questions)</li> <li>▪ Application members offered coverage through their job, someone else's job, or COBRA</li> <li>▪ Application members with dependent children who are over age 25 or who are married</li> <li>▪ Application members with dependent children living with a parent not on their federal income tax return</li> <li>▪ Dependents who are not sons/daughters</li> <li>▪ Applicants who are offered an individual coverage HRA or QSEHRA</li> </ul>	<p>Highest level of effort to implement and audit. EDE Entity would provide and service the full range of Consumer scenarios. Additionally, the EDE Entity would no longer need to redirect Consumers to alternative pathways for complex eligibility scenarios. Please note that the implementation of Phase 3 is comparatively more complex than the other phases and may require more time to implement, audit, and approve.</p>

**APPENDIX H: TECHNICAL AND TESTING STANDARDS  
FOR USING THE EDE PATHWAY**

---

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions the meaning provided in 45 C.F.R. § 155.20.

- (1) EDE Entity must possess a unique Partner ID assigned by the Centers for Medicare & Medicare Services (CMS). EDE Entity must use its Partner ID when interacting with the CMS Data Services Hub (Hub) and the EDE Application Program Interfaces (APIs) for EDE Entity's own line of business.

If EDE Entity uses a Primary EDE Entity's EDE Environment, EDE Entity must use its own Partner ID when interacting with the Hub and the EDE APIs. If EDE Entity is a Primary EDE Entity and provides an EDE Environment to another EDE Entity, as permitted under Section VIII.f, VIII.g, and VIII.h of this Agreement, the Primary EDE Entity must use the Partner ID assigned to the EDE Entity using its EDE Environment for any Hub or EDE API interactions for the other EDE Entity. If EDE Entity is a Primary EDE Entity, it must provide to CMS the Partner IDs of all entities that will implement and use Primary EDE Entity's EDE Environment.

- (2) CMS will provide EDE Entity with information outlining EDE API Specifications and with EDE-related Companion Guides, including the EDE Companion Guide, the Federally-facilitated Exchange (FFE) User Interface (UI) Application Principles for Integration with FFE APIs, and the UI Question Companion Guide, which is embedded within the FFE UI Application Principles for Integration with FFE APIs. The terms of these documents are specifically incorporated herein. EDE Entity's use of the EDE Environment must comply with any standards detailed in the EDE API Specifications guidance and the EDE-related Companion Guides.
- (3) EDE Entity must complete testing for each Hub-related transaction it will implement, and it shall not be allowed to exchange data with CMS in production mode until testing is satisfactorily passed, as determined by CMS in its sole discretion. Successful testing generally means the ability to pass approved standards, and to process data transmitted by EDE Entity to the Hub. The capability to submit these test transactions must be maintained by EDE Entity throughout the term of this Agreement.
- (4) EDE Entity agrees to submit test transactions to the Hub prior to the submission of any transactions to the FFE production system, and to determine that the transactions and responses comply with all requirements and specifications approved by CMS and/or the CMS contractor.
- (5) EDE Entity agrees that prior to the submission of any additional transaction types to the FFE production system, or as a result of making changes to an existing transaction type or system, it will submit test transactions to the Hub in accordance with paragraph (3) and (4) above.

- (6) EDE Entity acknowledges that CMS requires successful completion of an Operational Readiness Review (ORR) to the satisfaction of CMS, which must occur before EDE Entity is able to execute an ISA with CMS or submit any transactions using its EDE Environment to the FFE production system. The ORR will assess EDE Entity's compliance with CMS' regulatory requirements, this Agreement, and the Interconnection Security Agreement (ISA), including the required privacy and security controls. This Agreement may be terminated or access to CMS systems may be denied for a failure to comply with CMS requirements in connection to an ORR.
- (7) Upon approval for a significant change in the EDE Environment, including, but not limited to, initial approval to go-live with an EDE Environment, approval to go-live with an end-state phase change, or approval to proceed with a significant change to EDE Environment functionality, EDE Entity will limit enrollment volume in its production environment in accordance with the scale and schedule set by CMS, in its sole discretion, until CMS has verified the successful implementation of the EDE Entity's EDE Environment in production.
- (8) CMS, in its sole discretion, may restrict, delay, or deny an EDE Entity's ability to implement a significant change in the EDE Environment, consistent with paragraph (7) of this Appendix, if an EDE Entity has not maintained compliance with program requirements or the EDE Entity has triggered the conditions for Inactive, Approved Primary EDE Entities (Section IX.v of this Agreement). Failure to maintain compliance with program requirements includes, but is not limited to, an inability to meet CMS-issued deadlines for CMS-initiated Change Requests (Section IX.d of this Agreement) or failure to maintain an EDE Environment that complies with the standards detailed in the EDE API Specifications guidance and the EDE-related Companion Guides.
- (9) All compliance testing (Operational, Management and Technical) of EDE Entity will occur at a FIPS 199 MODERATE level due to the Personally Identifiable Information (PII) data that will be contained within EDE Entity's systems.

# Exhibit G

**AGREEMENT BETWEEN WEB-BROKER AND  
THE CENTERS FOR MEDICARE & MEDICAID SERVICES  
FOR THE FEDERALLY-FACILITATED EXCHANGES  
AND STATE-BASED EXCHANGES ON THE FEDERAL PLATFORM**

---

**THIS WEB-BROKER AGREEMENT** (“Agreement”) is entered into by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES (“CMS”), as the Party (as defined below) responsible for the management and oversight of the Federally-facilitated Exchanges (“FFE’s”), also referred to as “Federally-facilitated Marketplaces” or “FFMs” and the operation of the federal eligibility and enrollment platform, which includes the CMS Data Services Hub (“Hub”), relied upon by certain State-based Exchanges (“SBE’s”) for their eligibility and enrollment functions (including State-based Exchanges on the Federal Platform [“SBE-FPs”]), and TrueCoverage LLC

(hereinafter referred to as Web-broker), a Web-broker that uses a non-FFE Internet website in accordance with 45 C.F.R. §§ 155.220(c) and 155.221 to assist Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees in applying for eligibility for enrollment in Qualified Health Plans (“QHPs”) and for Advance Payments of the Premium Tax Credits (“APTCs”) and Cost-sharing Reductions (“CSRs”) for QHPs, and/or in completing enrollment in QHPs offered in the individual market through the FFEs or SBE-FPs, in applying for a determination of eligibility to participate in the FF-Small Business Health Options Program (“FF-SHOPs”) or SBE-FP SHOPS and/or in completing enrollment in QHPs offered through the FF-SHOPs or SBE-FP SHOPS; and providing related Customer Service. CMS and Web-broker are hereinafter referred to as the “Party” or, collectively, as the “Parties.” Unless otherwise noted, the provisions of this Agreement are applicable to Web-brokers seeking to assist Qualified Employers and Qualified Employees in purchasing and enrolling in coverage through an FF-SHOP or SBE-FP SHOP.

**WHEREAS:**

1. Section 1312(e) of the Affordable Care Act (“ACA”) provides that the Secretary of the U.S. Department of Health & Human Services (“HHS”) shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals, Qualified Employers, and Qualified Employees in QHPs through an Exchange, and to assist individuals in applying for APTC and CSRs, to the extent allowed by States. To participate in the FFEs or SBE-FPs, including an FF-SHOP or SBE-FP SHOP, Agents, Brokers, and Web-brokers must complete all necessary registration and training requirements under 45 C.F.R. § 155.220.
2. To facilitate the eligibility determination and enrollment processes, CMS will provide centralized and standardized business and technical services (“Hub Web Services”) through application programming interfaces (“APIs”) to Web-broker that will enable Web-broker to establish a secure connection with the Hub. The APIs will enable the secure transmission of key eligibility and enrollment Information between CMS and Web-broker. The Hub Web Services are not available for SHOP.
3. To facilitate the operation of the FFEs and SBE-FPs, CMS desires to: (a) disclose Personally Identifiable Information (“PII”), which is held in the Health Insurance Exchanges Program (“HIX”), to Web-broker; (b) provide Web-broker with access to the Hub Web Services, if applicable; and (c) permit Web-broker to create, collect, disclose,

access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—to the extent that these activities are necessary to carry out the functions that the ACA and implementing regulations permit Web-broker to carry out. The Hub Web Services are not available for SHOP.

4. Web-broker is an individual or entity licensed as an insurance producer, Agent, or Broker by the applicable State regulatory authority in at least one FFE or SBE-FP State; OR Web-broker is an Agent or Broker Direct Enrollment Technology Provider.
5. Web-broker desires to gain access to the Hub Web Services, and to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—to perform the Authorized Functions described in Section II.a of this Agreement. The Hub Web Services are not available for SHOP.
6. 45 C.F.R. § 155.260(b) provides that an Exchange must, among other things, require as a condition of contract or agreement with Non-Exchange Entities that the Non-Exchange Entity comply with privacy and security standards that are consistent with the standards in 45 C.F.R. §§ 155.260(a)(1) through (a)(6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 C.F.R. § 155.260(a)(3).
7. CMS has adopted privacy and security standards with which the Web-broker, a type of Non-Exchange Entity, must comply, which are set forth in Appendix A: Privacy and Security Standards for , Appendix B: Annual Security and Privacy Assessment (SPA), and the Non-Exchange Entity System Security and Privacy Plan (NEE SSP).<sup>1</sup>

Now, therefore, in consideration of the promises and covenants herein contained, the adequacy of which the Parties acknowledge, the Parties agree as follows:

I. Definitions.

Capitalized terms not otherwise specifically defined herein shall have the meaning set forth in the Appendix C: Definitions. Any capitalized term that is not defined herein or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

II. Acceptance of Standard Rules of Conduct.

Web-broker and CMS are entering into this Agreement to satisfy the requirements under 45 C.F.R. § 155.260(b)(2). Web-broker hereby acknowledges and agrees to accept and abide by the standard rules of conduct set forth below and in the Appendices, which are incorporated by reference in this Agreement, while and as engaging in any activity as Web-broker for purposes of the ACA. Web-broker shall strictly adhere to the privacy and security standards—and ensure that its employees, officers, directors, contractors, subcontractors, agents, and

---

<sup>1</sup> The references in this Agreement to security and privacy controls and implementation standards can be found in the NEE SSP located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

representatives strictly adhere to the same—to gain and maintain access to the Hub Web Services, if applicable, and to create, collect, disclose, access, maintain, store, and use PII for the efficient operation of the FFEs and SBE-FPs.

- a. Authorized Functions. Web-broker may create, collect, disclose, access, maintain, store, and use PII for:
  1. Assisting with application, eligibility, and enrollment processes for QHP offered through the FFEs and SBE-FPs, including FF-SHOPS and SBE-FP-SHOPS;
  2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons;
  3. Assisting with completing applications for the receipt of APTC or CSRs and with selecting an APTC amount, if applicable;
  4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR determination, if applicable;
  5. Assisting with the application for and determination of certificates of exemption, if applicable;
  6. Assisting with filing appeals of eligibility determinations in connection with the FFEs and SBE-FPs, including Qualified Employer appeals for FF-SHOPS and SBE-FP-SHOPS;
  7. Transmitting Information about the Consumer's, Applicant's, Qualified Individual's, or Enrollee's decisions regarding QHP enrollment and/or CSR and APTC Information to the FFEs and SBE-FPs, if applicable;
  8. Facilitating payment of the initial premium amount to the appropriate individual market QHP, if applicable;
  9. Facilitating payment of the initial and group premium amount for FF-SHOP and SBE-FP SHOP coverage, if applicable;
  10. Facilitating an Enrollee's ability to disenroll from a QHP;
  11. Educating Consumers, Applicants, or Enrollees on Insurance Affordability Programs and, if applicable, informing such individuals of eligibility for Medicaid or the Children's Health Insurance Program ("CHIP");
  12. Assisting Enrollees to report changes in eligibility status to the FFEs and SBE-FPs throughout the coverage year, including changes that may affect eligibility (e.g., adding a dependent);
  13. Handling FF-SHOP or SBE-FP SHOP coverage changes throughout the plan year that may impact eligibility, including, but not limited to, adding a new hire, removing an Employee no longer employed at the company, removing an Employee no longer employed full-time, and adding a newborn or spouse during a special enrollment period, if applicable;
  14. Correcting errors in the application for QHP enrollment;



15. Informing or reminding Enrollees when QHP coverage should be renewed, when Enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform Enrollees of QHP coverage options at renewal;
  16. Providing appropriate Information, materials, and programs to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees—or these individuals’ legal representatives or Authorized Representatives—to inform and educate them about the use and management of their health Information, as well as medical services and benefit options offered through the selected QHP or among the available QHP options;
  17. Contacting Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers and Qualified Employees—or these individuals’ legal representatives or Authorized Representatives—to assess their satisfaction or resolve complaints with services provided by Web-broker in connection with the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs, the Web-broker, or QHPs;
  18. Providing assistance in communicating with QHP Issuers;
  19. Providing Customer Service activities related to FF-SHOP or SBE-FP SHOP coverage if permitted under State and federal law, including correction of errors on FF-SHOP or SBE-FP SHOP applications and policies, handling complaints and appeals regarding FF-SHOP or SBE-FP SHOP coverage, responding to questions about FF-SHOP or SBE-FP insurance policies, assisting with communicating with State regulatory authorities regarding FF-SHOP or SBE-FP SHOP issues, and assistance in communicating with CMS;
  20. Fulfilling the legal responsibilities related to the efficient functions of QHP Issuers in the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs, as permitted or required by Web-broker’s contractual relationships with QHP Issuers; and
  21. Performing other functions substantially similar to those enumerated above and such other functions that CMS may approve in writing from time to time.
- b. Standards for Handling PII. Web-broker agrees that it will create, collect, disclose, access, maintain, use, or store PII that it receives directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, Qualified Employees—or these individuals’ legal representatives or Authorized Representatives—and from Hub Web Services, if applicable, only in accordance with all laws as applicable, including section 1411(g) of the ACA. The Hub Web Services are not available for SHOP.
1. Security and Privacy Controls. Web-broker agrees to monitor, periodically assess, and update its security and privacy controls documented in the NEE SSP and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including Appendix A: Privacy and Security Standards for , Appendix B: Annual Security and Privacy Assessment (SPA), NEE Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide, and the NEE SSP. Furthermore, Web-broker agrees to timely inform the Exchange of any material change in its administrative, technical, or operational environments, or any material change that would require an alteration of the privacy and security standards within this Agreement.



2. Downstream and Delegated Entities. Web-broker will satisfy the requirement in 45 C.F.R. § 155.260(b)(2)(v) to bind downstream and delegated entities to the same privacy and security standards that apply to Non-Exchange Entities by entering into written agreements with any downstream and delegated entities that will have access to PII as defined in this Agreement. Web-broker must require in writing all downstream and delegated entities adhere to the terms of this Agreement.
- c. Collection of PII. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, Web-broker may create, collect, disclose, access, maintain, store, and use the following data and PII from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees—or these individuals’ legal representatives or Authorized Representatives—including, but not limited to:
1. For individual market QHP coverage:
    - APTC percentage and amount applied
    - Auto disenrollment Information
    - Applicant name
    - Applicant address
    - Applicant birthdate
    - Applicant telephone number
    - Applicant email
    - Applicant Social Security Number
    - Applicant spoken and written language preference
    - Applicant Medicaid Eligibility indicator, start and end dates
    - Applicant CHIP eligibility indicator, start and end dates
    - Applicant QHP eligibility indicator, start and end dates
    - Applicant APTC percentage and amount applied eligibility indicator, start and end dates
    - Applicant household income
    - Applicant maximum APTC amount
    - Applicant CSR eligibility indicator, start and end dates
    - Applicant CSR level
    - Applicant QHP eligibility status change
    - Applicant APTC eligibility status change
    - Applicant CSR eligibility status change
    - Applicant Initial or Annual Open Enrollment Indicator, start and end dates
    - Applicant Special Enrollment Period eligibility indicator and reason code
    - Contact name
    - Contact address
    - Contact birthdate
    - Contact telephone number
    - Contact email
    - Contact spoken and written language preference
    - Enrollment group history (past six months)
    - Enrollment type period
    - FFE Applicant ID

- FFE Member ID
- Issuer Member ID
- Net premium amount
- Premium amount, start and end dates
- Credit or Debit Card Number, name on card
- Checking account and routing number
- Special Enrollment Period reason
- Subscriber indicator and relationship to subscriber
- Tobacco use indicator and last date of tobacco use
- Custodial parent
- Health coverage
- American Indian/Alaska Native status and name of tribe
- Marital status
- Race/ethnicity
- Requesting financial assistance
- Responsible person
- Dependent name
- Applicant/dependent sex
- Student status
- Subscriber indicator and relationship to subscriber
- Total individual responsibility amount

2. For SHOP QHP coverage:

**Category**  
**Description**

Employee PII  
 Employee Applicant Name  
 Employee Unique Employer Code  
 Employee Home Address  
 Employee Applicant Mailing Address  
 Employee Applicant Birthdate  
 Employee Social Security Number  
 Employee Applicant Telephone Number (and type)  
 Employee Applicant Email Address  
 Employee Applicant Spoken and Written Language Preference  
 Employee Tobacco Use Indicator and Last Date of Tobacco Use  
 Employee Sex  
 Employee Race and Ethnicity  
 Employer Business Name  
 If American Indian/Alaska Native: Name and Location of Tribe  
 Health Coverage Type (Individual or Family, if offered)  
 Health Plan Name and ID Number  
 Dental Plan Name and ID Number

**Category  
Description**

Employee PII continued	Other Sources of Coverage Accepting or Waiving Coverage Dependent Information, if applicable, including: <ul style="list-style-type: none"> <li>• Dependent Name</li> <li>• Dependent Date of Birth</li> <li>• Dependent Social Security Number</li> <li>• Dependent Relationship to Employee</li> <li>• Dependent Sex</li> <li>• Dependent Spoken and Written Language Preference</li> <li>• Dependent Race and Ethnicity</li> <li>• If American Indian/Alaska Native: Name and Location of Tribe</li> <li>• Dependent Tobacco Use Indicator and Last Date of Tobacco Use</li> <li>• If individual is living outside of home; name of individual, address, phone, email address</li> <li>• Dependent Other Sources of Coverage</li> <li>• Dependent Accepting or Waiving Coverage</li> <li>• Special Circumstances for Employees and Dependents, i.e., marriage, moving, adopting children, losing eligibility for coverage under a group health plan or losing Employer contribution, or giving birth</li> </ul>
Employer Offering Coverage Information	Employer Name/“Doing Business As” Employer Federal Tax ID Number Employer Address Business Type Employer Attestation to SHOP Eligibility Requirements Employer Contact Information Employer Contact Name and Title Employer Contact Mailing Address (if different than employer address) Employer Contact Phone Numbers (and type) Employer Contact Spoken and Written Language Preference Employer Contact Email Address Employer Contact Fax Number Secondary Contact Name (optional) Secondary Contact Phone number (and type) Secondary Contact Fax Number Secondary Contact Email Address Secondary Contact Authorizations Employer Coverage Offered Employer-selected AV Levels (Bronze, Silver, Gold, or Platinum) Benchmark Plan

**Category  
Description**

Employer Offering Coverage Information continued	<p>Offer of Dependent Coverage</p> <p>Agent/Broker/Assister/Navigator Name, Organization Name, Contact Information, FFM User ID</p> <p>Employer Contribution Information:</p> <ul style="list-style-type: none"> <li>• Benchmark Plan ID number-Medical Plan</li> <li>• Benchmark Plan ID number-Dental Plan</li> <li>• Percentage towards Employee-Medical Coverage</li> <li>• Percentage towards Employee Dental Coverage</li> <li>• Percentage towards Dependent Medical Coverage</li> <li>• Percentage towards Dependent Dental Coverage</li> <li>• Employer Offering-Single QHP or Single Metal Level or Single Issuer</li> <li>• Employer Offering-Single Stand-alone Dental Plan (“SADP”) or multiple SADPs</li> </ul> <p>Offer of Stand-alone Dental Coverage</p> <p>Desired Effective Date of Coverage</p> <p>Employee Selection Due Date</p> <p>Waiting Period for New Hires to Enroll</p> <p>Employee List, including:</p> <ul style="list-style-type: none"> <li>• Employee Name</li> <li>• Employee Date of Birth</li> <li>• Employee Age</li> <li>• Employee Social Security Number</li> <li>• Employee Email Address</li> <li>• Employee Employment Status</li> <li>• Employee’s Other Coverage</li> <li>• Number of Dependents</li> <li>• Dependent Information, including Dependent Name</li> <li>• Dependent Date of Birth</li> <li>• Dependent Age</li> <li>• Dependent Social Security Number</li> <li>• Dependent Email Address</li> <li>• Dependent’s Other Coverage</li> </ul> <p>Payment Method options, including:</p> <ul style="list-style-type: none"> <li>• Electronic Funds Transfer Information (Checking Account Number, Routing Number)</li> <li>• Credit Card Information (Credit Card type, Name on Credit Card, Credit Card Number, Expiration Date, Signature, Signature Date)</li> <li>• Checking Information</li> </ul> <p>Employer Attestation to Consolidated Omnibus Budget Reconciliation Act (“COBRA”)/Medicare Compliance Questions</p>
--	--

- d. Use of PII. PII collected from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—in the context of completing an application for QHP, APTC, or CSR eligibility, if applicable, or enrolling in a QHP, or any data transmitted from or through the Hub, if applicable, may be used only for Authorized Functions specified in Section II.a of this Agreement. Such Information may not be used for purposes other than authorized by this Agreement or as consented to by a Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and Qualified Employer—or these individuals’ legal representatives or Authorized Representatives.
- e. Collection and Use of Information Provided Under Other Authorities. This Agreement does not preclude Web-broker from collecting Information from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—for a non-FFE/non-SBE-FP/non-Hub purpose, and using, reusing, and disclosing the non-FFE/non-SBE-FP/non-Hub Information obtained as permitted by applicable law and/or other applicable authorities. Such Information must be stored separately from any PII collected in accordance with Section II.c of this Agreement. The Hub Web Services are not available for SHOP.
- f. Commitment to Protect PII. Web-broker shall not release, publish, or disclose Consumer, Applicant, Qualified Individual, or Enrollee PII to unauthorized personnel, and shall protect such Information in accordance with provisions of any laws and regulations governing the adequate safeguarding of Consumer, Applicant, Qualified Individual, or Enrollee PII, the misuse of which carries with it the potential to cause financial, reputational and other types of harm.
  1. Technical leads must be designated to facilitate direct contacts between the Parties to support the management and operation of the interconnection.
  2. The overall sensitivity level of data or Information that will be made available or exchanged across the interconnection will be designated as MODERATE as determined by Federal Information Processing Standards (FIPS) Publication 199.
  3. Web-broker agrees to comply with all federal laws and regulations regarding the handling of PII—regardless of where the organization is located or where the data are stored and accessed.
  4. Web-broker’s Rules of Behavior must be at least as stringent as the HHS Rules of Behavior.<sup>2</sup>
  5. Web-broker understands and agrees that all financial and legal liabilities arising from inappropriate disclosure or Breach of Consumer, Applicant, Qualified Individual, or Enrollee PII while such Information is in the possession of Web-broker shall be borne exclusively by Web-broker.
  6. Web-broker shall train and monitor staff on the requirements related to the authorized use and sharing of PII with third parties and the consequences of

---

<sup>2</sup> The HHS Rules of Behavior are available at the following link: <https://www.hhs.gov/ocio/policy/hhs-rob.html>.

unauthorized use or sharing of PII, and periodically audit their actual use and disclosure of PII.

- g. Ability of Individuals to Limit Collection and Use of PII. Web-broker agrees to provide the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee or Qualified Employer—or these individuals’ legal representatives or Authorized Representatives—the opportunity to opt in and have Web-broker collect, create, disclose, access, maintain, store and use their PII. Web-broker agrees to provide a mechanism through which the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee and Qualified Employer—or these individuals’ legal representatives or Authorized Representatives—can limit Web-broker’s creation, collection, disclosure, access, maintenance, storage, and use of their PII to the sole purpose of obtaining Web-broker’s assistance in performing Authorized Functions specified in Section II.a of this Agreement.
- h. Incident and Breach Reporting. Web-broker must implement Incident and Breach Handling procedures as required by the NEE SSP and that are consistent with CMS’s Incident and Breach Notification Procedures. Such policies and procedures must identify the Web-broker’s Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents or Breaches; provide details regarding the identification, response, recovery and follow-up of Incidents and Breaches, which should include Information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes. Web-broker agrees to report any Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at [cms\\_it\\_service\\_desk@cms.hhs.gov](mailto:cms_it_service_desk@cms.hhs.gov) within 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.

### III. Approval and Renewal Minimum Direct Enrollment (“DE”) Program Participation Requirements.

- a. Completion of Operational Readiness Review Required Under 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f).
  - 1. End-to-End Testing and Enrollment Validation Requirement. In order to be approved as a Web-broker, or to maintain status as an Existing Web-broker during Web-broker Agreement renewal, Web-broker must demonstrate a successful end-to-end DE transaction through any of the following: a history of enrollments completed via Classic DE or EDE during the term of the prior year’s Web-broker Agreement or by end-to-end testing either with the Hub or during the EDE business audit submission process within the term of the prior year’s Web-broker Agreement, as applicable.
  - 2. Operational and Oversight Information Form. In order to be approved as a Web-broker, Web-broker must submit an Operational and Oversight Information Form to CMS in the form and manner specified by CMS. In order to maintain status as an Existing Web-broker during Web-broker Agreement renewal, Web-broker must submit annually an Operational and Oversight Information Form to CMS in the form and manner specified by CMS.

3. Operational Information. When onboarding annually during Agreement renewal, and upon request, the Web-broker must provide CMS operational Information, including, but not limited to, its Designated Representative's National Producer Number (NPN), State licensure Information, and Information about its downstream Agents/Brokers, if applicable.
4. Pre-Approval Website Review. Prospective Web-brokers must receive and resolve any designated compliance findings identified by CMS during a pre-approval website review prior to receiving a countersigned Web-broker Agreement. To facilitate this review, upon request, a Prospective Web-broker must provide CMS with a set of credentials CMS can use to access the Prospective Web-broker's testing DE Environment (i.e., the pre-production environment) to complete the website review of the Prospective Web-broker's DE Environment. The Prospective Web-broker must ensure that the testing credentials are valid and that all APIs and components in the testing DE Environment are accessible for the duration of the review. This provision does not apply to Existing Web-brokers that have received a CMS website review during the term of the prior year's Web-broker Agreement.
5. Designated Representative Registration and Training with the Exchange. Web-broker's Designated Representative(s) must complete the applicable annual registration and training requirements with the Exchange. Web-broker, including Agent or Broker Direct Enrollment Technology Provider, must provide this information to CMS to connect to the DE or EDE web services in production.
6. Privacy and Security Documentation. In order to receive approval to participate in DE and utilize an approved DE Environment, Web-brokers must submit the complete set of documents outlined in Table 1 of Appendix A: Privacy and Security Standards for Web-brokers to CMS, except as noted in the "Submission Requirements" column and must comply with the privacy and security audit requirements under Section IX of this Agreement. The annual assessment results that serve as the basis for the documentation in Table 1 of Appendix B: Annual Security and Privacy Assessment (SPA) are only valid for a period of 365 Days from the completion date of the assessment. Web-brokers must complete the continuous monitoring requirements detailed in the Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide.<sup>3</sup>

The Web-broker must conduct penetration testing which examines the network, application, device, and physical security of its DE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Web-brokers must adhere to the requirements for Penetration Testing described in Section V.b and Appendix B: Annual Security and Privacy Assessment (SPA) of this Agreement.

- b. Web-broker Public List Requirements. In order to be listed on CMS's Web-broker Public List, Web-brokers must have completed the applicable onboarding or renewal processes (see Section III.a of this Agreement); have a valid, countersigned Web-broker

---

<sup>3</sup> The ISCM Strategy Guide is available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.



Agreement; and have an active, approved Secure Sockets Layer (SSL) production certificate with the Hub for the applicable plan year or an SSL production certificate pending CMS approval under Section III.a.5 of this Agreement.

#### IV. Downstream Use of Web-broker's DE Environment.

- a. Downstream Agent/Broker and DE Entity Application Assister Use of a Web-broker's DE Environment. A Web-broker that provides access to its DE Environment to downstream Agents and Brokers and DE Entity Application Assisters, consistent with 45 C.F.R. §§ 155.220(c)(4) and 155.221(c), must provide a DE Environment to its downstream Agents and Brokers and DE Entity Application Assisters that complies with this Agreement and the Web-broker requirements in 45 C.F.R. §§ 155.220 and 155.221. Web-broker must not provide the capability for downstream Agents/Brokers to use its DE Environment through the third party's own website or otherwise outside of Web-broker's approved website. The use of embedding tools and programming techniques by downstream Agents/Brokers, such as iframe technical implementations, that may enable the distortion, manipulation, or modification of the approved DE Environment and the overall DE End-User experience developed by Web-broker are prohibited.

As part of the DE or EDE-facilitated application and QHP application processes, Web-broker must not enable or allow the selection of QHPs by a consumer or Agent/Broker on a third-party website that exists outside of the Web-broker's approved DE Environment. This includes pre-populating or pre-selecting a QHP for a consumer that was selected on a downstream Agent's/Broker's website or a lead generator's website. This prohibition does not extend to websites that are provided, owned, and maintained by entities subject to CMS regulations for QHP display (i.e., Web-brokers and QHP Issuers).

The Web-broker must have a written contract or other written arrangement with the downstream Agent or Broker or DE Entity Application Assisters that governs the arrangement and requires the adherence to the terms of this Agreement.

Upon request, Web-broker must provide CMS with information about its downstream Agents/Brokers, Web-broker's oversight of its downstream Agents/Brokers, and the DE Environment(s) it provides to each of its downstream Agents/Brokers.

- b. QHP Issuer Use of a Web-broker's DE Environment. Web-broker may provide access to its DE Environment to QHP Issuers for use by the QHP Issuer and/or the QHP Issuer's downstream Agents and Brokers and DE Entity Application Assisters that is branded and specific to that QHP Issuer. In these cases, the Web-broker would be considered a downstream and delegated entity of the QHP Issuer under 45 C.F.R. § 156.340. There must be a written contract or other written arrangement between the Web-broker and the QHP Issuer that governs the arrangement and requires adherence to the terms of this Agreement. The QHP Issuer's DE Environment that is provided by the Web-broker must comply with the DE requirements applicable to QHP Issuers in 45 C.F.R. §§ 155.221 and 156.1230.

#### V. DE Environment and Website Requirements.

- a. Maintenance of an Accurate Testing DE Environment. Web-broker must maintain a testing DE Environment that accurately represents the Web-broker's production DE Environment and integration with the Classic DE pathway, including functional use of all



DE APIs. Web-brokers must maintain at least one testing DE Environment that reflects the Web-broker's current production DE Environments when developing and testing any prospective changes to its production DE Environments. This will require Web-broker to develop one or more separate testing DE Environments (other than production and the testing DE Environment that reflects production) for developing and testing prospective changes to Web-broker's production DE Environments. Network traffic into and out of all non-production environments is only permitted to facilitate system testing and must be restricted by source and destination access control lists, as well as ports and protocols, as documented in the NEE SSP, SA-11 implementation standard. Web-broker must not submit actual PII to the FFE Testing Environments. The Web-broker shall not submit test data to the FFE Production Environments. Web-broker's testing DE Environment shall be readily accessible to applicable CMS staff and contractors via the Internet to complete CMS audits.

Upon request, Web-broker must provide CMS with a set of credentials and any additional instructions necessary so that CMS can access the testing DE Environment that reflects the Web-broker's production environment to complete audits or otherwise confirm compliance of Web-broker's production DE Environments. The Web-broker must be able to provide test credentials for all DE Environments that Web-broker hosts or provides (and/or prototypes of those DE Environments), including, but not limited to, the Web-broker's Consumer-facing DE Environment, Web-broker's Agent/Broker-facing DE Environment, a Consumer-facing website that the Web-broker provides for use by Agents or Brokers, and an Agent- or Broker-facing DE Environment that the Web-broker provides for use by Agents/Brokers. Web-broker must ensure that the testing credentials are valid and that all APIs and components in the testing DE Environment, including the remote identity proofing (RIDP) services, are readily accessible via Internet for CMS to audit or otherwise confirm compliance of Web-broker's production DE Environment as determined necessary by CMS.

- b. Penetration Testing. The DE Entity must conduct penetration testing which examines the network, application, device, and physical security of its DE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Before conducting the penetration testing, the DE Entity must execute a Rules of Engagement with its Auditor's penetration testing team. The DE Entity must also notify its CMS designated technical counterparts on its annual penetration testing schedule a minimum of 5 business days prior to initiation of the penetration testing using the CMS-provided form.<sup>4</sup> During the penetration testing, the Auditor's testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment. The penetration testing shall be conducted in the lower environment that reflects the DE Entity's current production environment.
- c. Limit Concurrent Sessions. The Web-broker must limit the number of concurrent sessions to one (1) session per a single set of credentials/FFE user ID. However, multiple sessions associated with a single set of credentials/FFE user ID that is traceable to a

---

<sup>4</sup> The Penetration Testing Notification Form is available at the following links:  
<https://zone.cms.gov/document/privacy-and-security-audit>.

single device/browser is permitted.

- d. Health Reimbursement Arrangement (HRA) Messaging. If Web-broker implements full HRA functionality, Web-broker must implement required User Interface (UI) messaging for qualified individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the qualified individuals consistent with CMS guidance. Required UI messaging for various scenarios is detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.<sup>5</sup>
- e. APTC Selection and Attestation. Web-broker must allow Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—to select and attest to an APTC amount, if applicable, in accordance with 45 C.F.R. § 155.310(d)(2). Web-broker should use the specific language detailed in the FFE and FF-SHOP Enrollment Manual<sup>6</sup> when providing Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—with the ability to attest to an APTC amount.

#### VI. Effective Date and Term; Renewal.

- a. Effective Date and Term. This Agreement becomes effective on the date the last of the two Parties executes this Agreement and ends the Day before the first Day of the open enrollment period (“OEP”) under 45 C.F.R. § 155.410(e)(3) for the benefit year beginning January 1, 2025.
- b. Renewal. This Agreement may be renewed upon the mutual agreement of the Parties for subsequent and consecutive one (1) year periods upon thirty (30) Days’ advance written notice to Web-broker.

#### VII. Suspension.

- a. Suspension Pursuant to 45 C.F.R. §§ 155.220 and 155.221. The suspension of the ability of Web-broker to transact information with the Exchange shall be governed by the suspension standards adopted by the FFEs or SBE-FPs under 45 C.F.R. §§ 155.220 and 155.221.
- b. Duration of Suspension. Consistent with the standards under 45 C.F.R. §§ 155.220 and 155.221, Web-broker will remain suspended until Web-broker remedies or sufficiently mitigates the issue(s) that were the basis for the suspension to HHS’s satisfaction. If this Agreement expires prior to HHS removing the suspension, HHS will not execute a subsequent Web-broker Agreement with Web-broker until Web-broker remedies or sufficiently mitigates the issue(s) to HHS’s satisfaction.

#### VIII. Termination.

- a. Termination Without Cause. Either Party may terminate this Agreement without cause and for its convenience upon thirty (30) Days’ prior written notice to the other Party.

---

<sup>5</sup> The document Direct Enrollment API Specs is available on CMS zONE at the following link: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.

<sup>6</sup> The SHOP Enrollment Manual is available on CMS zONE at the following link: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.

Web-broker must reference and complete the NEE Decommissioning Plan and NEE Decommissioning Close Out Letter in situations where Web-broker will retire or decommission its DE Environment.<sup>7</sup>

- b. Termination of Agreement with Notice by CMS. The termination of this Agreement and the reconsideration of any such termination shall be governed by the termination and reconsideration standards adopted by the FFEs or SBE-FPs under 45 C.F.R. § 155.220. Notwithstanding the foregoing, the Web-broker shall be considered in “Habitual Default” of this Agreement in the event it has been served with a non-compliance notice under 45 C.F.R. § 155.220(g) more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately terminate this Agreement upon notice to Web-broker without any further opportunity to resolve the Breach and/or non-compliance. CMS may also temporarily suspend the ability of a Web-broker to make its website available to transact Information with HHS pursuant to 45 C.F.R. §§ 155.220(c)(4)(ii) or 155.221(d).
- c. Termination for Failure to Maintain Valid State Licensure. Web-broker acknowledges and agrees that valid State licensure in each State in which Web-broker assists Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—in applying for or obtaining coverage under a QHP through an FFE or SBE-FP is a precondition to the Web-broker’s authority under this Agreement. Accordingly, CMS may terminate this Agreement if Web-broker fails to maintain valid licensure in at least one FFE or SBE-FP State, and in each State for which Web-broker facilitates enrollment in a QHP through the FFE or an SBE-FP. Any such termination shall be governed by the standards adopted by the FFE under 45 C.F.R. § 155.220(g) and (h). If Web-broker is an Agent or Broker Direct Enrollment Technology Provider and maintains no contractual relationships with Agents or Brokers and is not owned or operated by an Agent or Broker, the entity would no longer meet the applicable definition under 45 C.F.R. § 155.20 to be an Agent or Broker Direct Enrollment Technology Provider. Web-broker understands and agrees that in such circumstances CMS may immediately terminate this Agreement for cause, or the Agent or Broker Direct Enrollment Technology Provider may provide advance notice to CMS to terminate this agreement without cause per Section VIII.a of this Agreement. If the Agent or Broker Direct Enrollment Technology Provider is unable to provide thirty (30) Days’ advance notice to CMS, the Agent or Broker Direct Enrollment Technology Provider must notify CMS within thirty (30) Days after the entity no longer meets the applicable definition under 45 C.F.R. § 155.20 to be an Agent or Broker Direct Enrollment Technology Provider.
- d. Destruction of PII. Web-broker covenants and agrees to destroy all PII in its possession at the end of the record retention period required under the NEE SSP, which is consistent with NIST SP 800-88 Rev. 1. If, upon the termination or expiration of this Agreement, Web-broker has in its possession PII for which no retention period is specified in the NEE SSP, such PII shall be destroyed within thirty (30) Days of the termination or

---

<sup>7</sup> The Non-Exchange Entity (NEE) Decommissioning Plan and NEE Decommissioning Close Out Letter are available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>

expiration of this Agreement. Web-broker's duty to protect and maintain the privacy and security of PII, as provided for in the NEE SSP, shall continue in full force and effect until such PII is destroyed and shall survive the termination or expiration of this Agreement.

- e. Termination of Registration from the FFEs. Web-broker acknowledges that the termination or expiration of this Agreement will result in the termination of the Web-broker's registration with the FFE.

**IX. Privacy and Security Audit Requirement.** In order to receive approval to participate in DE and utilize an approved DE Environment, Web-broker must contract with one or more independent Auditor(s) consistent with this Agreement's provisions and applicable regulatory requirements to conduct an annual security and privacy assessment (SPA) as described in Appendix B: Annual Security and Privacy Assessment (SPA), the ISCM Strategy Guide, and the NEE SSP.

The Auditor must document and attest in the SPA documentation that Web-broker's DE Environment, including its website and operations, complies with the terms of this Agreement, other applicable agreement(s) with CMS (including the EDE Business Agreement and Interconnection Security Agreement), the Framework for the Independent Assessment of Security and Privacy Controls, and applicable program requirements. EDE Entity must submit the resulting SPA documentation to CMS. The SPA must detail EDE Entity's compliance with the requirements set forth in Appendix B, including any requirements set forth in CMS guidance referenced in Appendix B. The SPA that Web-broker submits to CMS must demonstrate that Web-broker's Auditor(s) conducted its review in accordance with the review standards set forth in Appendix B, the ISCM Strategy Guide, and the NEE SSP.

CMS will approve Web-broker's DE Environment only once it has reviewed and approved the privacy and security audit findings reports. Final approval of Web-broker's DE Environment will be evidenced by CMS countersigning the ISA with Web-broker. Upon receipt of the counter-signed ISA, Web-broker will be approved to use its approved DE Environment consistent with applicable regulations, this Agreement, and the ISA.

- a. Identification of Auditor(s) and Subcontractors of Auditor(s). All Auditor(s), including any Auditor(s) that has subcontracted with Web-broker's Auditor(s), will be considered Downstream or Delegated Entities of Web-broker pursuant to Web-broker's respective agreement(s) with CMS and applicable program requirements. Web-broker must identify each Auditor it selects, and any subcontractor(s) of the Auditor(s), in Appendix E: Auditor Identification of this Agreement. Web-broker must also submit a copy of the signed agreement or contract between the Auditor(s) and Web-broker to CMS.
- b. Conflict of Interest. For any arrangement between Web-broker and an Auditor for audit purposes covered by this Agreement, Web-broker must select an Auditor that is free from any real or perceived conflict(s) of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. Web-broker must disclose to HHS any financial relationships between the Auditor, and individuals who own or are employed by the Auditor, and individuals who own or are employed by a Web-broker for which the Auditor is conducting an ORR privacy and security audit pursuant to 45 C.F.R. §§ 155.220(c)(6)(iv), 155.221(b)(4)(ii),

and 155.221(f). Web-broker must document and disclose any conflict(s) of interest in the form in Appendix F: Conflict of Interest Disclosure Form, if applicable.

- c. Auditor Independence and Objectivity. Web-broker's Auditor(s) must remain independent and objective throughout the audit process. An Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the DE Environment and the determination of security and privacy control effectiveness. Web-broker must not take any actions that impair the independence and objectivity of Web-broker's Auditor. Web-broker's Auditor must attest to their independence and objectivity in completing the DE audit(s).
- d. Required Documentation. Web-broker must maintain and/or submit the required documentation detailed in Appendix B: Annual Security and Privacy Assessment (SPA), including templates provided by CMS, to CMS in the manner specified in Appendix B: Annual Security and Privacy Assessment (SPA). Documentation that Web-broker must submit to CMS (as set forth in Section III and Appendices B, E, and F of this Agreement) will constitute Web-broker's Application.

#### X. Miscellaneous.

- a. Notice. All notices to Parties specifically required under this Agreement shall be given in writing and shall be delivered as follows:
  - If to CMS, by email at: [directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov)
  - If to Web-broker, to Web-broker's email address on record.

Notices sent by email shall be deemed to have been given when the appropriate confirmation of receipt has been received; notices not given on a business Day (i.e., Monday-Friday, excluding federal holidays) between 9:00 a.m. and 5:00 p.m. local time where the recipient is located shall be deemed to have been given at 9:00 a.m. on the next business Day for the recipient. A Party to this Agreement may change its contact information for notices and other communications by providing written notice of such changes in accordance with this provision. Such notice should be provided thirty (30) Days in advance of such change, unless circumstances warrant a shorter timeframe.

- b. Assignment and Subcontracting. Except as otherwise provided in this Section, Web-broker shall not assign this Agreement in whole or in part, whether by merger, acquisition, consolidation, reorganization, or otherwise any portion of the services to be provided by Web-broker under this Agreement without the express, prior written consent of CMS, which consent may be withheld, conditioned, granted, or denied in CMS' sole discretion. Web-broker must provide written notice at least thirty (30) Days prior to any such proposed assignment, including any change in ownership of Web-broker or any change in management or ownership of the DE Environment. Notwithstanding the foregoing, CMS does not require prior written consent for subcontracting arrangements that do not involve the operation, management, or control of the DE Environment. Web-broker must report all subcontracting arrangements on its annual Operational and Oversight Information form during the annual Web-broker agreement renewal process and submit revisions annually thereafter. Web-broker shall assume ultimate responsibility



for all services and functions described under this Agreement, including those that are subcontracted to other entities, and must ensure that subcontractors will perform all functions in accordance with all applicable requirements. Web-broker shall further be subject to such oversight and enforcement actions for functions or activities performed by subcontractor entities as may otherwise be provided for under applicable law and program requirements, including this Agreement with CMS. Notwithstanding any subcontracting of any responsibility under this Agreement, Web-broker shall not be released from any of its performance or compliance obligations hereunder, and shall remain fully bound to the terms and conditions of this Agreement as unaltered and unaffected by such subcontracting.

If Web-broker attempts to make an assignment, subcontracting arrangement or otherwise delegate its obligations hereunder in violation of this provision, such assignment, subcontract, or delegation shall be deemed void *ab initio* and of no force or effect, and Web-broker shall remain legally bound hereto and responsible for all obligations under this Agreement.

- c. Use of the Hub Web Services. Web-broker will only use a CMS-approved DE Environment when accessing the APIs and web services that facilitate functionality to enroll Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix A: Privacy and Security Standards for , Appendix B: Annual Security and Privacy Assessment (SPA), and Appendix D: Standards for Communication with the Hub.
- d. Survival. Web-broker’s duty to protect and maintain the privacy and security of PII and any other obligation under this Agreement which, by its express terms or nature and context is intended to survive expiration or termination of this Agreement, shall survive the expiration or termination of this Agreement.
- e. Severability. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement. In the event that any provision of this Agreement is determined to be invalid, unenforceable or otherwise illegal, such provision shall be deemed restated, in accordance with applicable law, to reflect as nearly as possible the original intention of the Parties, and the remainder of the Agreement shall be in full force and effect.
- f. Disclaimer of Joint Venture. Neither this Agreement nor the activities of Web-broker contemplated by and under this Agreement shall be deemed or construed to create in any way any partnership, joint venture or agency relationship between CMS and Web-broker. Neither Party is, nor shall either Party hold itself out to be, vested with any power or right to bind the other Party contractually or to act on behalf of the other Party, except to the extent expressly set forth in the ACA and the regulations codified thereunder, including as codified at 45 C.F.R. part 155.
- g. Remedies Cumulative. No remedy herein conferred upon or reserved to CMS under this Agreement is intended to be exclusive of any other remedy or remedies available to CMS under operative law and regulation, and each and every such remedy, to the extent

permitted by law, shall be cumulative and in addition to any other remedy now or hereafter existing at law or in equity or otherwise.

- h. Records. Web-broker shall maintain all records that it creates in the normal course of its business in connection with activity under this Agreement for the term of this Agreement in accordance with 45 C.F.R. § 155.220(c)(3)(i)(E). Subject to applicable legal requirements and reasonable policies, such records shall be made available to CMS to ensure compliance with the terms and conditions of this Agreement. The records shall be made available during regular business hours at Web-broker's offices, and CMS's review shall not interfere unreasonably with Web-broker's business activities. This clause survives the expiration or termination of this Agreement.
- i. Compliance with Law. Web-broker covenants and agrees to comply with any and all applicable laws, statutes, regulations, or ordinances of the United States of America and any Federal Government agency, board, or court that are applicable to the conduct of the activities that are the subject of this Agreement, including, but not necessarily limited to, any additional and applicable standards required by statute, and any regulations or policies implementing or interpreting such statutory provisions hereafter issued by CMS. In the event of a conflict between the terms of this Agreement and any statutory, regulatory, or sub-regulatory guidance released by CMS, the requirement that constitutes the stricter, higher, or more stringent level of compliance shall control.
- j. Governing Law and Consent to Jurisdiction. This Agreement will be governed by the laws and common law of the United States of America, including without limitation such regulations as may be promulgated by HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. Web-broker further agrees and consents to the jurisdiction of the Federal Courts located within the District of Columbia and the courts of appeal therefrom, and waives any claim of lack of jurisdiction or *forum non conveniens*.
- k. Amendment. CMS may amend this Agreement for purposes of reflecting changes in applicable law or regulations, with such amendments taking effect upon thirty (30) Days' written notice to Web-broker ("CMS notice period"), unless circumstances warrant an earlier effective date. Any amendments made under this provision will only have prospective effect and will not be applied retrospectively. Web-broker may reject such amendment by providing to CMS, during the CMS notice period, written notice of its intent to reject the amendment ("rejection notice period"). Any such rejection of an amendment made by CMS shall result in the termination of this Agreement upon expiration of the rejection notice period.
- l. Audit and Compliance Review. Web-broker agrees that CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees may conduct compliance reviews or audits, which includes the right to interview employees, contractors and business partners of Web-broker and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of Web-broker's compliance with the requirements of this Agreement upon reasonable notice to Web-broker, during Web-broker's regular business hours, and at Web-broker's regular business location. These audit and review rights include the right to audit Web-broker's compliance with and implementation of the privacy and security requirements

under this Agreement. Web-broker further agrees to allow reasonable access to the Information and facilities, including, but not limited to, Web-broker website testing environments, requested by CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees for the purpose of such a compliance review or audit. CMS may suspend or terminate this Agreement if Web-broker does not comply with such a compliance review request within seven (7) business Days. If any of Web-broker's obligations under this Agreement are delegated to other parties, Web-broker's agreement with any delegated or downstream entities must incorporate this Agreement provision. This clause survives the expiration or termination of this Agreement.

- m. Access to the FFEs and SBE-FPs. Any Web-broker; its Downstream and Delegated Entities, including downstream Agents/Brokers; and its assignees or subcontractors, including, employees, developers, agents, representatives, or contractors, cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to a Web-broker's systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through virtual private networks ("VPNs").

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]



This “Agreement Between Web-Broker and the Centers for Medicare & Medicaid Services for the Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform” has been signed and executed by:

**TO BE FILLED OUT BY WEB-BROKER**

The undersigned is an authorized official of Web-broker who is authorized to represent and bind Web-broker for purposes of this Agreement.

Ashwini Deshpande 10/20/2023  
Signature of Authorized Official of Web-broker Date

Ashwini Deshpande, CEO  
Printed Name and Title of Authorized Official of Web-broker

TrueCoverage LLC  
Web-broker Name

Sarika Balakrishnan  
Signature of Privacy Officer Attesting Compliance that Web-broker Systems Comply with Appendices A and B of this Agreement and the Non-Exchange Entity System Security and Privacy Plan

Sarika Balakrishnan, Manager  
Printed Name and Title of Privacy Officer Attesting Compliance that Web-broker Systems Comply with Appendices A and B of this Agreement and the Non-Exchange Entity System Security and Privacy Plan

2400 Louisiana Blvd NE, 04.TCL.MD\*.347.921  
Suite 100, Building 3, Web-broker Partner ID  
Albuquerque, NM 87110 **REDACTED**  
Web-broker Address Web-broker Contact Number

**Web-broker must indicate in the below checkbox whether Web-broker will assist Qualified Employees and/or Qualified Employers in applying for or enrolling in SHOP coverage for the benefit year as defined in Section VI.a of this Agreement:**

Web-broker *will* assist Qualified Employees and/or Qualified Employers in the benefit year as defined in this Agreement

Web-broker ***will not*** assist Qualified Employees and/or Qualified Employers in the benefit year as defined in this Agreement

---

**FOR CMS**

The undersigned are officials of CMS who are authorized to represent and bind CMS for purposes of this Agreement.

**Jeffrey Grant -S** Digitally signed by Jeffrey Grant -S  
Date: 2023.10.19 15:50:03 -04'00'

---

**Jeffrey D. Grant**

**Date**

Deputy Director for Operations

Center for Consumer Information and Insurance Oversight

Centers for Medicare & Medicaid Services

**George C. Hoffmann -S** Digitally signed by George C. Hoffmann -S  
Date: 2023.10.30 07:12:02 -04'00'

---

**George C. Hoffmann**

**Date**

CMS Deputy CIO

Deputy Director, Office of Information Technology (OIT)

Centers for Medicare & Medicaid Services (CMS)

### **Appendix A: Privacy and Security Standards for Web-brokers**

Federally-facilitated Exchanges (“FFE’s”) will enter into contractual agreements with all Non-Exchange Entities, including Web-brokers, that gain access to Personally Identifiable Information (“PII”) exchanged with the FFEs (including FF-SHOPs) and State-based Exchanges on the Federal Platform (“SBE-FPs”) (including SBE-FP-SHOPs), or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals’ legal representatives or Authorized Representatives. This Agreement and its appendices govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by Web-brokers in the context of the FFEs and SBE-FPs (including FF-SHOPs and SBE-FP-SHOPs). In signing this contractual Agreement, in which this Appendix A has been incorporated, Web-brokers agree to comply with the security and privacy standards and implementation specifications outlined in the Non-Exchange Entity System Security and Privacy Plan (NEE SSP)<sup>8</sup> while performing the Authorized Functions outlined in their respective Agreement(s) with CMS.

The standards documented in the NEE SSP are established in accordance with Section 1411(g) of the Affordable Care Act (“ACA”) (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 (“FISMA”) (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the principles in 45 C.F.R. §§ 155.260(a)(1) through (a)(6). All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

In addition, Web-brokers must comply with the annual security and privacy assessment (SPA) requirements in Appendix B.

---

<sup>8</sup> References to security and privacy controls and implementation standards can be found in the NEE SSP located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

### **Appendix B: Annual Security and Privacy Assessment (SPA)**

Consistent with 45 C.F.R. §§ 155.220(c)(6)(iv), 155.221(b)(4)(ii) and 155.221(f), the Web-broker must contract with one or more independent Auditors to conduct an annual SPA as described below and in the ICSM Strategy Guide and the NEE SPP. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

The SPA shall include the following:

- Documentation of existing security and privacy controls;
- Identification of potential security and privacy risks; and
- Corrective action plan describing approach and timeline to implement security and privacy controls to mitigate potential security and privacy risks.

(1) Independent Third-Party Audit. The Web-broker must contract with an independent third-party Auditor(s) with experience conducting Information system privacy and security audits to perform the SPA. The Web-broker and its Auditor(s) should refer to the Framework for Independent Assessment of Security and Privacy Controls<sup>9</sup> which provides an overview of the independent security and privacy assessment requirements.

The Web-broker and its Auditor(s) may reference existing audit results that address some or all of the SPA's requirements. Such existing audit results must have been generated by an independent third-party Auditor. In addition, such existing audit results must have been produced within 365 Days of completion of the SPA. If existing audit reports do not address all required elements of the SPA, the remaining elements must be addressed by an independent third-party Auditor.

(2) Assessment Methodology. The SPA methodology herein is based on the standard CMS methodology and is described in the Framework for Independent Assessment of Security and Privacy Controls. The Auditor must prepare and Web-broker must submit a Security Privacy Controls Assessment Test Plan (SAP) that describes the Auditor's scope and methodology of the assessment. Web-broker must submit the Auditor-prepared SAP at least thirty (30) Days prior to commencing the assessment. The assessment methods may include examination of documentation, logs, and configurations; interviews of personnel; and/or testing of technical controls. The SPA must provide an accurate depiction of the security and privacy controls in place, as well as potential security and privacy risks, by identifying the following:

- a. Application or system vulnerabilities, the associated business and system risks and potential impact;
- b. Weaknesses in the configuration management process such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system;
- c. Web-broker security and privacy policies and procedures; and
- d. Major documentation omissions and/or discrepancies.

---

<sup>9</sup> This document is located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

- (3) Tests and Analysis Performed. The SPA must include tests that analyze applications, systems, and associated infrastructure.<sup>10</sup> The tests should begin with high-level analyses and increase in specificity. Tests and analyses performed during an assessment should include:
- a. Security Control technical testing;
  - b. Penetration testing;
  - c. Adherence to privacy program policies;
  - d. Network and component vulnerability scanning;
  - e. Configuration assessment;
  - f. Documentation review;
  - g. Personnel interviews; and
  - h. Observations.
- (4) Noncompliance and Applicability. The Web-broker must develop a corrective action plan to mitigate any security and privacy risks if the SPA identifies a deficiency in the Web-broker's security and privacy controls as documented in a Plan of Action & Milestones (PO&M). Alternatively, the Web-broker may document why it believes a critical control is not applicable to its system or circumstances. The SPA results do not alter this Agreement, including any penalties for non-compliance. If the Web-broker's SPA includes findings suggesting significant security or privacy risks, and the Web-broker does not commence development and implementation of a corrective action plan to the reasonable satisfaction of CMS, a comprehensive audit may be initiated by CMS, and/or this Agreement may be terminated for cause. In addition, CMS may delay providing final approval or may withdraw prior approval of Web-broker's DE Environment if the Web-broker does not address to the reasonable satisfaction of CMS the findings suggesting significant security or privacy risks.
- (5) Non-Exchange Entity System Security Plan ("NEE SSP"). The Web-broker must implement the controls documented in the Security and Privacy Controls for Web-brokers Supplement, though, CMS strongly recommends Web-brokers participating in Classic DE implement all the NEE SSP controls.<sup>11</sup> The Web-broker's Auditor(s) must verify and document the Web-broker's implementation and compliance with at least the controls listed in the Security and Privacy Controls for Web-brokers Supplement. The Security Privacy Assessment Report (SAR) will be accepted by CMS as documentation of compliance with those controls so long as the assessment has been conducted within 365 Days of the completion date of the previous assessment.
- (6) SPA Documentation Submission. The following table identifies the required SPA documentation that Web-Brokers must submit to CMS.

**Table 1: Web-broker Privacy and Security Document Submission Requirements**

---

<sup>10</sup> The Security and Privacy Controls Assessment Test Plan (SAP) Template and the Security and Privacy Assessment Report (SAR) Template provide additional guidance on testing methodology and reporting requirements. These documents are located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

<sup>11</sup> The Security and Privacy Controls for Web-brokers Supplement will be posted at the following link on CMS zONE: <https://zone.cms.gov/document/privacy-and-security-audit>.

Document	Description	Submission Requirements
<b>Security Privacy Controls Assessment Test Plan (SAP)</b>	<ul style="list-style-type: none"> <li>▪ The SAP describes the Auditor's scope and methodology of the assessment.</li> <li>▪ The SAP includes an attestation of the Auditor's independence.</li> <li>▪ The SAP must be completed by the Auditor and submitted to CMS for review, prior to conducting the security and privacy assessment (SPA).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the Entity-specific DE/EDE PME site at least thirty (30) days before commencing the privacy and security audit; during the planning phase.</li> </ul>
<b>Security and Privacy Assessment Report (SAR)</b>	<ul style="list-style-type: none"> <li>▪ The report should contain a summary of findings that includes ALL findings from the assessment to include documentation reviews, control testing, scanning, penetration testing, interview(s), etc. <ul style="list-style-type: none"> <li>○ Explain if and how findings are consolidated.</li> <li>○ Ensure risk level determination is properly calculated, especially when weaknesses are identified as part of the Center for Internet Security (CIS) Top 20 and/or OWASP Top 10.</li> </ul> </li> <li>▪ The assessment must be conducted by an independent third-party Auditor with experience outlined in the <i>Framework for Independent Assessment</i>. Among the experience required include familiarity with National Institute of Standards and Technology (NIST) standards, the Health Insurance Portability and Accountability Act (HIPAA), and other applicable federal privacy and cybersecurity regulations and guidance.:</li> <li>▪ Alternatively, the Web-broker may reference existing audit results that address some or all of the assessment's requirements, assuming the existing audit results were produced by a third-party Auditor in conformity with the requirements described above. <ul style="list-style-type: none"> <li>○ If existing audit reports do not address all required elements of the assessment, the remaining elements must be addressed utilizing one of the first two assessment options.</li> <li>○ If existing audit reports are utilized, the reports must have been based on assessment activities completed within the last year.</li> </ul> </li> <li>▪ The SAR should not include comments that describe the third-party assessor's process for verifying the requirement, unless there is a specific issue or concern with respect to the requirement that warrants raising the concern to CMS.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the Entity-specific DE/EDE PME site using the SAR template on CMS zONE<sup>12</sup></li> <li>▪ Only one final report should be submitted to CMS. Unless CMS has provided comments and/or requested edits to the original submission and requested a revised resubmission, no additional reports should be submitted.</li> </ul>
<b>Annual Penetration Testing</b>	<ul style="list-style-type: none"> <li>▪ The penetration test must include the DE Environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the Entity-specific DE/EDE PME site with the SAR</li> </ul>
<b>Network and Component Vulnerability Scans</b>	<ul style="list-style-type: none"> <li>▪ A Web-broker must submit the most recent three (3) months of its Vulnerability Scan Reports.</li> <li>▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&amp;M (the POA&amp;M is expected to be updated monthly, if applicable, but only submitted as indicated in the following row unless additional submissions are requested by CMS).</li> <li>▪ Similar findings can be consolidated.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via web-broker's entity-specific DE/EDE PME site with the SAR</li> </ul>
<b>Plan of Action and Milestones (POA&amp;M)</b>	<ul style="list-style-type: none"> <li>▪ Submit a POA&amp;M if its third-party assessor identifies any privacy and security compliance issues in the SAR.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the web-broker's entity-specific DE/EDE PME site using</li> </ul>

<sup>12</sup> Documents, templates, and other materials will be posted at the following link on CMS zONE:  
<https://zone.cms.gov/document/privacy-and-security-audit>.

Document	Description	Submission Requirements
	<ul style="list-style-type: none"> <li>▪ Ensure all open findings from the SAR have been incorporated into the POA&amp;M.</li> <li>▪ Explain if and how findings from the SAR were consolidated on the POA&amp;M; include SAR reference numbers, if applicable.</li> <li>▪ Ensure the weakness source references each source in detail to include type of audit/assessment and applicable date range.</li> <li>▪ Ensure the weakness description is as detailed as possible to include location/server/etc., if applicable.</li> <li>▪ Ensure scheduled completion dates, milestones with dates, and appropriate risk levels are included.</li> </ul>	the POA&M template on CMS zONE with the SAR
<b>Non-Exchange Entity System Security and Privacy Plan (NEE SSP) – if requested</b>	<ul style="list-style-type: none"> <li>▪ The NEE SSP must include complete and detailed Information about the Prospective or Existing Web-broker's implementation specifications of required security and privacy controls.</li> <li>▪ The implementation of security and privacy controls must be completely documented in the SSP before the audit is initiated.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Web-brokers are not required to submit the NEE SSP to CMS. However, CMS may request and review the NEE SSP.</li> <li>▪ If requested to submit, Web-brokers must use the NEE SSP template on CMS zONE.</li> </ul>
<b>Risk Acceptance Form</b>	<ul style="list-style-type: none"> <li>▪ Ensure accepted risks are documented using the Risk Acceptance Form and submitted with the POA&amp;M during the regular POA&amp;M submission schedule<sup>13</sup>.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the web-broker's entity-specific DE/EDE PME site using the Risk Acceptance Form on CMS zONE with the POA&amp;M.</li> </ul>

- (7) Submission of SPA to CMS. The Web-broker must submit the SPA electronically in a format specified by CMS during the Agreement renewal or initial onboarding process, but no later than June 30, for Existing and Prospective Web-brokers, to mitigate risk of any delay in completing the onboarding process and/or participation in the open enrollment period (OEP) as defined in Section VI.a of this Agreement. Web-brokers must submit applicable SPA documentation in accordance with the ISCM Strategy Guide throughout the term of the Agreement.
- (8) CMS Review of Web-broker SPA Submission. CMS will review the Web-broker's SPA submission. If the SPA indicates that the Web-broker has not sufficiently implemented any identified required control(s), CMS will require remedial action. A Web-broker that does not submit the required SPA documentation or implement any required remedial actions may be subject to the Termination with Cause provision (Section VIII.b) of this Agreement or prohibited from executing the subsequent plan year's Agreement. In addition, CMS may delay providing final approval or may withdraw prior approval of Web-broker's DE Environment if the Web-broker does not address to the reasonable satisfaction of CMS findings suggesting significant security or privacy risks.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

<sup>13</sup> The *Risk Acceptance Form* is available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.



### Appendix C: Definitions

This Appendix defines terms that are used in the Agreement and other Appendices. Any capitalized term used in the Agreement or Appendices that is not defined therein or in this Appendix has the meaning provided in 45 C.F.R. § 155.20.

- (1) **Advance Payments of the Premium Tax Credit (“APTC”)** has the meaning set forth in 45 C.F.R. § 155.20.
- (2) **Affordable Care Act (“ACA”)** means the Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), which are referred to collectively as the Affordable Care Act or ACA.
- (3) **Agent or Broker** has the meaning set forth in 45 C.F.R. § 155.20.
- (4) **Agent or Broker Direct Enrollment Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.
- (5) **Applicant** has the meaning set forth in 45 C.F.R. § 155.20.
- (6) **Auditor** means a person or organization that meets the requirements set forth in this Agreement and contracts with a Direct Enrollment (DE) Entity for the purposes of conducting an Operational Readiness Review (ORR) in accordance with 45 C.F.R. §§ 155.220(c)(6) and 155.221(b)(4) and (f), this Agreement and CMS-issued guidance.
- (7) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in the Agreement that incorporates this Appendix C: Definitions.
- (8) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 C.F.R. § 155.227.
- (9) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information (“PII”) or (2) an authorized user accesses or potentially accesses PII for anything other than an authorized purpose.
- (10) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (“CMS”).
- (11) **Certified Application Counselor** means an organization, staff person, or volunteer meeting the requirements set forth in 45 C.F.R. § 155.225.
- (12) **Classic Direct Enrollment (“Classic DE”)** means, for the purposes of this Agreement, the original version of Direct Enrollment, which utilizes a double redirect from a Direct Enrollment (DE) Entity’s website to HealthCare.gov where the eligibility application is submitted and an eligibility determination is received, and back to the DE Entity’s website for Qualified Health Plan (“QHP”) shopping and plan selection consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(i), 155.221, 156.265 and/or 156.1230(b).

- (13) **Classic Direct Enrollment Pathway (“Classic DE Pathway”)** means, for the purposes of this Agreement, the application and enrollment process used by Direct Enrollment (DE) Entities for Classic DE.
- (14) **CMS** means the Centers for Medicare & Medicaid Services.
- (15) **CMS Companion Guides** means a CMS-authored guide, available on the CMS website, which is meant to be used in conjunction with and supplement relevant implementation guides published by the Accredited Standards Committee.
- (16) **CMS Data Services Hub (“Hub”)** is the CMS federally-managed service to interface data among connecting entities, including HHS, certain other federal agencies, and State Medicaid agencies. The Hub is not available for the Small Business Health Options Program (SHOP).
- (17) **CMS Data Services Hub Web Services (“Hub Web Services”)** means business and technical services made available by CMS to enable the determination of certain eligibility and enrollment or federal financial payment data through the Federally-facilitated Exchange (“FFE”) website, including the collection of personal and financial information necessary for Consumer, Applicant, Qualified Individual, or Enrollee account creations; Qualified Health Plan (“QHP”) application submissions; and Insurance Affordability Program eligibility determinations. The Hub Web Services are not available for the Small Business Health Options Program (SHOP).
- (18) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (“QHP”) offered through an Exchange or Insurance Affordability Program, or whom an Agent, Broker, or Web-broker registered with the FFE, Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a QHP, applying for APTC and CSRs, and/or completing enrollment in a QHP through the FFEs or State-based Exchanges on the Federal Platform (“SBE-FPs”) for individual market coverage.
- (19) **Cost-sharing Reductions (“CSRs”)** has the meaning set forth in 45 C.F.R. § 155.20.
- (20) **Customer Service** means assistance regarding eligibility and Health Insurance Coverage provided to a Consumer, Applicant, or Qualified Individual, including, but not limited to, responding to questions and complaints; providing information about eligibility; applying for APTC and CSRs, and Health Insurance Coverage; and explaining enrollment processes in connection with the FFEs. Includes assistance provided to Qualified Employers and Qualified Employees regarding FF-SHOP and SBE-FP SHOP coverage.
- (21) **Day or Days** means calendar days unless otherwise expressly indicated in the relevant provision of the Agreement that incorporates this Appendix C: Definitions.
- (22) **Designated Representative** means an Agent or Broker that has the legal authority to act on behalf of the Web-broker.
- (23) **Direct Enrollment (“DE”)** means, for the purposes of this Agreement, the process by which a Direct Enrollment (DE) Entity may assist an Applicant or Enrollee with enrolling in a QHP in a manner that is considered through the Exchange consistent with applicable requirements in 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or

156.1230. Direct Enrollment is the collective term used when referring to both Classic Direct Enrollment and Enhanced Direct Enrollment.

- (24) **Direct Enrollment (“DE”) End-User Experience** means all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions under this Agreement.
- (25) **Direct Enrollment (“DE”) Entity** has the meaning set forth in 45 C.F.R. § 155.20.
- (26) **Direct Enrollment (DE) Entity Application Assisters** has the meaning set forth in 45 C.F.R. § 155.20.
- (27) **Direct Enrollment (“DE”) Environment** means an Information technology application or platform provided, owned, and maintained by a DE Entity through which a DE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee Information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.
- (28) **Enhanced Direct Enrollment (“EDE”)** means, for purposes of this Agreement, the version of Direct Enrollment which allows Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—to complete all steps in the application, eligibility and enrollment processes on an EDE Entity’s website consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(ii), 155.221, 156.265 and/or 156.1230(b) using application programming interfaces (APIs) as provided, owned, and maintained by CMS to transfer data between the Exchange and the EDE Entity’s website.
- (29) **Enhanced Direct Enrollment (“EDE”) Entity** means a DE Entity that has been approved by CMS to use the Enhanced Direct Enrollment (EDE) Pathway.
- (30) **Enhanced Direct Enrollment (“EDE”) Pathway** means the APIs and functionality comprising the systems that enable EDE as provided, owned, and maintained by CMS.
- (31) **Enrollee** has the meaning set forth in 45 C.F.R. § 155.20.
- (32) **Exchange** has the meaning set forth in 45 C.F.R. § 155.20.
- (33) **Existing Web-broker** means a Web-broker that completes the Web-broker Agreement renewal process in order to maintain its status as a Web-broker and continue operating for the plan year that occurs within the term of this Agreement.
- (34) **Federally-facilitated Exchange (“FFE”)** means an **Exchange** (or **Marketplace**) established by the Department of Health and Human Services (HHS) and operated by CMS under Section 1321(c)(1) of the ACA for individual or small group market coverage, including the Federally-facilitated Small Business Health Options Program (**FF-SHOP**). **Federally-facilitated Marketplaces (FFMs)** has the same meaning as FFEs.

- (35) **Health Insurance Coverage** has the meaning set forth in 45 C.F.R. § 155.20.
- (36) **Health Insurance Exchanges Program (“HIX”)** means the System of Records that CMS uses in the administration of the FFE. As a System of Records, the use and disclosure of the SORN Records maintained by the HIX must comply with the Privacy Act of 1974, the implementing regulations at 45 C.F.R. Part 5b, and the “routine uses” that were established for the HIX in the Federal Register at 78 FR 8538 (February 6, 2013), and amended by 78 FR 32256 (May 29, 2013) and 78 FR 63211 (October 23, 2013).
- (37) **HHS** means the United States Department of Health & Human Services.
- (38) **Health Insurance Portability and Accountability Act (“HIPAA”)** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and its implementing regulations.
- (39) **Incident** or **Security Incident**, has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and means an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of Information or an Information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- (40) **Information** means any communication or representation of knowledge, such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
- (41) **Insurance Affordability Program** means a program that is one of the following:
  - (1) A State Medicaid program under title XIX of the Social Security Act.
  - (2) A State Children’s Health Insurance Program (“CHIP”) under title XXI of the Social Security Act.
  - (3) A State basic health program established under section 1331 of the Patient Protection and Affordable Care Act.
  - (4) A program that makes coverage in a Qualified Health Plan (“QHP”) through the Exchange with APTC established under section 36B of the Internal Revenue Code available to Qualified Individuals.
  - (5) A program that makes available coverage in a QHP through the Exchange with CSRs established under section 1402 of the ACA.
- (42) **Issuer** has the meaning set forth in 45 C.F.R. § 144.103.
- (43) **Non-Exchange Entity** has the meaning at 45 C.F.R. § 155.260(b)(1), and includes, but is not limited, to Qualified Health Plan (“QHP”) Issuers, Navigators, Agents, Brokers, and Web-brokers.
- (44) **OMB** means the Office of Management and Budget.
- (45) **Personally Identifiable Information (“PII”)** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other Information that is linked or linkable to a specific individual.

- (46) **Prospective Web-broker** is an entity seeking to become a Web-broker that does not have an executed Web-broker Agreement for the current plan year.
- (47) **Qualified Employer** has the meaning set forth in 45 C.F.R. § 155.20.
- (48) **Qualified Employee** has the meaning set forth in 45 C.F.R. § 155.20
- (49) **Qualified Health Plan (“QHP”)** has the meaning set forth in 45 C.F.R. § 155.20.
- (50) **Qualified Health Plan (“QHP”) Issuer** has the meaning set forth in 45 C.F.R. § 155.20.
- (51) **Qualified Individual** has the meaning set forth in 45 C.F.R. § 155.20.
- (52) **Security Control** means a safeguard or countermeasure prescribed for an Information system or an organization designed to protect the confidentiality, integrity, and availability of its Information and to meet a set of defined security requirements.
- (53) **State** means the State that has licensed the Agent, Broker, Web-broker, or Issuer that is a party to this Agreement and in which the Agent, Broker, Web-broker or Issuer is operating.
- (54) **State-based Exchange (“SBE”)** means an Exchange established by a State that receives approval to operate under 45 C.F.R. § 155.105. **State-based Marketplace (“SBM”)** has the same meaning as SBE.
- (55) **State-based Exchange on the Federal Platform (“SBE-FP”)** means an Exchange established by a State that receives approval under 45 C.F.R. § 155.106(c) to utilize the federal platform to support select eligibility and enrollment functions. **State-based Marketplace on the Federal Platform (“SBM-FP”)** has the same meaning as SBE-FP.
- (56) **System of Records** means a group of Records under the control of any federal agency from which Information is retrieved by name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
- (57) **System of Records Notice (“SORN”)** means a notice published in the Federal Register notifying the public of a System of Records maintained by a federal agency. The notice describes privacy considerations that have been addressed in implementing the system.
- (58) **System of Record Notice (“SORN”) Record** means any item, collection, or grouping of Information about an individual that is maintained by an agency, including, but not limited to, that individual’s education, financial transactions, medical history, and criminal or employment history and that contains that individual’s name, or an identifying number, symbol, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph, that is part of a System of Records.
- (59) **Web-broker** has the meaning set forth in 45 C.F.R. § 155.20.

### **Appendix D: Standards for Communication with the Hub**

The CMS Data Services Hub (“Hub”) and Hub Web Services are not available for the Small Business Health Options Program (SHOP). Therefore, this Appendix is not applicable to Web-broker participation in SHOP. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

- (1) Web-broker must possess a unique Partner ID assigned by the Centers for Medicare & Medicare Services (“CMS”). Web-broker must use its unique Partner ID when interacting with the Hub and the Direct Enrollment (“DE”) Application Program Interfaces (“APIs”) for Web-broker’s own line of business.
- (2) If Web-broker provides a DE Environment to an Issuer for the exclusive use of enrollment in that Issuer’s plans, the Web-broker must ensure that each Issuer maintains its own, unique Partner ID with the Hub.
- (3) Web-broker must complete testing for each Hub-related transaction it will implement, and it shall not be allowed to exchange data with CMS in production mode until testing is satisfactorily passed, as determined by CMS in its sole discretion. Successful testing generally means the ability to pass all applicable Health Insurance Portability and Accountability Act (“HIPAA”) of 1996 compliance standards, or other CMS-approved standards, and to process electronic data and Information transmitted by Web-broker to the Hub. The capability to submit these test transactions will be maintained by Web-broker throughout the term of this Agreement.
- (4) Transactions must be formatted in accordance with the Accredited Standards Committee Implementation Guides adopted under HIPAA, available at <http://store.x12.org/store/>, as applicable and appropriate for the type of transaction. CMS will make available Companion Guides for the transactions, which specify necessary situational data elements.
- (5) Web-broker agrees to abide by the applicable policies affecting electronic data interchange submissions and submitters as published in any of the guidance documents related to the CMS Federally-facilitated Exchange (“FFE”) or Hub, as well as applicable standards in the appropriate CMS Manual(s) or CMS Companion Guide(s), as published on the CMS website. These materials can be found at <https://www.cms.gov/ccii/resources/regulations-and-guidance/downloads/companion-guide-for-ffe-enrollment-transaction-v15.pdf> and <http://www.cms.gov/ccii/resources/regulations-and-guidance/index.html>.
- (6) Web-broker agrees to submit test transactions to the Hub prior to the submission of any transactions to the FFE production system and to determine that the transactions and responses comply with all requirements and specifications approved by the CMS and/or the CMS contractor.<sup>14</sup>

---

<sup>14</sup> While CMS owns data in the FFE, contractors operate the FFE system in which the enrollment and financial management data flow. Contractors provide the pipeline network for the transmission of electronic data, including



- (7) Web-broker agrees that prior to the submission of any additional transaction types to the FFE production system, or as a result of making changes to an existing transaction type or system, it will submit test transactions to the Hub in accordance with paragraph (2) above.
- (8) If Web-broker enters into relationships with other affiliated entities, or their authorized designees for submitting and receiving FFE data, it must execute contracts with such entities stipulating that such entities and any of its subcontractors or affiliates must utilize software tested and approved by Web-broker as being in the proper format and compatible with the FFE system. Entities that enter into contract with Web-broker and access Personally Identifiable Information (“PII”) are required to maintain the same or more stringent security and privacy controls as Web-broker.
- (9) Pursuant to 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f), Web-broker must successfully complete an Operational Readiness Review (“ORR”) to the satisfaction of CMS before Web-broker is able to submit any transactions to the FFE production system or agrees that CMS may require further reviews or corrective actions at any time during the term of this Agreement. The ORR will assess Web-broker’s compliance with CMS’ regulatory and contractual requirements, to include the critical Privacy and Security Controls. This Agreement may be terminated or access to CMS systems may be denied for a failure to comply with ORR requirements or if, at the sole discretion of CMS, the results are unsatisfactory.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

---

the transport of Exchange data to and from the Hub and Web-broker so that Web-broker may discern the activity related to enrollment functions of persons they serve. Web-broker may also use the transported data to receive descriptions of financial transactions from CMS.

**Appendix E: Auditor Identification**

Web-broker agrees to identify, in Part I below, all Auditors selected to complete the annual security and privacy assessment (SPA) and any subcontractors of the Auditor(s), if applicable. In the case of multiple Auditors, please indicate the role of each Auditor in completing the SPA. Include additional sheets, if necessary. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

**TO BE FILLED OUT BY WEB-BROKER**

**I. Complete These Rows to Identify Auditors Selected to Complete SPA**

Printed Name and Title of Authorized Official of Auditor 1	Shibani Gupta
Auditor 1 Business Name	Absurance
Auditor 1 Address	5300 Ranch Point, Katy, TX 77494
Printed Name and Title of Contact of Auditor 1 (if different from Authorized Official)	
Auditor 1 Contact Phone Number	REDACTED
Auditor 1 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	Auditor - Business and Privacy & Security Audits
Printed Name and Title of Authorized Official of Auditor 2	
Auditor 2 Business Name	
Auditor 2 Address	
Printed Name and Title of Contact of Auditor 2 (if different from Authorized Official)	
Auditor 2 Contact Phone Number	
Auditor 2 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	



**Appendix F: Conflict of Interest Disclosure Form**

**TO BE FILLED OUT BY WEB-BROKER**

Web-broker must disclose to the Department of Health & Human Services (HHS) any financial relationships between the Auditor(s) identified in Appendix E: Auditor Identification of this Agreement, and individuals who own or are employed by the Auditor(s), and individuals who own or are employed by a Web-broker for which the Auditor(s) is conducting an annual security and privacy assessment (SPA) pursuant to Appendix A: Privacy and Security Standards for Web-brokers of this Agreement and 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f). Web-broker must disclose any affiliation that may give rise to any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

Please describe below any relationships, transactions, positions (volunteer or otherwise), or circumstances that you believe could contribute to a conflict of interest:

- Web-broker has no conflict of interest to report for the Auditor(s) identified in Appendix E: Auditor Identification.
- Web-broker has the following conflict of interest to report for the Auditor(s) identified in Appendix E: Auditor Identification:

1. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
2. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
3. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# **Exhibit H**

**AGREEMENT BETWEEN WEB-BROKER AND  
THE CENTERS FOR MEDICARE & MEDICAID SERVICES  
FOR THE FEDERALLY-FACILITATED EXCHANGES  
AND STATE-BASED EXCHANGES ON THE FEDERAL PLATFORM**

---

**THIS WEB-BROKER AGREEMENT** (“Agreement”) is entered into by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES (“CMS”), as the Party (as defined below) responsible for the management and oversight of the Federally-facilitated Exchanges (“FFE’s”), also referred to as “Federally-facilitated Marketplaces” or “FFMs” and the operation of the federal eligibility and enrollment platform, which includes the CMS Data Services Hub (“Hub”), relied upon by certain State-based Exchanges (“SBE’s”) for their eligibility and enrollment functions (including State-based Exchanges on the Federal Platform [“SBE-FPs”]), and Benefitalign LLC

(hereinafter referred to as Web-broker), a Web-broker that uses a non-FFE Internet website in accordance with 45 C.F.R. §§ 155.220(c) and 155.221 to assist Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees in applying for eligibility for enrollment in Qualified Health Plans (“QHPs”) and for Advance Payments of the Premium Tax Credits (“APTCs”) and Cost-sharing Reductions (“CSRs”) for QHPs, and/or in completing enrollment in QHPs offered in the individual market through the FFEs or SBE-FPs, in applying for a determination of eligibility to participate in the FF-Small Business Health Options Program (“FF-SHOPs”) or SBE-FP SHOPS and/or in completing enrollment in QHPs offered through the FF-SHOPs or SBE-FP SHOPS; and providing related Customer Service. CMS and Web-broker are hereinafter referred to as the “Party” or, collectively, as the “Parties.” Unless otherwise noted, the provisions of this Agreement are applicable to Web-brokers seeking to assist Qualified Employers and Qualified Employees in purchasing and enrolling in coverage through an FF-SHOP or SBE-FP SHOP.

**WHEREAS:**

1. Section 1312(e) of the Affordable Care Act (“ACA”) provides that the Secretary of the U.S. Department of Health & Human Services (“HHS”) shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals, Qualified Employers, and Qualified Employees in QHPs through an Exchange, and to assist individuals in applying for APTC and CSRs, to the extent allowed by States. To participate in the FFEs or SBE-FPs, including an FF-SHOP or SBE-FP SHOP, Agents, Brokers, and Web-brokers must complete all necessary registration and training requirements under 45 C.F.R. § 155.220.
2. To facilitate the eligibility determination and enrollment processes, CMS will provide centralized and standardized business and technical services (“Hub Web Services”) through application programming interfaces (“APIs”) to Web-broker that will enable Web-broker to establish a secure connection with the Hub. The APIs will enable the secure transmission of key eligibility and enrollment Information between CMS and Web-broker. The Hub Web Services are not available for SHOP.
3. To facilitate the operation of the FFEs and SBE-FPs, CMS desires to: (a) disclose Personally Identifiable Information (“PII”), which is held in the Health Insurance Exchanges Program (“HIX”), to Web-broker; (b) provide Web-broker with access to the Hub Web Services, if applicable; and (c) permit Web-broker to create, collect, disclose,

access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—to the extent that these activities are necessary to carry out the functions that the ACA and implementing regulations permit Web-broker to carry out. The Hub Web Services are not available for SHOP.

4. Web-broker is an individual or entity licensed as an insurance producer, Agent, or Broker by the applicable State regulatory authority in at least one FFE or SBE-FP State; OR Web-broker is an Agent or Broker Direct Enrollment Technology Provider.
5. Web-broker desires to gain access to the Hub Web Services, and to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—to perform the Authorized Functions described in Section II.a of this Agreement. The Hub Web Services are not available for SHOP.
6. 45 C.F.R. § 155.260(b) provides that an Exchange must, among other things, require as a condition of contract or agreement with Non-Exchange Entities that the Non-Exchange Entity comply with privacy and security standards that are consistent with the standards in 45 C.F.R. §§ 155.260(a)(1) through (a)(6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 C.F.R. § 155.260(a)(3).
7. CMS has adopted privacy and security standards with which the Web-broker, a type of Non-Exchange Entity, must comply, which are set forth in Appendix A: Privacy and Security Standards for , Appendix B: Annual Security and Privacy Assessment (SPA), and the Non-Exchange Entity System Security and Privacy Plan (NEE SSP).<sup>1</sup>

Now, therefore, in consideration of the promises and covenants herein contained, the adequacy of which the Parties acknowledge, the Parties agree as follows:

I. Definitions.

Capitalized terms not otherwise specifically defined herein shall have the meaning set forth in the Appendix C: Definitions. Any capitalized term that is not defined herein or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

II. Acceptance of Standard Rules of Conduct.

Web-broker and CMS are entering into this Agreement to satisfy the requirements under 45 C.F.R. § 155.260(b)(2). Web-broker hereby acknowledges and agrees to accept and abide by the standard rules of conduct set forth below and in the Appendices, which are incorporated by reference in this Agreement, while and as engaging in any activity as Web-broker for purposes of the ACA. Web-broker shall strictly adhere to the privacy and security standards—and ensure that its employees, officers, directors, contractors, subcontractors, agents, and

---

<sup>1</sup> The references in this Agreement to security and privacy controls and implementation standards can be found in the NEE SSP located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

representatives strictly adhere to the same—to gain and maintain access to the Hub Web Services, if applicable, and to create, collect, disclose, access, maintain, store, and use PII for the efficient operation of the FFEs and SBE-FPs.

- a. Authorized Functions. Web-broker may create, collect, disclose, access, maintain, store, and use PII for:
  1. Assisting with application, eligibility, and enrollment processes for QHP offered through the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs;
  2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons;
  3. Assisting with completing applications for the receipt of APTC or CSRs and with selecting an APTC amount, if applicable;
  4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR determination, if applicable;
  5. Assisting with the application for and determination of certificates of exemption, if applicable;
  6. Assisting with filing appeals of eligibility determinations in connection with the FFEs and SBE-FPs, including Qualified Employer appeals for FF-SHOPs and SBE-FP-SHOPs;
  7. Transmitting Information about the Consumer's, Applicant's, Qualified Individual's, or Enrollee's decisions regarding QHP enrollment and/or CSR and APTC Information to the FFEs and SBE-FPs, if applicable;
  8. Facilitating payment of the initial premium amount to the appropriate individual market QHP, if applicable;
  9. Facilitating payment of the initial and group premium amount for FF-SHOP and SBE-FP SHOP coverage, if applicable;
  10. Facilitating an Enrollee's ability to disenroll from a QHP;
  11. Educating Consumers, Applicants, or Enrollees on Insurance Affordability Programs and, if applicable, informing such individuals of eligibility for Medicaid or the Children's Health Insurance Program ("CHIP");
  12. Assisting Enrollees to report changes in eligibility status to the FFEs and SBE-FPs throughout the coverage year, including changes that may affect eligibility (e.g., adding a dependent);
  13. Handling FF-SHOP or SBE-FP SHOP coverage changes throughout the plan year that may impact eligibility, including, but not limited to, adding a new hire, removing an Employee no longer employed at the company, removing an Employee no longer employed full-time, and adding a newborn or spouse during a special enrollment period, if applicable;
  14. Correcting errors in the application for QHP enrollment;

15. Informing or reminding Enrollees when QHP coverage should be renewed, when Enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform Enrollees of QHP coverage options at renewal;
  16. Providing appropriate Information, materials, and programs to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees—or these individuals' legal representatives or Authorized Representatives—to inform and educate them about the use and management of their health Information, as well as medical services and benefit options offered through the selected QHP or among the available QHP options;
  17. Contacting Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers and Qualified Employees—or these individuals' legal representatives or Authorized Representatives—to assess their satisfaction or resolve complaints with services provided by Web-broker in connection with the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs, the Web-broker, or QHPs;
  18. Providing assistance in communicating with QHP Issuers;
  19. Providing Customer Service activities related to FF-SHOP or SBE-FP SHOP coverage if permitted under State and federal law, including correction of errors on FF-SHOP or SBE-FP SHOP applications and policies, handling complaints and appeals regarding FF-SHOP or SBE-FP SHOP coverage, responding to questions about FF-SHOP or SBE-FP insurance policies, assisting with communicating with State regulatory authorities regarding FF-SHOP or SBE-FP SHOP issues, and assistance in communicating with CMS;
  20. Fulfilling the legal responsibilities related to the efficient functions of QHP Issuers in the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs, as permitted or required by Web-broker's contractual relationships with QHP Issuers; and
  21. Performing other functions substantially similar to those enumerated above and such other functions that CMS may approve in writing from time to time.
- b. Standards for Handling PII. Web-broker agrees that it will create, collect, disclose, access, maintain, use, or store PII that it receives directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, Qualified Employees—or these individuals' legal representatives or Authorized Representatives—and from Hub Web Services, if applicable, only in accordance with all laws as applicable, including section 1411(g) of the ACA. The Hub Web Services are not available for SHOP.
1. Security and Privacy Controls. Web-broker agrees to monitor, periodically assess, and update its security and privacy controls documented in the NEE SSP and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including Appendix A: Privacy and Security Standards for , Appendix B: Annual Security and Privacy Assessment (SPA), NEE Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide, and the NEE SSP. Furthermore, Web-broker agrees to timely inform the Exchange of any material change in its administrative, technical, or operational environments, or any material change that would require an alteration of the privacy and security standards within this Agreement.

2. Downstream and Delegated Entities. Web-broker will satisfy the requirement in 45 C.F.R. § 155.260(b)(2)(v) to bind downstream and delegated entities to the same privacy and security standards that apply to Non-Exchange Entities by entering into written agreements with any downstream and delegated entities that will have access to PII as defined in this Agreement. Web-broker must require in writing all downstream and delegated entities adhere to the terms of this Agreement.
- c. Collection of PII. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, Web-broker may create, collect, disclose, access, maintain, store, and use the following data and PII from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees—or these individuals’ legal representatives or Authorized Representatives—including, but not limited to:
    1. For individual market QHP coverage:
      - APTC percentage and amount applied
      - Auto disenrollment Information
      - Applicant name
      - Applicant address
      - Applicant birthdate
      - Applicant telephone number
      - Applicant email
      - Applicant Social Security Number
      - Applicant spoken and written language preference
      - Applicant Medicaid Eligibility indicator, start and end dates
      - Applicant CHIP eligibility indicator, start and end dates
      - Applicant QHP eligibility indicator, start and end dates
      - Applicant APTC percentage and amount applied eligibility indicator, start and end dates
      - Applicant household income
      - Applicant maximum APTC amount
      - Applicant CSR eligibility indicator, start and end dates
      - Applicant CSR level
      - Applicant QHP eligibility status change
      - Applicant APTC eligibility status change
      - Applicant CSR eligibility status change
      - Applicant Initial or Annual Open Enrollment Indicator, start and end dates
      - Applicant Special Enrollment Period eligibility indicator and reason code
      - Contact name
      - Contact address
      - Contact birthdate
      - Contact telephone number
      - Contact email
      - Contact spoken and written language preference
      - Enrollment group history (past six months)
      - Enrollment type period
      - FFE Applicant ID

- FFE Member ID
- Issuer Member ID
- Net premium amount
- Premium amount, start and end dates
- Credit or Debit Card Number, name on card
- Checking account and routing number
- Special Enrollment Period reason
- Subscriber indicator and relationship to subscriber
- Tobacco use indicator and last date of tobacco use
- Custodial parent
- Health coverage
- American Indian/Alaska Native status and name of tribe
- Marital status
- Race/ethnicity
- Requesting financial assistance
- Responsible person
- Dependent name
- Applicant/dependent sex
- Student status
- Subscriber indicator and relationship to subscriber
- Total individual responsibility amount

2. For SHOP QHP coverage:

**Category**  
**Description**

Employee PII  
 Employee Applicant Name  
 Employee Unique Employer Code  
 Employee Home Address  
 Employee Applicant Mailing Address  
 Employee Applicant Birthdate  
 Employee Social Security Number  
 Employee Applicant Telephone Number (and type)  
 Employee Applicant Email Address  
 Employee Applicant Spoken and Written Language Preference  
 Employee Tobacco Use Indicator and Last Date of Tobacco Use  
 Employee Sex  
 Employee Race and Ethnicity  
 Employer Business Name  
 If American Indian/Alaska Native: Name and Location of Tribe  
 Health Coverage Type (Individual or Family, if offered)  
 Health Plan Name and ID Number  
 Dental Plan Name and ID Number



**Category  
Description**

Employee PII continued	<p>Other Sources of Coverage</p> <p>Accepting or Waiving Coverage</p> <p>Dependent Information, if applicable, including:</p> <ul style="list-style-type: none"> <li>• Dependent Name</li> <li>• Dependent Date of Birth</li> <li>• Dependent Social Security Number</li> <li>• Dependent Relationship to Employee</li> <li>• Dependent Sex</li> <li>• Dependent Spoken and Written Language Preference</li> <li>• Dependent Race and Ethnicity</li> <li>• If American Indian/Alaska Native: Name and Location of Tribe</li> <li>• Dependent Tobacco Use Indicator and Last Date of Tobacco Use</li> <li>• If individual is living outside of home; name of individual, address, phone, email address</li> <li>• Dependent Other Sources of Coverage</li> <li>• Dependent Accepting or Waiving Coverage</li> <li>• Special Circumstances for Employees and Dependents, i.e., marriage, moving, adopting children, losing eligibility for coverage under a group health plan or losing Employer contribution, or giving birth</li> </ul>
Employer Offering Coverage Information	<p>Employer Name/“Doing Business As”</p> <p>Employer Federal Tax ID Number</p> <p>Employer Address</p> <p>Business Type</p> <p>Employer Attestation to SHOP Eligibility Requirements</p> <p>Employer Contact Information</p> <p>Employer Contact Name and Title</p> <p>Employer Contact Mailing Address (if different than employer address)</p> <p>Employer Contact Phone Numbers (and type)</p> <p>Employer Contact Spoken and Written Language Preference</p> <p>Employer Contact Email Address</p> <p>Employer Contact Fax Number</p> <p>Secondary Contact Name (optional)</p> <p>Secondary Contact Phone number (and type)</p> <p>Secondary Contact Fax Number</p> <p>Secondary Contact Email Address</p> <p>Secondary Contact Authorizations</p> <p>Employer Coverage Offered</p> <p>Employer-selected AV Levels (Bronze, Silver, Gold, or Platinum)</p> <p>Benchmark Plan</p>

**Category  
Description**

Employer Offering Coverage Information continued	<p>Offer of Dependent Coverage</p> <p>Agent/Broker/Assister/Navigator Name, Organization Name, Contact Information, FFM User ID</p> <p>Employer Contribution Information:</p> <ul style="list-style-type: none"> <li>• Benchmark Plan ID number-Medical Plan</li> <li>• Benchmark Plan ID number-Dental Plan</li> <li>• Percentage towards Employee-Medical Coverage</li> <li>• Percentage towards Employee Dental Coverage</li> <li>• Percentage towards Dependent Medical Coverage</li> <li>• Percentage towards Dependent Dental Coverage</li> <li>• Employer Offering-Single QHP or Single Metal Level or Single Issuer</li> <li>• Employer Offering-Single Stand-alone Dental Plan (“SADP”) or multiple SADPs</li> </ul> <p>Offer of Stand-alone Dental Coverage</p> <p>Desired Effective Date of Coverage</p> <p>Employee Selection Due Date</p> <p>Waiting Period for New Hires to Enroll</p> <p>Employee List, including:</p> <ul style="list-style-type: none"> <li>• Employee Name</li> <li>• Employee Date of Birth</li> <li>• Employee Age</li> <li>• Employee Social Security Number</li> <li>• Employee Email Address</li> <li>• Employee Employment Status</li> <li>• Employee’s Other Coverage</li> <li>• Number of Dependents</li> <li>• Dependent Information, including Dependent Name</li> <li>• Dependent Date of Birth</li> <li>• Dependent Age</li> <li>• Dependent Social Security Number</li> <li>• Dependent Email Address</li> <li>• Dependent’s Other Coverage</li> </ul> <p>Payment Method options, including:</p> <ul style="list-style-type: none"> <li>• Electronic Funds Transfer Information (Checking Account Number, Routing Number)</li> <li>• Credit Card Information (Credit Card type, Name on Credit Card, Credit Card Number, Expiration Date, Signature, Signature Date)</li> <li>• Checking Information</li> </ul> <p>Employer Attestation to Consolidated Omnibus Budget Reconciliation Act (“COBRA”)/Medicare Compliance Questions</p>
--	--

- d. Use of PII. PII collected from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—in the context of completing an application for QHP, APTC, or CSR eligibility, if applicable, or enrolling in a QHP, or any data transmitted from or through the Hub, if applicable, may be used only for Authorized Functions specified in Section II.a of this Agreement. Such Information may not be used for purposes other than authorized by this Agreement or as consented to by a Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and Qualified Employer—or these individuals’ legal representatives or Authorized Representatives.
- e. Collection and Use of Information Provided Under Other Authorities. This Agreement does not preclude Web-broker from collecting Information from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—for a non-FFE/non-SBE-FP/non-Hub purpose, and using, reusing, and disclosing the non-FFE/non-SBE-FP/non-Hub Information obtained as permitted by applicable law and/or other applicable authorities. Such Information must be stored separately from any PII collected in accordance with Section II.c of this Agreement. The Hub Web Services are not available for SHOP.
- f. Commitment to Protect PII. Web-broker shall not release, publish, or disclose Consumer, Applicant, Qualified Individual, or Enrollee PII to unauthorized personnel, and shall protect such Information in accordance with provisions of any laws and regulations governing the adequate safeguarding of Consumer, Applicant, Qualified Individual, or Enrollee PII, the misuse of which carries with it the potential to cause financial, reputational and other types of harm.
  1. Technical leads must be designated to facilitate direct contacts between the Parties to support the management and operation of the interconnection.
  2. The overall sensitivity level of data or Information that will be made available or exchanged across the interconnection will be designated as MODERATE as determined by Federal Information Processing Standards (FIPS) Publication 199.
  3. Web-broker agrees to comply with all federal laws and regulations regarding the handling of PII—regardless of where the organization is located or where the data are stored and accessed.
  4. Web-broker’s Rules of Behavior must be at least as stringent as the HHS Rules of Behavior.<sup>2</sup>
  5. Web-broker understands and agrees that all financial and legal liabilities arising from inappropriate disclosure or Breach of Consumer, Applicant, Qualified Individual, or Enrollee PII while such Information is in the possession of Web-broker shall be borne exclusively by Web-broker.
  6. Web-broker shall train and monitor staff on the requirements related to the authorized use and sharing of PII with third parties and the consequences of

---

<sup>2</sup> The HHS Rules of Behavior are available at the following link: <https://www.hhs.gov/ocio/policy/hhs-rob.html>.

unauthorized use or sharing of PII, and periodically audit their actual use and disclosure of PII.

- g. Ability of Individuals to Limit Collection and Use of PII. Web-broker agrees to provide the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee or Qualified Employer—or these individuals’ legal representatives or Authorized Representatives—the opportunity to opt in and have Web-broker collect, create, disclose, access, maintain, store and use their PII. Web-broker agrees to provide a mechanism through which the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee and Qualified Employer—or these individuals’ legal representatives or Authorized Representatives—can limit Web-broker’s creation, collection, disclosure, access, maintenance, storage, and use of their PII to the sole purpose of obtaining Web-broker’s assistance in performing Authorized Functions specified in Section II.a of this Agreement.
- h. Incident and Breach Reporting. Web-broker must implement Incident and Breach Handling procedures as required by the NEE SSP and that are consistent with CMS’s Incident and Breach Notification Procedures. Such policies and procedures must identify the Web-broker’s Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents or Breaches; provide details regarding the identification, response, recovery and follow-up of Incidents and Breaches, which should include Information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes. Web-broker agrees to report any Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at [cms\\_it\\_service\\_desk@cms.hhs.gov](mailto:cms_it_service_desk@cms.hhs.gov) within 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.

### III. Approval and Renewal Minimum Direct Enrollment (“DE”) Program Participation Requirements.

- a. Completion of Operational Readiness Review Required Under 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f).
  - 1. End-to-End Testing and Enrollment Validation Requirement. In order to be approved as a Web-broker, or to maintain status as an Existing Web-broker during Web-broker Agreement renewal, Web-broker must demonstrate a successful end-to-end DE transaction through any of the following: a history of enrollments completed via Classic DE or EDE during the term of the prior year’s Web-broker Agreement or by end-to-end testing either with the Hub or during the EDE business audit submission process within the term of the prior year’s Web-broker Agreement, as applicable.
  - 2. Operational and Oversight Information Form. In order to be approved as a Web-broker, Web-broker must submit an Operational and Oversight Information Form to CMS in the form and manner specified by CMS. In order to maintain status as an Existing Web-broker during Web-broker Agreement renewal, Web-broker must submit annually an Operational and Oversight Information Form to CMS in the form and manner specified by CMS.

3. Operational Information. When onboarding annually during Agreement renewal, and upon request, the Web-broker must provide CMS operational Information, including, but not limited to, its Designated Representative's National Producer Number (NPN), State licensure Information, and Information about its downstream Agents/Brokers, if applicable.
4. Pre-Approval Website Review. Prospective Web-brokers must receive and resolve any designated compliance findings identified by CMS during a pre-approval website review prior to receiving a countersigned Web-broker Agreement. To facilitate this review, upon request, a Prospective Web-broker must provide CMS with a set of credentials CMS can use to access the Prospective Web-broker's testing DE Environment (i.e., the pre-production environment) to complete the website review of the Prospective Web-broker's DE Environment. The Prospective Web-broker must ensure that the testing credentials are valid and that all APIs and components in the testing DE Environment are accessible for the duration of the review. This provision does not apply to Existing Web-brokers that have received a CMS website review during the term of the prior year's Web-broker Agreement.
5. Designated Representative Registration and Training with the Exchange. Web-broker's Designated Representative(s) must complete the applicable annual registration and training requirements with the Exchange. Web-broker, including Agent or Broker Direct Enrollment Technology Provider, must provide this information to CMS to connect to the DE or EDE web services in production.
6. Privacy and Security Documentation. In order to receive approval to participate in DE and utilize an approved DE Environment, Web-brokers must submit the complete set of documents outlined in Table 1 of Appendix A: Privacy and Security Standards for Web-brokers to CMS, except as noted in the "Submission Requirements" column and must comply with the privacy and security audit requirements under Section IX of this Agreement. The annual assessment results that serve as the basis for the documentation in Table 1 of Appendix B: Annual Security and Privacy Assessment (SPA) are only valid for a period of 365 Days from the completion date of the assessment. Web-brokers must complete the continuous monitoring requirements detailed in the Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide.<sup>3</sup>

The Web-broker must conduct penetration testing which examines the network, application, device, and physical security of its DE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Web-brokers must adhere to the requirements for Penetration Testing described in Section V.b and Appendix B: Annual Security and Privacy Assessment (SPA) of this Agreement.

- b. Web-broker Public List Requirements. In order to be listed on CMS's Web-broker Public List, Web-brokers must have completed the applicable onboarding or renewal processes (see Section III.a of this Agreement); have a valid, countersigned Web-broker

---

<sup>3</sup> The ISCM Strategy Guide is available on CMS zONE at the following link:  
<https://zone.cms.gov/document/privacy-and-security-audit>.

Agreement; and have an active, approved Secure Sockets Layer (SSL) production certificate with the Hub for the applicable plan year or an SSL production certificate pending CMS approval under Section III.a.5 of this Agreement.

#### IV. Downstream Use of Web-broker's DE Environment.

- a. Downstream Agent/Broker and DE Entity Application Assister Use of a Web-broker's DE Environment. A Web-broker that provides access to its DE Environment to downstream Agents and Brokers and DE Entity Application Assisters, consistent with 45 C.F.R. §§ 155.220(c)(4) and 155.221(c), must provide a DE Environment to its downstream Agents and Brokers and DE Entity Application Assisters that complies with this Agreement and the Web-broker requirements in 45 C.F.R. §§ 155.220 and 155.221. Web-broker must not provide the capability for downstream Agents/Brokers to use its DE Environment through the third party's own website or otherwise outside of Web-broker's approved website. The use of embedding tools and programming techniques by downstream Agents/Brokers, such as iframe technical implementations, that may enable the distortion, manipulation, or modification of the approved DE Environment and the overall DE End-User experience developed by Web-broker are prohibited.

As part of the DE or EDE-facilitated application and QHP application processes, Web-broker must not enable or allow the selection of QHPs by a consumer or Agent/Broker on a third-party website that exists outside of the Web-broker's approved DE Environment. This includes pre-populating or pre-selecting a QHP for a consumer that was selected on a downstream Agent's/Broker's website or a lead generator's website. This prohibition does not extend to websites that are provided, owned, and maintained by entities subject to CMS regulations for QHP display (i.e., Web-brokers and QHP Issuers).

The Web-broker must have a written contract or other written arrangement with the downstream Agent or Broker or DE Entity Application Assisters that governs the arrangement and requires the adherence to the terms of this Agreement.

Upon request, Web-broker must provide CMS with information about its downstream Agents/Brokers, Web-broker's oversight of its downstream Agents/Brokers, and the DE Environment(s) it provides to each of its downstream Agents/Brokers.

- b. QHP Issuer Use of a Web-broker's DE Environment. Web-broker may provide access to its DE Environment to QHP Issuers for use by the QHP Issuer and/or the QHP Issuer's downstream Agents and Brokers and DE Entity Application Assisters that is branded and specific to that QHP Issuer. In these cases, the Web-broker would be considered a downstream and delegated entity of the QHP Issuer under 45 C.F.R. § 156.340. There must be a written contract or other written arrangement between the Web-broker and the QHP Issuer that governs the arrangement and requires adherence to the terms of this Agreement. The QHP Issuer's DE Environment that is provided by the Web-broker must comply with the DE requirements applicable to QHP Issuers in 45 C.F.R. §§ 155.221 and 156.1230.

#### V. DE Environment and Website Requirements.

- a. Maintenance of an Accurate Testing DE Environment. Web-broker must maintain a testing DE Environment that accurately represents the Web-broker's production DE Environment and integration with the Classic DE pathway, including functional use of all



DE APIs. Web-brokers must maintain at least one testing DE Environment that reflects the Web-broker's current production DE Environments when developing and testing any prospective changes to its production DE Environments. This will require Web-broker to develop one or more separate testing DE Environments (other than production and the testing DE Environment that reflects production) for developing and testing prospective changes to Web-broker's production DE Environments. Network traffic into and out of all non-production environments is only permitted to facilitate system testing and must be restricted by source and destination access control lists, as well as ports and protocols, as documented in the NEE SSP, SA-11 implementation standard. Web-broker must not submit actual PII to the FFE Testing Environments. The Web-broker shall not submit test data to the FFE Production Environments. Web-broker's testing DE Environment shall be readily accessible to applicable CMS staff and contractors via the Internet to complete CMS audits.

Upon request, Web-broker must provide CMS with a set of credentials and any additional instructions necessary so that CMS can access the testing DE Environment that reflects the Web-broker's production environment to complete audits or otherwise confirm compliance of Web-broker's production DE Environments. The Web-broker must be able to provide test credentials for all DE Environments that Web-broker hosts or provides (and/or prototypes of those DE Environments), including, but not limited to, the Web-broker's Consumer-facing DE Environment, Web-broker's Agent/Broker-facing DE Environment, a Consumer-facing website that the Web-broker provides for use by Agents or Brokers, and an Agent- or Broker-facing DE Environment that the Web-broker provides for use by Agents/Brokers. Web-broker must ensure that the testing credentials are valid and that all APIs and components in the testing DE Environment, including the remote identity proofing (RIDP) services, are readily accessible via Internet for CMS to audit or otherwise confirm compliance of Web-broker's production DE Environment as determined necessary by CMS.

- b. Penetration Testing. The DE Entity must conduct penetration testing which examines the network, application, device, and physical security of its DE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Before conducting the penetration testing, the DE Entity must execute a Rules of Engagement with its Auditor's penetration testing team. The DE Entity must also notify its CMS designated technical counterparts on its annual penetration testing schedule a minimum of 5 business days prior to initiation of the penetration testing using the CMS-provided form.<sup>4</sup> During the penetration testing, the Auditor's testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment. The penetration testing shall be conducted in the lower environment that reflects the DE Entity's current production environment.
- c. Limit Concurrent Sessions. The Web-broker must limit the number of concurrent sessions to one (1) session per a single set of credentials/FFE user ID. However, multiple sessions associated with a single set of credentials/FFE user ID that is traceable to a

---

<sup>4</sup> The Penetration Testing Notification Form is available at the following links:  
<https://zone.cms.gov/document/privacy-and-security-audit>.

single device/browser is permitted.

- d. Health Reimbursement Arrangement (HRA) Messaging. If Web-broker implements full HRA functionality, Web-broker must implement required User Interface (UI) messaging for qualified individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the qualified individuals consistent with CMS guidance. Required UI messaging for various scenarios is detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.<sup>5</sup>
- e. APTC Selection and Attestation. Web-broker must allow Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—to select and attest to an APTC amount, if applicable, in accordance with 45 C.F.R. § 155.310(d)(2). Web-broker should use the specific language detailed in the FFE and FF-SHOP Enrollment Manual<sup>6</sup> when providing Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals’ legal representatives or Authorized Representatives—with the ability to attest to an APTC amount.

#### VI. Effective Date and Term; Renewal.

- a. Effective Date and Term. This Agreement becomes effective on the date the last of the two Parties executes this Agreement and ends the Day before the first Day of the open enrollment period (“OEP”) under 45 C.F.R. § 155.410(e)(3) for the benefit year beginning January 1, 2025.
- b. Renewal. This Agreement may be renewed upon the mutual agreement of the Parties for subsequent and consecutive one (1) year periods upon thirty (30) Days’ advance written notice to Web-broker.

#### VII. Suspension.

- a. Suspension Pursuant to 45 C.F.R. §§ 155.220 and 155.221. The suspension of the ability of Web-broker to transact information with the Exchange shall be governed by the suspension standards adopted by the FFEs or SBE-FPs under 45 C.F.R. §§ 155.220 and 155.221.
- b. Duration of Suspension. Consistent with the standards under 45 C.F.R. §§ 155.220 and 155.221, Web-broker will remain suspended until Web-broker remedies or sufficiently mitigates the issue(s) that were the basis for the suspension to HHS’s satisfaction. If this Agreement expires prior to HHS removing the suspension, HHS will not execute a subsequent Web-broker Agreement with Web-broker until Web-broker remedies or sufficiently mitigates the issue(s) to HHS’s satisfaction.

#### VIII. Termination.

- a. Termination Without Cause. Either Party may terminate this Agreement without cause and for its convenience upon thirty (30) Days’ prior written notice to the other Party.

---

<sup>5</sup> The document Direct Enrollment API Specs is available on CMS zONE at the following link: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.

<sup>6</sup> The SHOP Enrollment Manual is available on CMS zONE at the following link: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.



Web-broker must reference and complete the NEE Decommissioning Plan and NEE Decommissioning Close Out Letter in situations where Web-broker will retire or decommission its DE Environment.<sup>7</sup>

- b. Termination of Agreement with Notice by CMS. The termination of this Agreement and the reconsideration of any such termination shall be governed by the termination and reconsideration standards adopted by the FFEs or SBE-FPs under 45 C.F.R. § 155.220. Notwithstanding the foregoing, the Web-broker shall be considered in “Habitual Default” of this Agreement in the event it has been served with a non-compliance notice under 45 C.F.R. § 155.220(g) more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately terminate this Agreement upon notice to Web-broker without any further opportunity to resolve the Breach and/or non-compliance. CMS may also temporarily suspend the ability of a Web-broker to make its website available to transact Information with HHS pursuant to 45 C.F.R. §§ 155.220(c)(4)(ii) or 155.221(d).
- c. Termination for Failure to Maintain Valid State Licensure. Web-broker acknowledges and agrees that valid State licensure in each State in which Web-broker assists Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—in applying for or obtaining coverage under a QHP through an FFE or SBE-FP is a precondition to the Web-broker’s authority under this Agreement. Accordingly, CMS may terminate this Agreement if Web-broker fails to maintain valid licensure in at least one FFE or SBE-FP State, and in each State for which Web-broker facilitates enrollment in a QHP through the FFE or an SBE-FP. Any such termination shall be governed by the standards adopted by the FFE under 45 C.F.R. § 155.220(g) and (h). If Web-broker is an Agent or Broker Direct Enrollment Technology Provider and maintains no contractual relationships with Agents or Brokers and is not owned or operated by an Agent or Broker, the entity would no longer meet the applicable definition under 45 C.F.R. § 155.20 to be an Agent or Broker Direct Enrollment Technology Provider. Web-broker understands and agrees that in such circumstances CMS may immediately terminate this Agreement for cause, or the Agent or Broker Direct Enrollment Technology Provider may provide advance notice to CMS to terminate this agreement without cause per Section VIII.a of this Agreement. If the Agent or Broker Direct Enrollment Technology Provider is unable to provide thirty (30) Days’ advance notice to CMS, the Agent or Broker Direct Enrollment Technology Provider must notify CMS within thirty (30) Days after the entity no longer meets the applicable definition under 45 C.F.R. § 155.20 to be an Agent or Broker Direct Enrollment Technology Provider.
- d. Destruction of PII. Web-broker covenants and agrees to destroy all PII in its possession at the end of the record retention period required under the NEE SSP, which is consistent with NIST SP 800-88 Rev. 1. If, upon the termination or expiration of this Agreement, Web-broker has in its possession PII for which no retention period is specified in the NEE SSP, such PII shall be destroyed within thirty (30) Days of the termination or

---

<sup>7</sup> The Non-Exchange Entity (NEE) Decommissioning Plan and NEE Decommissioning Close Out Letter are available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>

expiration of this Agreement. Web-broker's duty to protect and maintain the privacy and security of PII, as provided for in the NEE SSP, shall continue in full force and effect until such PII is destroyed and shall survive the termination or expiration of this Agreement.

- e. Termination of Registration from the FFEs. Web-broker acknowledges that the termination or expiration of this Agreement will result in the termination of the Web-broker's registration with the FFE.

**IX. Privacy and Security Audit Requirement.** In order to receive approval to participate in DE and utilize an approved DE Environment, Web-broker must contract with one or more independent Auditor(s) consistent with this Agreement's provisions and applicable regulatory requirements to conduct an annual security and privacy assessment (SPA) as described in Appendix B: Annual Security and Privacy Assessment (SPA), the ISCM Strategy Guide, and the NEE SSP.

The Auditor must document and attest in the SPA documentation that Web-broker's DE Environment, including its website and operations, complies with the terms of this Agreement, other applicable agreement(s) with CMS (including the EDE Business Agreement and Interconnection Security Agreement), the Framework for the Independent Assessment of Security and Privacy Controls, and applicable program requirements. EDE Entity must submit the resulting SPA documentation to CMS. The SPA must detail EDE Entity's compliance with the requirements set forth in Appendix B, including any requirements set forth in CMS guidance referenced in Appendix B. The SPA that Web-broker submits to CMS must demonstrate that Web-broker's Auditor(s) conducted its review in accordance with the review standards set forth in Appendix B, the ISCM Strategy Guide, and the NEE SSP.

CMS will approve Web-broker's DE Environment only once it has reviewed and approved the privacy and security audit findings reports. Final approval of Web-broker's DE Environment will be evidenced by CMS countersigning the ISA with Web-broker. Upon receipt of the counter-signed ISA, Web-broker will be approved to use its approved DE Environment consistent with applicable regulations, this Agreement, and the ISA.

- a. Identification of Auditor(s) and Subcontractors of Auditor(s). All Auditor(s), including any Auditor(s) that has subcontracted with Web-broker's Auditor(s), will be considered Downstream or Delegated Entities of Web-broker pursuant to Web-broker's respective agreement(s) with CMS and applicable program requirements. Web-broker must identify each Auditor it selects, and any subcontractor(s) of the Auditor(s), in Appendix E: Auditor Identification of this Agreement. Web-broker must also submit a copy of the signed agreement or contract between the Auditor(s) and Web-broker to CMS.
- b. Conflict of Interest. For any arrangement between Web-broker and an Auditor for audit purposes covered by this Agreement, Web-broker must select an Auditor that is free from any real or perceived conflict(s) of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. Web-broker must disclose to HHS any financial relationships between the Auditor, and individuals who own or are employed by the Auditor, and individuals who own or are employed by a Web-broker for which the Auditor is conducting an ORR privacy and security audit pursuant to 45 C.F.R. §§ 155.220(c)(6)(iv), 155.221(b)(4)(ii),

and 155.221(f). Web-broker must document and disclose any conflict(s) of interest in the form in Appendix F: Conflict of Interest Disclosure Form, if applicable.

- c. Auditor Independence and Objectivity. Web-broker's Auditor(s) must remain independent and objective throughout the audit process. An Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the DE Environment and the determination of security and privacy control effectiveness. Web-broker must not take any actions that impair the independence and objectivity of Web-broker's Auditor. Web-broker's Auditor must attest to their independence and objectivity in completing the DE audit(s).
- d. Required Documentation. Web-broker must maintain and/or submit the required documentation detailed in Appendix B: Annual Security and Privacy Assessment (SPA), including templates provided by CMS, to CMS in the manner specified in Appendix B: Annual Security and Privacy Assessment (SPA). Documentation that Web-broker must submit to CMS (as set forth in Section III and Appendices B, E, and F of this Agreement) will constitute Web-broker's Application.

X. Miscellaneous.

- a. Notice. All notices to Parties specifically required under this Agreement shall be given in writing and shall be delivered as follows:
  - If to CMS, by email at: [directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov)
  - If to Web-broker, to Web-broker's email address on record.

Notices sent by email shall be deemed to have been given when the appropriate confirmation of receipt has been received; notices not given on a business Day (i.e., Monday-Friday, excluding federal holidays) between 9:00 a.m. and 5:00 p.m. local time where the recipient is located shall be deemed to have been given at 9:00 a.m. on the next business Day for the recipient. A Party to this Agreement may change its contact information for notices and other communications by providing written notice of such changes in accordance with this provision. Such notice should be provided thirty (30) Days in advance of such change, unless circumstances warrant a shorter timeframe.

- b. Assignment and Subcontracting. Except as otherwise provided in this Section, Web-broker shall not assign this Agreement in whole or in part, whether by merger, acquisition, consolidation, reorganization, or otherwise any portion of the services to be provided by Web-broker under this Agreement without the express, prior written consent of CMS, which consent may be withheld, conditioned, granted, or denied in CMS' sole discretion. Web-broker must provide written notice at least thirty (30) Days prior to any such proposed assignment, including any change in ownership of Web-broker or any change in management or ownership of the DE Environment. Notwithstanding the foregoing, CMS does not require prior written consent for subcontracting arrangements that do not involve the operation, management, or control of the DE Environment. Web-broker must report all subcontracting arrangements on its annual Operational and Oversight Information form during the annual Web-broker agreement renewal process and submit revisions annually thereafter. Web-broker shall assume ultimate responsibility

for all services and functions described under this Agreement, including those that are subcontracted to other entities, and must ensure that subcontractors will perform all functions in accordance with all applicable requirements. Web-broker shall further be subject to such oversight and enforcement actions for functions or activities performed by subcontractor entities as may otherwise be provided for under applicable law and program requirements, including this Agreement with CMS. Notwithstanding any subcontracting of any responsibility under this Agreement, Web-broker shall not be released from any of its performance or compliance obligations hereunder, and shall remain fully bound to the terms and conditions of this Agreement as unaltered and unaffected by such subcontracting.

If Web-broker attempts to make an assignment, subcontracting arrangement or otherwise delegate its obligations hereunder in violation of this provision, such assignment, subcontract, or delegation shall be deemed void *ab initio* and of no force or effect, and Web-broker shall remain legally bound hereto and responsible for all obligations under this Agreement.

- c. Use of the Hub Web Services. Web-broker will only use a CMS-approved DE Environment when accessing the APIs and web services that facilitate functionality to enroll Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix A: Privacy and Security Standards for , Appendix B: Annual Security and Privacy Assessment (SPA), and Appendix D: Standards for Communication with the Hub.
- d. Survival. Web-broker’s duty to protect and maintain the privacy and security of PII and any other obligation under this Agreement which, by its express terms or nature and context is intended to survive expiration or termination of this Agreement, shall survive the expiration or termination of this Agreement.
- e. Severability. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement. In the event that any provision of this Agreement is determined to be invalid, unenforceable or otherwise illegal, such provision shall be deemed restated, in accordance with applicable law, to reflect as nearly as possible the original intention of the Parties, and the remainder of the Agreement shall be in full force and effect.
- f. Disclaimer of Joint Venture. Neither this Agreement nor the activities of Web-broker contemplated by and under this Agreement shall be deemed or construed to create in any way any partnership, joint venture or agency relationship between CMS and Web-broker. Neither Party is, nor shall either Party hold itself out to be, vested with any power or right to bind the other Party contractually or to act on behalf of the other Party, except to the extent expressly set forth in the ACA and the regulations codified thereunder, including as codified at 45 C.F.R. part 155.
- g. Remedies Cumulative. No remedy herein conferred upon or reserved to CMS under this Agreement is intended to be exclusive of any other remedy or remedies available to CMS under operative law and regulation, and each and every such remedy, to the extent

permitted by law, shall be cumulative and in addition to any other remedy now or hereafter existing at law or in equity or otherwise.

- h. Records. Web-broker shall maintain all records that it creates in the normal course of its business in connection with activity under this Agreement for the term of this Agreement in accordance with 45 C.F.R. § 155.220(c)(3)(i)(E). Subject to applicable legal requirements and reasonable policies, such records shall be made available to CMS to ensure compliance with the terms and conditions of this Agreement. The records shall be made available during regular business hours at Web-broker's offices, and CMS's review shall not interfere unreasonably with Web-broker's business activities. This clause survives the expiration or termination of this Agreement.
- i. Compliance with Law. Web-broker covenants and agrees to comply with any and all applicable laws, statutes, regulations, or ordinances of the United States of America and any Federal Government agency, board, or court that are applicable to the conduct of the activities that are the subject of this Agreement, including, but not necessarily limited to, any additional and applicable standards required by statute, and any regulations or policies implementing or interpreting such statutory provisions hereafter issued by CMS. In the event of a conflict between the terms of this Agreement and any statutory, regulatory, or sub-regulatory guidance released by CMS, the requirement that constitutes the stricter, higher, or more stringent level of compliance shall control.
- j. Governing Law and Consent to Jurisdiction. This Agreement will be governed by the laws and common law of the United States of America, including without limitation such regulations as may be promulgated by HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. Web-broker further agrees and consents to the jurisdiction of the Federal Courts located within the District of Columbia and the courts of appeal therefrom, and waives any claim of lack of jurisdiction or *forum non conveniens*.
- k. Amendment. CMS may amend this Agreement for purposes of reflecting changes in applicable law or regulations, with such amendments taking effect upon thirty (30) Days' written notice to Web-broker ("CMS notice period"), unless circumstances warrant an earlier effective date. Any amendments made under this provision will only have prospective effect and will not be applied retrospectively. Web-broker may reject such amendment by providing to CMS, during the CMS notice period, written notice of its intent to reject the amendment ("rejection notice period"). Any such rejection of an amendment made by CMS shall result in the termination of this Agreement upon expiration of the rejection notice period.
- l. Audit and Compliance Review. Web-broker agrees that CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees may conduct compliance reviews or audits, which includes the right to interview employees, contractors and business partners of Web-broker and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of Web-broker's compliance with the requirements of this Agreement upon reasonable notice to Web-broker, during Web-broker's regular business hours, and at Web-broker's regular business location. These audit and review rights include the right to audit Web-broker's compliance with and implementation of the privacy and security requirements

under this Agreement. Web-broker further agrees to allow reasonable access to the Information and facilities, including, but not limited to, Web-broker website testing environments, requested by CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees for the purpose of such a compliance review or audit. CMS may suspend or terminate this Agreement if Web-broker does not comply with such a compliance review request within seven (7) business Days. If any of Web-broker's obligations under this Agreement are delegated to other parties, Web-broker's agreement with any delegated or downstream entities must incorporate this Agreement provision. This clause survives the expiration or termination of this Agreement.

- m. Access to the FFEs and SBE-FPs. Any Web-broker; its Downstream and Delegated Entities, including downstream Agents/Brokers; and its assignees or subcontractors, including, employees, developers, agents, representatives, or contractors, cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to a Web-broker's systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through virtual private networks ("VPNs").

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]



This “Agreement Between Web-Broker and the Centers for Medicare & Medicaid Services for the Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform” has been signed and executed by:

**TO BE FILLED OUT BY WEB-BROKER**

The undersigned is an authorized official of Web-broker who is authorized to represent and bind Web-broker for purposes of this Agreement.

*Manal Mehta*

10-19-2023

Signature of Authorized Official of Web-broker

Date

**Manal Mehta, CEO**

Printed Name and Title of Authorized Official of Web-broker

**Benefitalign LLC**

Web-broker Name

*T White*

Signature of Privacy Officer Attesting Compliance that Web-broker Systems Comply with Appendices A and B of this Agreement and the Non-Exchange Entity System Security and Privacy Plan

**Tamara White, Sr. Director**

Printed Name and Title of Privacy Officer Attesting Compliance that Web-broker Systems Comply with Appendices A and B of this Agreement and the Non-Exchange Entity System Security and Privacy Plan

**2400 Louisiana Blvd NE,**

**04.BFT.MD\*.450.850**

**Building 3, Albuquerque,**

Web-broker Partner ID

**NM 87110**

**REDACTED**

Web-broker Address

Web-broker Contact Number

**Web-broker must indicate in the below checkbox whether Web-broker will assist Qualified Employees and/or Qualified Employers in applying for or enrolling in SHOP coverage for the benefit year as defined in Section VI.a of this Agreement:**

Web-broker *will* assist Qualified Employees and/or Qualified Employers in the benefit year as defined in this Agreement

Web-broker ***will not*** assist Qualified Employees and/or Qualified Employers in the benefit year as defined in this Agreement



Centers for Medicare & Medicaid Services

---

**FOR CMS**

The undersigned are officials of CMS who are authorized to represent and bind CMS for purposes of this Agreement.

**Jeffrey Grant -S** Digitally signed by Jeffrey Grant -S  
Date: 2023.10.19 15:50:03 -04'00'

---

**Jeffrey D. Grant**

**Date**

Deputy Director for Operations

Center for Consumer Information and Insurance Oversight

Centers for Medicare & Medicaid Services

**George C. Hoffmann -S** Digitally signed by George C. Hoffmann -S  
Date: 2023.10.30 07:12:02 -04'00'

---

**George C. Hoffmann**

**Date**

CMS Deputy CIO

Deputy Director, Office of Information Technology (OIT)

Centers for Medicare & Medicaid Services (CMS)

### **Appendix A: Privacy and Security Standards for Web-brokers**

Federally-facilitated Exchanges (“FFE’s”) will enter into contractual agreements with all Non-Exchange Entities, including Web-brokers, that gain access to Personally Identifiable Information (“PII”) exchanged with the FFEs (including FF-SHOPs) and State-based Exchanges on the Federal Platform (“SBE-FPs”) (including SBE-FP-SHOPs), or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals’ legal representatives or Authorized Representatives. This Agreement and its appendices govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by Web-brokers in the context of the FFEs and SBE-FPs (including FF-SHOPs and SBE-FP-SHOPs). In signing this contractual Agreement, in which this Appendix A has been incorporated, Web-brokers agree to comply with the security and privacy standards and implementation specifications outlined in the Non-Exchange Entity System Security and Privacy Plan (NEE SSP)<sup>8</sup> while performing the Authorized Functions outlined in their respective Agreement(s) with CMS.

The standards documented in the NEE SSP are established in accordance with Section 1411(g) of the Affordable Care Act (“ACA”) (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 (“FISMA”) (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the principles in 45 C.F.R. §§ 155.260(a)(1) through (a)(6). All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

In addition, Web-brokers must comply with the annual security and privacy assessment (SPA) requirements in Appendix B.

---

<sup>8</sup> References to security and privacy controls and implementation standards can be found in the NEE SSP located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

### **Appendix B: Annual Security and Privacy Assessment (SPA)**

Consistent with 45 C.F.R. §§ 155.220(c)(6)(iv), 155.221(b)(4)(ii) and 155.221(f), the Web-broker must contract with one or more independent Auditors to conduct an annual SPA as described below and in the ICSM Strategy Guide and the NEE SPP. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

The SPA shall include the following:

- Documentation of existing security and privacy controls;
- Identification of potential security and privacy risks; and
- Corrective action plan describing approach and timeline to implement security and privacy controls to mitigate potential security and privacy risks.

(1) Independent Third-Party Audit. The Web-broker must contract with an independent third-party Auditor(s) with experience conducting Information system privacy and security audits to perform the SPA. The Web-broker and its Auditor(s) should refer to the Framework for Independent Assessment of Security and Privacy Controls<sup>9</sup> which provides an overview of the independent security and privacy assessment requirements.

The Web-broker and its Auditor(s) may reference existing audit results that address some or all of the SPA's requirements. Such existing audit results must have been generated by an independent third-party Auditor. In addition, such existing audit results must have been produced within 365 Days of completion of the SPA. If existing audit reports do not address all required elements of the SPA, the remaining elements must be addressed by an independent third-party Auditor.

(2) Assessment Methodology. The SPA methodology herein is based on the standard CMS methodology and is described in the Framework for Independent Assessment of Security and Privacy Controls. The Auditor must prepare and Web-broker must submit a Security Privacy Controls Assessment Test Plan (SAP) that describes the Auditor's scope and methodology of the assessment. Web-broker must submit the Auditor-prepared SAP at least thirty (30) Days prior to commencing the assessment. The assessment methods may include examination of documentation, logs, and configurations; interviews of personnel; and/or testing of technical controls. The SPA must provide an accurate depiction of the security and privacy controls in place, as well as potential security and privacy risks, by identifying the following:

- a. Application or system vulnerabilities, the associated business and system risks and potential impact;
- b. Weaknesses in the configuration management process such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system;
- c. Web-broker security and privacy policies and procedures; and
- d. Major documentation omissions and/or discrepancies.

---

<sup>9</sup> This document is located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

- (3) Tests and Analysis Performed. The SPA must include tests that analyze applications, systems, and associated infrastructure.<sup>10</sup> The tests should begin with high-level analyses and increase in specificity. Tests and analyses performed during an assessment should include:
- a. Security Control technical testing;
  - b. Penetration testing;
  - c. Adherence to privacy program policies;
  - d. Network and component vulnerability scanning;
  - e. Configuration assessment;
  - f. Documentation review;
  - g. Personnel interviews; and
  - h. Observations.
- (4) Noncompliance and Applicability. The Web-broker must develop a corrective action plan to mitigate any security and privacy risks if the SPA identifies a deficiency in the Web-broker's security and privacy controls as documented in a Plan of Action & Milestones (PO&M). Alternatively, the Web-broker may document why it believes a critical control is not applicable to its system or circumstances. The SPA results do not alter this Agreement, including any penalties for non-compliance. If the Web-broker's SPA includes findings suggesting significant security or privacy risks, and the Web-broker does not commence development and implementation of a corrective action plan to the reasonable satisfaction of CMS, a comprehensive audit may be initiated by CMS, and/or this Agreement may be terminated for cause. In addition, CMS may delay providing final approval or may withdraw prior approval of Web-broker's DE Environment if the Web-broker does not address to the reasonable satisfaction of CMS the findings suggesting significant security or privacy risks.
- (5) Non-Exchange Entity System Security Plan ("NEE SSP"). The Web-broker must implement the controls documented in the Security and Privacy Controls for Web-brokers Supplement, though, CMS strongly recommends Web-brokers participating in Classic DE implement all the NEE SSP controls.<sup>11</sup> The Web-broker's Auditor(s) must verify and document the Web-broker's implementation and compliance with at least the controls listed in the Security and Privacy Controls for Web-brokers Supplement. The Security Privacy Assessment Report (SAR) will be accepted by CMS as documentation of compliance with those controls so long as the assessment has been conducted within 365 Days of the completion date of the previous assessment.
- (6) SPA Documentation Submission. The following table identifies the required SPA documentation that Web-Brokers must submit to CMS.

**Table 1: Web-broker Privacy and Security Document Submission Requirements**

---

<sup>10</sup> The Security and Privacy Controls Assessment Test Plan (SAP) Template and the Security and Privacy Assessment Report (SAR) Template provide additional guidance on testing methodology and reporting requirements. These documents are located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

<sup>11</sup> The Security and Privacy Controls for Web-brokers Supplement will be posted at the following link on CMS zONE: <https://zone.cms.gov/document/privacy-and-security-audit>.

Document	Description	Submission Requirements
<b>Security Privacy Controls Assessment Test Plan (SAP)</b>	<ul style="list-style-type: none"> <li>▪ The SAP describes the Auditor's scope and methodology of the assessment.</li> <li>▪ The SAP includes an attestation of the Auditor's independence.</li> <li>▪ The SAP must be completed by the Auditor and submitted to CMS for review, prior to conducting the security and privacy assessment (SPA).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the Entity-specific DE/EDE PME site at least thirty (30) days before commencing the privacy and security audit; during the planning phase.</li> </ul>
<b>Security and Privacy Assessment Report (SAR)</b>	<ul style="list-style-type: none"> <li>▪ The report should contain a summary of findings that includes ALL findings from the assessment to include documentation reviews, control testing, scanning, penetration testing, interview(s), etc. <ul style="list-style-type: none"> <li>○ Explain if and how findings are consolidated.</li> <li>○ Ensure risk level determination is properly calculated, especially when weaknesses are identified as part of the Center for Internet Security (CIS) Top 20 and/or OWASP Top 10.</li> </ul> </li> <li>▪ The assessment must be conducted by an independent third-party Auditor with experience outlined in the <i>Framework for Independent Assessment</i>. Among the experience required include familiarity with National Institute of Standards and Technology (NIST) standards, the Health Insurance Portability and Accountability Act (HIPAA), and other applicable federal privacy and cybersecurity regulations and guidance.:</li> <li>▪ Alternatively, the Web-broker may reference existing audit results that address some or all of the assessment's requirements, assuming the existing audit results were produced by a third-party Auditor in conformity with the requirements described above. <ul style="list-style-type: none"> <li>○ If existing audit reports do not address all required elements of the assessment, the remaining elements must be addressed utilizing one of the first two assessment options.</li> <li>○ If existing audit reports are utilized, the reports must have been based on assessment activities completed within the last year.</li> </ul> </li> <li>▪ The SAR should not include comments that describe the third-party assessor's process for verifying the requirement, unless there is a specific issue or concern with respect to the requirement that warrants raising the concern to CMS.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the Entity-specific DE/EDE PME site using the SAR template on CMS zONE<sup>12</sup></li> <li>▪ Only one final report should be submitted to CMS. Unless CMS has provided comments and/or requested edits to the original submission and requested a revised resubmission, no additional reports should be submitted.</li> </ul>
<b>Annual Penetration Testing</b>	<ul style="list-style-type: none"> <li>▪ The penetration test must include the DE Environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the Entity-specific DE/EDE PME site with the SAR</li> </ul>
<b>Network and Component Vulnerability Scans</b>	<ul style="list-style-type: none"> <li>▪ A Web-broker must submit the most recent three (3) months of its Vulnerability Scan Reports.</li> <li>▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&amp;M (the POA&amp;M is expected to be updated monthly, if applicable, but only submitted as indicated in the following row unless additional submissions are requested by CMS).</li> <li>▪ Similar findings can be consolidated.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via web-broker's entity-specific DE/EDE PME site with the SAR</li> </ul>
<b>Plan of Action and Milestones (POA&amp;M)</b>	<ul style="list-style-type: none"> <li>▪ Submit a POA&amp;M if its third-party assessor identifies any privacy and security compliance issues in the SAR.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the web-broker's entity-specific DE/EDE PME site using</li> </ul>

<sup>12</sup> Documents, templates, and other materials will be posted at the following link on CMS zONE:  
<https://zone.cms.gov/document/privacy-and-security-audit>.

Document	Description	Submission Requirements
	<ul style="list-style-type: none"> <li>▪ Ensure all open findings from the SAR have been incorporated into the POA&amp;M.</li> <li>▪ Explain if and how findings from the SAR were consolidated on the POA&amp;M; include SAR reference numbers, if applicable.</li> <li>▪ Ensure the weakness source references each source in detail to include type of audit/assessment and applicable date range.</li> <li>▪ Ensure the weakness description is as detailed as possible to include location/server/etc., if applicable.</li> <li>▪ Ensure scheduled completion dates, milestones with dates, and appropriate risk levels are included.</li> </ul>	the POA&M template on CMS zONE with the SAR
<b>Non-Exchange Entity System Security and Privacy Plan (NEE SSP) – if requested</b>	<ul style="list-style-type: none"> <li>▪ The NEE SSP must include complete and detailed Information about the Prospective or Existing Web-broker's implementation specifications of required security and privacy controls.</li> <li>▪ The implementation of security and privacy controls must be completely documented in the SSP before the audit is initiated.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Web-brokers are not required to submit the NEE SSP to CMS. However, CMS may request and review the NEE SSP.</li> <li>▪ If requested to submit, Web-brokers must use the NEE SSP template on CMS zONE.</li> </ul>
<b>Risk Acceptance Form</b>	<ul style="list-style-type: none"> <li>▪ Ensure accepted risks are documented using the Risk Acceptance Form and submitted with the POA&amp;M during the regular POA&amp;M submission schedule<sup>13</sup>.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submit via the web-broker's entity-specific DE/EDE PME site using the Risk Acceptance Form on CMS zONE with the POA&amp;M.</li> </ul>

- (7) Submission of SPA to CMS. The Web-broker must submit the SPA electronically in a format specified by CMS during the Agreement renewal or initial onboarding process, but no later than June 30, for Existing and Prospective Web-brokers, to mitigate risk of any delay in completing the onboarding process and/or participation in the open enrollment period (OEP) as defined in Section VI.a of this Agreement. Web-brokers must submit applicable SPA documentation in accordance with the ISCM Strategy Guide throughout the term of the Agreement.
- (8) CMS Review of Web-broker SPA Submission. CMS will review the Web-broker's SPA submission. If the SPA indicates that the Web-broker has not sufficiently implemented any identified required control(s), CMS will require remedial action. A Web-broker that does not submit the required SPA documentation or implement any required remedial actions may be subject to the Termination with Cause provision (Section VIII.b) of this Agreement or prohibited from executing the subsequent plan year's Agreement. In addition, CMS may delay providing final approval or may withdraw prior approval of Web-broker's DE Environment if the Web-broker does not address to the reasonable satisfaction of CMS findings suggesting significant security or privacy risks.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

<sup>13</sup> The *Risk Acceptance Form* is available on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

### Appendix C: Definitions

This Appendix defines terms that are used in the Agreement and other Appendices. Any capitalized term used in the Agreement or Appendices that is not defined therein or in this Appendix has the meaning provided in 45 C.F.R. § 155.20.

- (1) **Advance Payments of the Premium Tax Credit (“APTC”)** has the meaning set forth in 45 C.F.R. § 155.20.
- (2) **Affordable Care Act (“ACA”)** means the Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), which are referred to collectively as the Affordable Care Act or ACA.
- (3) **Agent or Broker** has the meaning set forth in 45 C.F.R. § 155.20.
- (4) **Agent or Broker Direct Enrollment Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.
- (5) **Applicant** has the meaning set forth in 45 C.F.R. § 155.20.
- (6) **Auditor** means a person or organization that meets the requirements set forth in this Agreement and contracts with a Direct Enrollment (DE) Entity for the purposes of conducting an Operational Readiness Review (ORR) in accordance with 45 C.F.R. §§ 155.220(c)(6) and 155.221(b)(4) and (f), this Agreement and CMS-issued guidance.
- (7) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in the Agreement that incorporates this Appendix C: Definitions.
- (8) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 C.F.R. § 155.227.
- (9) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information (“PII”) or (2) an authorized user accesses or potentially accesses PII for anything other than an authorized purpose.
- (10) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (“CMS”).
- (11) **Certified Application Counselor** means an organization, staff person, or volunteer meeting the requirements set forth in 45 C.F.R. § 155.225.
- (12) **Classic Direct Enrollment (“Classic DE”)** means, for the purposes of this Agreement, the original version of Direct Enrollment, which utilizes a double redirect from a Direct Enrollment (DE) Entity’s website to HealthCare.gov where the eligibility application is submitted and an eligibility determination is received, and back to the DE Entity’s website for Qualified Health Plan (“QHP”) shopping and plan selection consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(i), 155.221, 156.265 and/or 156.1230(b).



- (13) **Classic Direct Enrollment Pathway (“Classic DE Pathway”)** means, for the purposes of this Agreement, the application and enrollment process used by Direct Enrollment (DE) Entities for Classic DE.
- (14) **CMS** means the Centers for Medicare & Medicaid Services.
- (15) **CMS Companion Guides** means a CMS-authored guide, available on the CMS website, which is meant to be used in conjunction with and supplement relevant implementation guides published by the Accredited Standards Committee.
- (16) **CMS Data Services Hub (“Hub”)** is the CMS federally-managed service to interface data among connecting entities, including HHS, certain other federal agencies, and State Medicaid agencies. The Hub is not available for the Small Business Health Options Program (SHOP).
- (17) **CMS Data Services Hub Web Services (“Hub Web Services”)** means business and technical services made available by CMS to enable the determination of certain eligibility and enrollment or federal financial payment data through the Federally-facilitated Exchange (“FFE”) website, including the collection of personal and financial information necessary for Consumer, Applicant, Qualified Individual, or Enrollee account creations; Qualified Health Plan (“QHP”) application submissions; and Insurance Affordability Program eligibility determinations. The Hub Web Services are not available for the Small Business Health Options Program (SHOP).
- (18) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (“QHP”) offered through an Exchange or Insurance Affordability Program, or whom an Agent, Broker, or Web-broker registered with the FFE, Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a QHP, applying for APTC and CSRs, and/or completing enrollment in a QHP through the FFEs or State-based Exchanges on the Federal Platform (“SBE-FPs”) for individual market coverage.
- (19) **Cost-sharing Reductions (“CSRs”)** has the meaning set forth in 45 C.F.R. § 155.20.
- (20) **Customer Service** means assistance regarding eligibility and Health Insurance Coverage provided to a Consumer, Applicant, or Qualified Individual, including, but not limited to, responding to questions and complaints; providing information about eligibility; applying for APTC and CSRs, and Health Insurance Coverage; and explaining enrollment processes in connection with the FFEs. Includes assistance provided to Qualified Employers and Qualified Employees regarding FF-SHOP and SBE-FP SHOP coverage.
- (21) **Day or Days** means calendar days unless otherwise expressly indicated in the relevant provision of the Agreement that incorporates this Appendix C: Definitions.
- (22) **Designated Representative** means an Agent or Broker that has the legal authority to act on behalf of the Web-broker.
- (23) **Direct Enrollment (“DE”)** means, for the purposes of this Agreement, the process by which a Direct Enrollment (DE) Entity may assist an Applicant or Enrollee with enrolling in a QHP in a manner that is considered through the Exchange consistent with applicable requirements in 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or



156.1230. Direct Enrollment is the collective term used when referring to both Classic Direct Enrollment and Enhanced Direct Enrollment.

- (24) **Direct Enrollment (“DE”) End-User Experience** means all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions under this Agreement.
- (25) **Direct Enrollment (“DE”) Entity** has the meaning set forth in 45 C.F.R. § 155.20.
- (26) **Direct Enrollment (DE) Entity Application Assisters** has the meaning set forth in 45 C.F.R. § 155.20.
- (27) **Direct Enrollment (“DE”) Environment** means an Information technology application or platform provided, owned, and maintained by a DE Entity through which a DE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee Information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.
- (28) **Enhanced Direct Enrollment (“EDE”)** means, for purposes of this Agreement, the version of Direct Enrollment which allows Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals’ legal representatives or Authorized Representatives—to complete all steps in the application, eligibility and enrollment processes on an EDE Entity’s website consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(ii), 155.221, 156.265 and/or 156.1230(b) using application programming interfaces (APIs) as provided, owned, and maintained by CMS to transfer data between the Exchange and the EDE Entity’s website.
- (29) **Enhanced Direct Enrollment (“EDE”) Entity** means a DE Entity that has been approved by CMS to use the Enhanced Direct Enrollment (EDE) Pathway.
- (30) **Enhanced Direct Enrollment (“EDE”) Pathway** means the APIs and functionality comprising the systems that enable EDE as provided, owned, and maintained by CMS.
- (31) **Enrollee** has the meaning set forth in 45 C.F.R. § 155.20.
- (32) **Exchange** has the meaning set forth in 45 C.F.R. § 155.20.
- (33) **Existing Web-broker** means a Web-broker that completes the Web-broker Agreement renewal process in order to maintain its status as a Web-broker and continue operating for the plan year that occurs within the term of this Agreement.
- (34) **Federally-facilitated Exchange (“FFE”)** means an **Exchange** (or **Marketplace**) established by the Department of Health and Human Services (HHS) and operated by CMS under Section 1321(c)(1) of the ACA for individual or small group market coverage, including the Federally-facilitated Small Business Health Options Program (**FF-SHOP**). **Federally-facilitated Marketplaces (FFMs)** has the same meaning as FFEs.

- (35) **Health Insurance Coverage** has the meaning set forth in 45 C.F.R. § 155.20.
- (36) **Health Insurance Exchanges Program (“HIX”)** means the System of Records that CMS uses in the administration of the FFE. As a System of Records, the use and disclosure of the SORN Records maintained by the HIX must comply with the Privacy Act of 1974, the implementing regulations at 45 C.F.R. Part 5b, and the “routine uses” that were established for the HIX in the Federal Register at 78 FR 8538 (February 6, 2013), and amended by 78 FR 32256 (May 29, 2013) and 78 FR 63211 (October 23, 2013).
- (37) **HHS** means the United States Department of Health & Human Services.
- (38) **Health Insurance Portability and Accountability Act (“HIPAA”)** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and its implementing regulations.
- (39) **Incident** or **Security Incident**, has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and means an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of Information or an Information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- (40) **Information** means any communication or representation of knowledge, such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
- (41) **Insurance Affordability Program** means a program that is one of the following:
  - (1) A State Medicaid program under title XIX of the Social Security Act.
  - (2) A State Children’s Health Insurance Program (“CHIP”) under title XXI of the Social Security Act.
  - (3) A State basic health program established under section 1331 of the Patient Protection and Affordable Care Act.
  - (4) A program that makes coverage in a Qualified Health Plan (“QHP”) through the Exchange with APTC established under section 36B of the Internal Revenue Code available to Qualified Individuals.
  - (5) A program that makes available coverage in a QHP through the Exchange with CSRs established under section 1402 of the ACA.
- (42) **Issuer** has the meaning set forth in 45 C.F.R. § 144.103.
- (43) **Non-Exchange Entity** has the meaning at 45 C.F.R. § 155.260(b)(1), and includes, but is not limited, to Qualified Health Plan (“QHP”) Issuers, Navigators, Agents, Brokers, and Web-brokers.
- (44) **OMB** means the Office of Management and Budget.
- (45) **Personally Identifiable Information (“PII”)** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other Information that is linked or linkable to a specific individual.

- (46) **Prospective Web-broker** is an entity seeking to become a Web-broker that does not have an executed Web-broker Agreement for the current plan year.
- (47) **Qualified Employer** has the meaning set forth in 45 C.F.R. § 155.20.
- (48) **Qualified Employee** has the meaning set forth in 45 C.F.R. § 155.20
- (49) **Qualified Health Plan (“QHP”)** has the meaning set forth in 45 C.F.R. § 155.20.
- (50) **Qualified Health Plan (“QHP”) Issuer** has the meaning set forth in 45 C.F.R. § 155.20.
- (51) **Qualified Individual** has the meaning set forth in 45 C.F.R. § 155.20.
- (52) **Security Control** means a safeguard or countermeasure prescribed for an Information system or an organization designed to protect the confidentiality, integrity, and availability of its Information and to meet a set of defined security requirements.
- (53) **State** means the State that has licensed the Agent, Broker, Web-broker, or Issuer that is a party to this Agreement and in which the Agent, Broker, Web-broker or Issuer is operating.
- (54) **State-based Exchange (“SBE”)** means an Exchange established by a State that receives approval to operate under 45 C.F.R. § 155.105. **State-based Marketplace (“SBM”)** has the same meaning as SBE.
- (55) **State-based Exchange on the Federal Platform (“SBE-FP”)** means an Exchange established by a State that receives approval under 45 C.F.R. § 155.106(c) to utilize the federal platform to support select eligibility and enrollment functions. **State-based Marketplace on the Federal Platform (“SBM-FP”)** has the same meaning as SBE-FP.
- (56) **System of Records** means a group of Records under the control of any federal agency from which Information is retrieved by name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
- (57) **System of Records Notice (“SORN”)** means a notice published in the Federal Register notifying the public of a System of Records maintained by a federal agency. The notice describes privacy considerations that have been addressed in implementing the system.
- (58) **System of Record Notice (“SORN”) Record** means any item, collection, or grouping of Information about an individual that is maintained by an agency, including, but not limited to, that individual’s education, financial transactions, medical history, and criminal or employment history and that contains that individual’s name, or an identifying number, symbol, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph, that is part of a System of Records.
- (59) **Web-broker** has the meaning set forth in 45 C.F.R. § 155.20.

### **Appendix D: Standards for Communication with the Hub**

The CMS Data Services Hub (“Hub”) and Hub Web Services are not available for the Small Business Health Options Program (SHOP). Therefore, this Appendix is not applicable to Web-broker participation in SHOP. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

- (1) Web-broker must possess a unique Partner ID assigned by the Centers for Medicare & Medicare Services (“CMS”). Web-broker must use its unique Partner ID when interacting with the Hub and the Direct Enrollment (“DE”) Application Program Interfaces (“APIs”) for Web-broker’s own line of business.
- (2) If Web-broker provides a DE Environment to an Issuer for the exclusive use of enrollment in that Issuer’s plans, the Web-broker must ensure that each Issuer maintains its own, unique Partner ID with the Hub.
- (3) Web-broker must complete testing for each Hub-related transaction it will implement, and it shall not be allowed to exchange data with CMS in production mode until testing is satisfactorily passed, as determined by CMS in its sole discretion. Successful testing generally means the ability to pass all applicable Health Insurance Portability and Accountability Act (“HIPAA”) of 1996 compliance standards, or other CMS-approved standards, and to process electronic data and Information transmitted by Web-broker to the Hub. The capability to submit these test transactions will be maintained by Web-broker throughout the term of this Agreement.
- (4) Transactions must be formatted in accordance with the Accredited Standards Committee Implementation Guides adopted under HIPAA, available at <http://store.x12.org/store/>, as applicable and appropriate for the type of transaction. CMS will make available Companion Guides for the transactions, which specify necessary situational data elements.
- (5) Web-broker agrees to abide by the applicable policies affecting electronic data interchange submissions and submitters as published in any of the guidance documents related to the CMS Federally-facilitated Exchange (“FFE”) or Hub, as well as applicable standards in the appropriate CMS Manual(s) or CMS Companion Guide(s), as published on the CMS website. These materials can be found at <https://www.cms.gov/ccii/resources/regulations-and-guidance/downloads/companion-guide-for-ffe-enrollment-transaction-v15.pdf> and <http://www.cms.gov/ccii/resources/regulations-and-guidance/index.html>.
- (6) Web-broker agrees to submit test transactions to the Hub prior to the submission of any transactions to the FFE production system and to determine that the transactions and responses comply with all requirements and specifications approved by the CMS and/or the CMS contractor.<sup>14</sup>

---

<sup>14</sup> While CMS owns data in the FFE, contractors operate the FFE system in which the enrollment and financial management data flow. Contractors provide the pipeline network for the transmission of electronic data, including

- (7) Web-broker agrees that prior to the submission of any additional transaction types to the FFE production system, or as a result of making changes to an existing transaction type or system, it will submit test transactions to the Hub in accordance with paragraph (2) above.
- (8) If Web-broker enters into relationships with other affiliated entities, or their authorized designees for submitting and receiving FFE data, it must execute contracts with such entities stipulating that such entities and any of its subcontractors or affiliates must utilize software tested and approved by Web-broker as being in the proper format and compatible with the FFE system. Entities that enter into contract with Web-broker and access Personally Identifiable Information (“PII”) are required to maintain the same or more stringent security and privacy controls as Web-broker.
- (9) Pursuant to 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f), Web-broker must successfully complete an Operational Readiness Review (“ORR”) to the satisfaction of CMS before Web-broker is able to submit any transactions to the FFE production system or agrees that CMS may require further reviews or corrective actions at any time during the term of this Agreement. The ORR will assess Web-broker’s compliance with CMS’ regulatory and contractual requirements, to include the critical Privacy and Security Controls. This Agreement may be terminated or access to CMS systems may be denied for a failure to comply with ORR requirements or if, at the sole discretion of CMS, the results are unsatisfactory.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

---

the transport of Exchange data to and from the Hub and Web-broker so that Web-broker may discern the activity related to enrollment functions of persons they serve. Web-broker may also use the transported data to receive descriptions of financial transactions from CMS.

**Appendix E: Auditor Identification**

Web-broker agrees to identify, in Part I below, all Auditors selected to complete the annual security and privacy assessment (SPA) and any subcontractors of the Auditor(s), if applicable. In the case of multiple Auditors, please indicate the role of each Auditor in completing the SPA. Include additional sheets, if necessary. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

**TO BE FILLED OUT BY WEB-BROKER**

**I. Complete These Rows to Identify Auditors Selected to Complete SPA**

Printed Name and Title of Authorized Official of Auditor 1	<b>Shibani Gupta</b>
Auditor 1 Business Name	Abssurance
Auditor 1 Address	5300 Ranch Point, Katy, TX 77494
Printed Name and Title of Contact of Auditor 1 (if different from Authorized Official)	
Auditor 1 Contact Phone Number	
Auditor 1 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	Auditor - Business and Privacy & Security Audits
Printed Name and Title of Authorized Official of Auditor 2	
Auditor 2 Business Name	
Auditor 2 Address	
Printed Name and Title of Contact of Auditor 2 (if different from Authorized Official)	
Auditor 2 Contact Phone Number	
Auditor 2 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	

**Appendix F: Conflict of Interest Disclosure Form**

**TO BE FILLED OUT BY WEB-BROKER**

Web-broker must disclose to the Department of Health & Human Services (HHS) any financial relationships between the Auditor(s) identified in Appendix E: Auditor Identification of this Agreement, and individuals who own or are employed by the Auditor(s), and individuals who own or are employed by a Web-broker for which the Auditor(s) is conducting an annual security and privacy assessment (SPA) pursuant to Appendix A: Privacy and Security Standards for Web-brokers of this Agreement and 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f). Web-broker must disclose any affiliation that may give rise to any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

Please describe below any relationships, transactions, positions (volunteer or otherwise), or circumstances that you believe could contribute to a conflict of interest:

- Web-broker has no conflict of interest to report for the Auditor(s) identified in Appendix E: Auditor Identification.
- Web-broker has the following conflict of interest to report for the Auditor(s) identified in Appendix E: Auditor Identification:

1. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
2. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
3. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# **Exhibit I**



**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**



**Centers for Medicare & Medicaid Services**

**INTERCONNECTION SECURITY AGREEMENT (ISA)  
BETWEEN  
CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)  
AND  
ENHANCED DIRECT ENROLLMENT (EDE) ENTITY  
Benefitalign LLC**

**ISA Version 1.0**

**10/16/2023**

The following Benefitalign LLC ISA Change Log is maintained to record all changes since the last submission.

## Record of Changes

Version	Date	Author / Owner	Description of Change	CR #
0.1	10/04/2023	Security officer	Baselined	
0.2	10/16/2023	Infrastructure Manager	Updated Sec 3.2, Appendix A and B as per current information	
1.0	10/19/2023	CISO	Reviewed, Approved and Released	

CR: Change Request

## Table of Contents

<b>1. Introduction</b>	<b>1</b>
<b>2. CMS Background</b>	<b>2</b>
2.1 CMS	2
2.2 CMS Information Security Program	2
2.3 CMS Roles and Responsibilities	2
2.3.1 CMS Chief Information Officer (CIO)	2
2.3.2 CMS Chief Information Security Officer (CISO)	2
2.3.3 CMS Senior Official for Privacy (SOP)	2
2.3.4 CMS Information System Security Officer (ISSO)	2
2.3.5 Center for Consumer Information and Insurance Oversight (CCIIO)	3
2.3.6 CMS Cyber Integration Center (CCIC)	3
<b>3. Non-CMS Organization Background</b>	<b>3</b>
3.1 Beneficialign	3
3.2 IT Security Program	3
3.3 Roles and Responsibilities	4
3.3.1 CISO (Chief Information Security Officer)	4
3.3.2 Privacy Officer	5
3.3.3 Management Information Security Forum (MISF)	6
3.3.4 ISMS Internal Auditor	6
<b>4. Scope</b>	<b>7</b>
<b>5. Authority</b>	<b>7</b>
<b>6. Statement of Requirements</b>	<b>8</b>
6.1 General Information/Data Description	8
6.1.1 CMS Hub Description	8
6.1.2 Beneficialign System Description	9
6.2 Services Offered	11
6.3 Security and Privacy Controls	11
<b>7. Request to Connect</b>	<b>12</b>
7.1 Required Documents	12
<b>8. Security Responsibilities</b>	<b>12</b>
8.1 Communication / Information Security Points of Contact	13
8.2 Responsible Parties	13
<b>9. Personnel / User Security</b>	<b>13</b>
9.1 User Community	13

9.2	Commitment to Protect Sensitive Information.....	14
9.3	Training and Awareness.....	14
9.4	Personnel Changes / De-Registration.....	15
<b>10.</b>	<b>Policies.....</b>	<b>15</b>
10.1	Rules of Behavior.....	15
10.2	Security Documentation.....	15
<b>11.</b>	<b>Network Security.....</b>	<b>16</b>
11.1	Network Management.....	16
11.2	Material Network Changes.....	16
11.3	New Interconnections.....	17
11.4	Network Inventory.....	17
11.5	Firewall Management.....	17
11.6	Penetration Test.....	17
<b>12.</b>	<b>Incident Prevention, Detection, and Response.....</b>	<b>18</b>
12.1	Incident Handling.....	18
12.2	Intrusion Detection.....	19
12.3	Disasters and Other Contingencies.....	19
<b>13.</b>	<b>Notice.....</b>	<b>19</b>
<b>14.</b>	<b>Modifications.....</b>	<b>20</b>
<b>15.</b>	<b>Compliance.....</b>	<b>20</b>
<b>16.</b>	<b>Termination.....</b>	<b>20</b>
<b>17.</b>	<b>Cost Considerations.....</b>	<b>21</b>
<b>18.</b>	<b>Timeline.....</b>	<b>21</b>
<b>19.</b>	<b>Order of Precedence.....</b>	<b>21</b>
<b>20.</b>	<b>Confidentiality.....</b>	<b>21</b>
<b>21.</b>	<b>Survival.....</b>	<b>22</b>
<b>22.</b>	<b>Records.....</b>	<b>22</b>
<b>23.</b>	<b>Assignment and Severability.....</b>	<b>22</b>
<b>24.</b>	<b>Warranty.....</b>	<b>22</b>
<b>25.</b>	<b>Limitation of Liability.....</b>	<b>23</b>
<b>26.</b>	<b>Force Majeure.....</b>	<b>23</b>

---

**27. Signatures ..... 24**

**Appendix A. Responsible Parties ..... 27**

    A.1 Authorizing Official .....27

    A.2 Other Designated Contacts.....27

    A.3 Assignment of Security and Privacy Responsibility .....28

**Appendix B. Primary EDE Entities Connection and Data Sharing with Upstream  
EDE Entities ..... 30**

    B.1 Upstream EDE Entities Overview.....30

    B.2 Data Connections .....31

    B.3 Additional Functionality or Systems.....35

    B.4 Data Flow/Topological Diagram.....39

## List of Figures

Figure 1. EDE Data Flow Diagram.....	9
Figure 2: Data Flow Diagram – Integration with CMS .....	11
Figure 2. AvMed Data Flow/Topological Diagram.....	39
Figure 3. Inshura Data Flow/Topological Diagram.....	40

## List of Tables

Table 1. System Authorizing Official.....	27
Table 2. Information System Management Point of Contact .....	27
Table 3. Information System Technical Point of Contact.....	27
Table 4. EDE Entity Name Internal ISSO (or Equivalent) Point of Contact.....	28
Table 5. EDE Entity Internal Official for Privacy (or Equivalent) Point of Contact.....	28
Table 6. CMS ISSO Point of Contact .....	29
Table 7. Record of Changes for Appendix B.....	30
Table 8. Upstream EDE Entity Overview.....	30
Table 9. Interconnections and Data Exchange Between EDE Environment Provider and Upstream Entities.....	32
Table 10. Additional Functionality or Systems .....	37

# 1. Introduction

The purpose of this Interconnection Security Agreement (ISA) is to establish procedures for mutual cooperation and coordination between the Centers for Medicare & Medicaid Services (CMS) and the Enhanced Direct Enrollment (EDE) Entity,<sup>1</sup> Benefitalign LLC (hereafter referenced as the “Non-CMS Organization”), regarding the development, management, operation, and security of a connection between CMS’s Data Service Hub (Hub) (hereafter known as the CMS Network) and the Non-CMS Organization’s network. This ISA is intended to minimize security risks and ensure the confidentiality, integrity, and availability (CIA) of CMS information<sup>2</sup> as well as the information that is owned by the external organization that has a network interconnection<sup>3</sup> with CMS. This ISA ensures the adequate security<sup>4</sup> of CMS information being accessed and provides that all network access satisfies the mission requirements of both CMS and the Non-CMS Organization (hereafter referenced as “both parties”).

Federal policy requires agencies to develop ISAs for federal information systems and networks that share or exchange information with external information systems and networks. This ISA is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Rev. 1, *Managing the Security of Information Exchanges*,<sup>5</sup> and shall comply with the security required by Federal Acquisition Regulation (FAR) clause 52.239-1, *Privacy or Security Safeguards*. The guidelines establish information security (IS) measures that shall be taken to protect the connected systems and networks and shared data. CMS Information Technology (IT) managers and IS personnel shall comply with the NIST guidelines in managing the process of interconnecting information systems and networks.

This ISA documents interconnection arrangements and IS responsibilities for both parties, outlines security safeguards, and provides the technical and operational security requirements. This ISA also specifies business and legal requirements for the information systems and networks being interconnected. This ISA authorizes mutual permission to connect both parties and establishes a commitment to protect data that is exchanged between the networks or processed and stored on systems that reside on the networks. Through this ISA, both parties shall minimize the susceptibility of their connected systems and networks to IS risks and aid in mitigation and recovery from IS incidents.

---

<sup>1</sup> EDE Entities are considered Non-Exchange Entities (NEE) and, as such, are required to comply with the privacy and security standards that are at least as protective as the standards the Exchange has established and implemented for itself.

<sup>2</sup> “Information” is defined as “any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.” (Executive Order 12958)

<sup>3</sup> “Network interconnection” is defined as the primary “direct connection of two or more IT networks for the purpose of sharing data and other information resources.” (This is based on the definition of system interconnection in NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.)

<sup>4</sup> “Adequate security” is defined as “a level of security that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information.” (Office of Management and Budget [OMB] Circular A-130)

<sup>5</sup> Located at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-47r1.pdf>.

## 2. CMS Background

### 2.1 CMS

As an Operating Division of the Department of Health and Human Services (HHS), CMS administers Medicare, Medicaid, and the Children’s Health Insurance Program (CHIP), as well as programs created under the Patient Protection and Affordable Care Act (PPACA) of 2010, including the Health Insurance Exchange program. It is CMS’ mission to ensure effective, up-to-date healthcare coverage and to promote quality care for beneficiaries.

### 2.2 CMS Information Security Program

The CMS IS Program helps CMS accomplish its mission by ensuring the CIA of CMS information resources. The CMS IS Program has developed policies, standards, procedures, and guidelines that ensure the adequate protection of agency information and comply with federal laws and regulations. CMS monitors the security of its network twenty-four (24) hours a day, seven (7) days a week (i.e., 24/7) through various management, operational, and technical processes. Training initiatives are continuously updated to ensure that managers, users, and technical personnel are aware that they are responsible for the adequate security of their information systems.

### 2.3 CMS Roles and Responsibilities

#### 2.3.1 CMS Chief Information Officer (CIO)

The CMS CIO is responsible for the overall implementation and administration of the CMS Information Security and Privacy Program.

#### 2.3.2 CMS Chief Information Security Officer (CISO)

The CMS CISO supports the CMS CIO in the implementation of the CMS Information Security Program. The CMS CISO directs, coordinates, and evaluates CMS’s Information Security policy. The CISO collaborates with the CMS Senior Official for Privacy to carry out Information Security and Privacy responsibilities.

#### 2.3.3 CMS Senior Official for Privacy (SOP)

The CMS SOP carries out the CIO’s privacy responsibilities under federal requirements in conjunction with the CISO. The CMS SOP leads CMS privacy programs and promotes proper information security and privacy practices and is responsible for the development and implementation of privacy policies and procedures.

#### 2.3.4 CMS Information System Security Officer (ISSO)

The CMS ISSO is the liaison for IS within their assigned area of responsibility. ISSOs implement standard IS policies and collaborate across CMS concerning the CIA of information resources. Although the ISSOs report directly to their own management, they have responsibilities to the CMS CISO as part of their IS responsibilities, and therefore, to the CMS



CIO. In their IS role, ISSOs take direction from the CMS CIO or the CMS CISO when action is required to protect CMS assets from potential vulnerabilities and threats. The CMS CISO and ISSOs will work with Non-CMS Organization to enhance IS measures.

### **2.3.5 Center for Consumer Information and Insurance Oversight (CCIO)**

The CCIO, as the CMS Business Owner (BO), is responsible for the management and oversight of CMS's Health Insurance Exchange Hub system, which is the CMS information system that requires the interconnection with the Non-CMS Organization. The BO serves as the primary point of contact (POC) for the CMS information system.

### **2.3.6 CMS Cyber Integration Center (CCIC)**

The CCIC monitors the security of the CMS information system 24/7 using the expertise of Information Technology (IT) security professionals and automated IS processes. The CCIC identifies IS incidents, characterizes the nature and severity of incidents, and provides immediate diagnostic and corrective actions when appropriate. CCIC members are trained in investigating IS events such as web defacements, computer compromises, and viruses. The CCIC continuously enhances its IS auditing methods as well as incident handling procedures to respond to the growing demands of IS.

## **3. Non-CMS Organization Background**

### **3.1 Benefitalign**

As a technology leader, Benefitalign is serving the health insurance and employee benefits industry. We have developed software products to help independent brokers compete more effectively by utilizing the best technology to provide customers what they want. Our Quote to Card solutions simplifies the health insurance search and enrolment process, and can help brokers achieve their business objectives more quickly and at a lower cost.

Benefitalign cloud-based platform is scalable, easy to manage, customizable, designed to attract and connect with members for Health Information Exchange (HIX) and consumer centric health plan sites.

Benefit administration feature enables online sales and marketing across all channels such as retail, brokers, direct sales - all from one platform.

Our solution enables streamlined end-to-end benefit plan management including Internal employees (health plans/carriers and brokers) and External customers (individuals and groups).

### **3.2 IT Security Program**

Other than the NIST controls as mandated by CMS Benefitalign LLC is certified for:

- **SOC 2 Type 2** attestation implies Benefitalign's adherence to implementing effective internal controls for ensuring the security and privacy. It also checks the design and operating effectiveness over a period of time (typically, 6/12 months).

- **ISO 27001:2022-** Standard provides a framework and guidelines for establishing, implementing and managing an Information Security Management Systems (ISMS). This provides Benefitalign with a systematic approach to documentation, management responsibility, internal audits, device corrective and preventive action and continual improvement of CIA posture.
- **PCI DSS 3.2.1 SAQ-D** - Payment Card Industry Data Security Standard. help secure and protect the entire payment card ecosystem (process or transmit credit card data). Achieve compliance to safeguard organizations from cyber threats.

Benefitalign has policies, process and procedures implemented in line with above standards and maintains strict compliance.

Threats and vulnerabilities in our organization's information assets are evaluated and analyzed. Vulnerability assessments and penetration testing is performed yearly/half yearly/quarterly as required, in addition, we proactively use the Nessus tool monthly to scan our internal networks and servers. To mitigate any security risks, we also ensure timely updates of software patches.

The SSP is the primary document used for describing Benefitalign's IT systems and supporting application(s) security and privacy environment and for documenting the implementation of security and privacy controls for the protection of all data received, stored, processed, and transmitted by the ACA support IT systems and supporting applications.

All our employees are made aware of and constantly reminded of the importance of information security and data protection practices, which include the establishment and implementation of control measures and procedures to minimize IS risks.

Authentication, authorization, and accountability procedures are established for issuing and revoking user accounts. It specifies how users authenticate, create passwords, aging requirements and audit trail maintenance.

Virus protection measures are taken to protect against viruses, which include maintaining workstation-based products, email scanning, web-content filtering, and file transfers for malicious content.

We have comprehensive Disaster Recovery and Business Continuity plans to respond to various man-made or natural disaster scenarios.

### 3.3 Roles and Responsibilities

Benefitalign's Information Security (IS) organization's leadership roles equivalent to CMS roles and are responsible for implementing IT and IS policies, procedures, and tools that support CIA are defined as follows:

#### 3.3.1 CISO (Chief Information Security Officer)

- Direct and approve the design of security systems.
- Ensure that disaster recovery and business continuity plans are in place, tested, and event ready.

- Review and approve security policies, controls and cyber incident response planning. • Approve identity and access control policies.
- Review investigations after breaches or incidents - including impact analysis and recommendations for avoiding similar vulnerabilities.
- Maintain a current understanding of the IT threat landscape for the industry.
- Ensure compliance with changing laws and applicable regulations and translate such knowledge for identification of risks and actionable plans to protect the business.
- Schedule periodic security audits.
- Oversee identity and access management.
- Make sure that cyber security policies and procedures are communicated to all personnel and that compliance is enforced.
- Manage all teams - employees, contractors and vendors involved in IT security, which may include hiring.
- Provide training and mentoring to security team members.
- Constantly update and tweak the cyber security strategy to leverage new technology and threat information.
- Brief the executive team on status and risks, including taking the role of champion for the overall strategy and necessary budget.
- Communicate best practices and risks to all the areas of business.

### 3.3.2 Privacy Officer

- Establish, coordinate, and lead the Privacy Governance.
- Perform privacy risk assessments and related compliance monitoring initiatives.
- Ensure that the organization maintains appropriate privacy and confidentiality consent, authorization forms, information notices and materials reflecting the organization's policies and regulatory compliance requirements.
- Oversee, direct, and deliver privacy training and orientation to all employees.
- Establish a procedure to track access to PHI that can be reviewed during audits.
- Implement a process for receiving, documenting, tracking, investigating, and acting on all complaints concerning breaches in privacy policies and procedures.
- Ensure that all employees are acting in total compliance with privacy policies and procedures and deploy sanctions in the event of a breach.
- Work with all personnel involved in the release of PHI to ensure full co-ordination and co-operation under policies and procedures and federal HIPAA compliance and regulation.

- Maintain up-to-date knowledge of federal and state privacy laws and HIPAA compliance and regulations

### 3.3.3 Management Information Security Forum (MISF)

The team comprises of functional heads representing different entities within the organization.

- Review security policies and recommend for approval.
- Conduct department level Risk Assessment and Treatment.
- Review organization level Risk Assessment and Treatment.
- Promote and implement security policies.
- Evaluate information security incidents.
- Develop and test departmental level Business Continuity Plans.

### 3.3.4 ISMS Internal Auditor

- Conduct timely implementation of risk-based internal audits as directed by controller complying with annual audit plan.
- Assist on various audit projects and matters and ensure to have initial focus on revenue assurance.
- Conduct risk evaluation of assigned functional area or department in established timeframe.
- Implement internal audit tasks in areas of risk management and internal control.
- Perform all assigned audit assignment at financial, operational and administrative processes and systems.
- Evaluate internal audit suitability, efficiency, cost-effectiveness and internal controls effectiveness.
- Identify level of conformance with established rules, regulations, policies and procedures.
- Examine validity and reliability of financial, accounting and other data and report any deviations.
- Participate in audit engagement planning, reporting, scoping, execution and follow-up as defined.
- Study and learn Company's policy and procedures.
- Evaluate comprehensive business processes and transactions to analyze productiveness of controls and risk alleviation.
- Identify internal audit control environment enhancement opportunities.
- Conduct testing adhering with accreditation and varied regulatory requirements.
- Support development of internal audit programs for operational audits and special reviews etc.

## 4. Scope

The scope of this ISA is based on, but is not limited to, the following activities, users, and components:

- Interconnection between a CMS information system(s) and the Non-CMS Organization.
- Existing and future users, including employees from both parties, contractors, and subcontractors at any tier; and other federally and non-federally funded users managing, engineering, accessing, or utilizing the Non-CMS Organization Network.
- Related network components belonging to both parties, such as hosts, routers, and switches; IT devices that assist in managing security such as firewalls, intrusion detection systems (IDS), and vulnerability scanning tools; desktop workstations; servers; and major applications (MA) that are associated with the network connection between both parties.<sup>6</sup>

## 5. Authority

By connecting with the CMS network and CMS information system, the Non-CMS Organization agrees to be bound by this ISA and use the CMS Network and CMS information system(s) in compliance with this ISA.

The authority for this ISA is based on, but not limited to, the following, if and to the extent applicable:

- Federal Information Security Modernization Act of 2014 (FISMA);
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems;
- 18 U.S.C. § 641 Criminal Code: Public Money, Property or Records;
- 18 U.S.C. § 1905 Criminal Code: Disclosure of Confidential Information;
- Privacy Act of 1974, 5 U.S.C. § 552a;
- Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191;
- 45 C.F.R. § 155.260 Privacy and Security of Personally Identifiable Information;
- 45 C.F.R. § 155.280 Oversight and Monitoring of Privacy and Security Requirements; and
- Patient Protection and Affordable Care Act of 2010.

---

<sup>6</sup> A “major application” is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. (OMB A-130)

This ISA is also in compliance with HHS policies<sup>7</sup> and CMS policies listed at the CMS IS webpage.<sup>8</sup>

## 6. Statement of Requirements

The expected benefit of the interconnection is as part of its EDE implementation, Benefitalign needs to interface with the Marketplace via CMS' APIs in order to retrieve Eligibility and notices, retrieve data matching issues (DMIs) and/or SEP verification issues (SVIs) and upload documents to resolve those DMIs and/or SVIs as well as submit enrollments. By interfacing with the Marketplace via EDE pathway, Benefitalign can avoid multiple redirections to CMS and partner websites back and forth thereby giving the consumers and brokers a seamless experience of staying on a single platform without any redirection when using the EDE pathway phase 3 integration with CMS systems. The expected benefit of the integration between Benefitalign LLC and CMS via the EDE pathway is to exchange the data with utmost security, confidentiality and integrity. Furthermore, the interconnection will also allow an increase in the number of transactions, reduce maintenance calls, and improve cost efficiencies on support activities. This will lead to increased customer satisfaction thereby resulting in greater sales opportunities for Benefitalign.

### 6.1 General Information/Data Description

#### 6.1.1 CMS Hub Description

All communication with the Hub is facilitated via Web services over the Internet. The Hub conveys information, using Transport Layer Security (TLS), version 1.2 for data encryption, server authentication, and message integrity. It uses Public Key Infrastructure (PKI) to authenticate connections. To protect the confidentiality of data transmitted from one system to another system, messages are encrypted, using the Hypertext Transfer Protocol Secure (HTTPS) protocol.

All Application Programming Interface (API) transactions provided by an EDE Entity will go through the Hub for confirmation that the requesting EDE Entity is authorized by CMS. Upon confirmation, the API request will be passed to the Federally-facilitated Exchange (FFE), at which point the FFE will validate the API request. The groups of services depicted in Figure 1 enable the FFE to provide internal and external stakeholders with the following capabilities:

- **Marketplace Consumer Record (MCR) APIs:** Enable the Exchange to provide customer-related data and search capabilities.
- **Standalone Eligibility Service (SES) APIs:** Enable the Exchange to determine the customer's eligibility for Qualified Health Plans (QHP) and /or Qualified Dental Plans (QDP) and associated subsidies.

<sup>7</sup> Located at: <https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/index.html>.

<sup>8</sup> Located at: <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/>.

- **Issuer and Enrollment Services (IES) APIs:** Enable the Exchange to provide data to redirect consumers to the issuer payment portal.
- **Document Storage and Retrieval Service (DSRS) APIs:** Enable the Exchange to provide document upload and retrieval of Exchange-generated notices.
- **Eligibility and Enrollment (EE) APIs:** Enable the Exchange to provide enrollment generation capabilities.

Figure 1 is a high-level topological diagram illustrating the interconnectivity between the Hub and EDE entity systems.

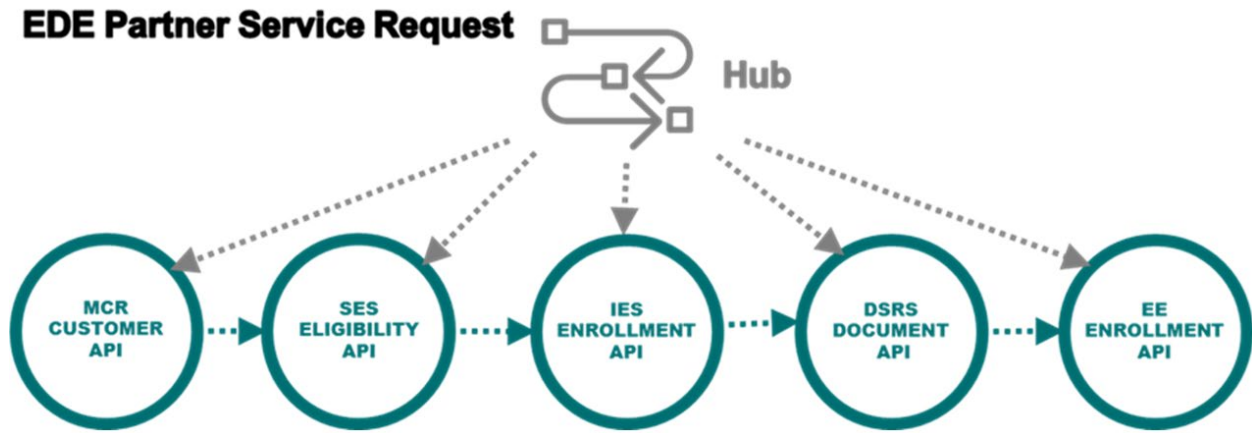


Figure 1. EDE Data Flow Diagram

### 6.1.2 Benefitalign System Description

Benefitalign’s web application BrokerEngage (BE) does not interact with any external third-party APIs other than CMS’ APIs to exchange the data. BE captures data and information which is necessary to invoke the CMS’ APIs. Data is collected from the end user via the BrokerEngage web client and exchanged with CMS using JSON as well as XML format in compliance with CMS guidelines.

The following data are captured from the user and submitted to CMS using the API’s provided by CMS

Data exchanged	API Used to pass to CMS	Notes
First name, last name, SSN, DOB	ID Proofing	
First name, last name, SSN, DOB	Person Search API	
FFM Application Id and Identity Proofing Identifier	Permission API	This API will revoke permission of an application with Identify Proofing Identifier



FFM Application Id	DMI & SVI API	
FFM Application Id and Documents	Document upload API	
DSRS Id (Document Id)	Notice Retrieval API	Based on the document ID, API will return the documents uploaded in CMS
FFM Application Id	Payment Redirect API	Based on the Application ID, the payment URL will be provided by CMS to capture the details from customer.
FFM Application Id	Meta Search API	Based on the Application, all the metadata related to the application is retrieved
Household Contact Information [Name, DOB, Gender, address, phone, email, tobacco usage]  Household Composition [dependent members, tax information, family & legal relationship]  More about household (Sex, SSN, Race/Ethnicity, NonMAGI, Medicaid Block)  Citizenship/Immigration details  Income details	SES Eligibility API's.	
FFM Application ID.	Get Enrollment Fetch Eligibility	
FFM Application ID and details of Exchange Plan, customer has selected to enroll.	Submit Enrollment	

Figure 2 is a high-level topological diagram illustrating the interconnectivity between the BrokerEngage and CMS.



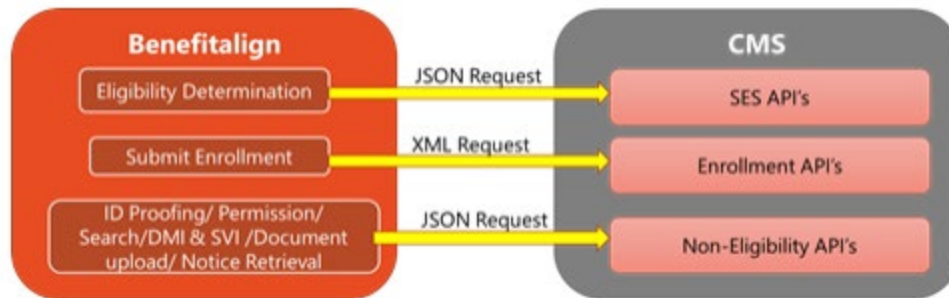


Figure 2: Data Flow Diagram – Integration with CMS

## 6.2 Services Offered

### CMS shall:

- Provide 24/7 operation of the CMS IT Service Desk (1-800-562-1963, 410-786-2580, or [cms\\_it\\_service\\_desk@cms.hhs.gov](mailto:cms_it_service_desk@cms.hhs.gov)) for the Non-CMS Organization POC to communicate any security issues; and
- Provide installation, configuration, and maintenance of CMS edge router(s) with interfaces to multiple CMS core and edge routers.

### Benefitalign shall:

- Provide Customer Service operation from 8AM to 8PM EST Monday through Friday.
- Provide Customer Service Desk over phone (888-556-3382) or through mail ([solutions@benefitalign.com](mailto:solutions@benefitalign.com)) to communicate any network and security related issues.
- Provide functional and technical support for BrokerEngage application.

## 6.3 Security and Privacy Controls

### CMS shall:

- Comply with the latest *CMS Acceptable Risk Safeguards (ARS)*<sup>9</sup>, which are based on the most recent NIST SP 800-53 and HHS policy and standards.

### Benefitalign shall:

- Adhere to the security and privacy requirements specified in the *Non-Exchange Entity (NEE) System Security and Privacy Plan (SSP)* document,<sup>10</sup> which are specifically incorporated herein.

<sup>9</sup> The *CMS Acceptable Risk Safeguards (ARS)* is located at: <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library>.

<sup>10</sup> The *Non-Exchange Entity System Security and Plan (SSP)* is located at: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>.

## 7. Request to Connect

The Non-CMS Organization sends to CMS a completed ISA document and artifacts of compliance with security and privacy control requirements. After review of the ISA, along with all required artifacts and an evaluation of risk, the CMS CIO, or designee, will act on the request to connect to the Hub in writing by signing the ISA or by denying the request. No PII shall pass through any CMS network before the Non-CMS Organization obtains a fully signed ISA.

The Non-CMS Organization must also send to CMS a signed EDE Agreement and meet all requirements set forth in that Agreement before CMS will permit connection to the Hub.

### 7.1 Required Documents

Pursuant to 45 C.F.R. § 155.260, Privacy and Security of Personally Identifiable Information, and 45 C.F.R. § 155.280, Oversight and Monitoring of Privacy and Security Requirements, the Beneficialign shall report, on a continuing basis, the status of their security posture to Beneficialign's authorizing official and CMS. If the Non-CMS Organization does not meet the required reporting timeframes, the ISA may be revoked. Before CMS can make a risk-based decision on the system's ISA, the following agreements and compliance artifacts are required:

1. EDE Agreement;
2. Interconnection Security Agreement (ISA), renewed every year or whenever there is a major change;
3. Security Assessment Report (SAR), performed by an auditor, and Plan of Action & Milestones (POA&M); and
4. Information Security and Privacy Continuous Monitoring (ISCM)<sup>11</sup> artifacts.

## 8. Security Responsibilities

### Both parties shall:

- Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system with the highest sensitivity levels.
- Non-CMS Organization's responsibilities under this provision are in addition to those specified in Section 6.3.

---

<sup>11</sup> The *Non-Exchange Entity (NEE) Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide* is located at: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>.

## 8.1 Communication / Information Security Points of Contact

### Both parties shall:

- Designate a technical lead for their respective network and provide POC information to facilitate direct contacts between technical leads of each party to support the management and operation of the interconnection;
- Maintain open lines of communication between POCs at both the managerial and technical levels to ensure the successful management and operation of the interconnection; and
- Inform their counterpart promptly of any change in technical POCs and interconnections.

### CMS shall:

- Ensure its staff informs their counterparts at the Non-CMS Organization promptly of any change in technical POC and interconnection; and
- Identify a CMS ISSO to serve as a liaison between CMS and the Non-CMS Organization and assist the Non-CMS Organization in ensuring that its IS controls meet or exceed CMS requirements.

### Beneficial shall:

- Designate an IS POC, the equivalent of the CMS ISSO, who shall act on behalf of the Non-CMS Organization and communicate all IS issues involving the Non-CMS Organization to CMS via the CMS ISSO.

## 8.2 Responsible Parties

Appendix A is a list of the responsible parties for each system. Appendix A will be updated whenever necessary. Updating Appendix, A does not require either party to re-sign this ISA. It is the responsibility of each respective approving authority to ensure the timely updating of Appendix A and to notify the alternate party of such changes; each party will use reasonable efforts to do so within thirty (30) days of any material personnel change.

## 9. Personnel / User Security

### 9.1 User Community

#### Both parties shall:

- Ensure that all employees, contractors, and other authorized users with access to the CMS Network and the Non-CMS Organization as well as the data sent and received from either organization are not security risks and meet the personnel security / suitability

requirements of the *CMS Business Partners System Security Manual* (2018)<sup>12</sup> as a guide, which is specifically incorporated herein.

**Beneficial shall:**

- Enforce the following IS best practices:
  - **Least Privilege** – Only authorizing access to the minimal amount of resources required for a function;
  - **Separation of Duties** – A security method that manages conflict of interest, the appearance of conflict of interest, and fraud. It restricts the amount of power held by any one individual; and
  - **Role-Based Security** – Access controls to perform certain operations ("permissions") are assigned to specific roles.

## 9.2 Commitment to Protect Sensitive Information

**Both parties shall:**

- Not release, publish, or disclose information to unauthorized personnel, and shall protect such information in accordance with this ISA, the EDE Agreement, and any other pertinent laws and regulations governing the responsibility to adequately safeguard federal agency systems.

**Beneficial shall:**

- Require that its employees and contractors comply with the security requirements set forth in this ISA, EDE Agreement, and the organization's specific information security policies, standards, and procedures.
- Require that outsourced operations where non-CMS personnel may have access to information, CMS systems, and network components comply with requirements of Federal Acquisition Regulation (FAR) clause 52.239-1, Privacy or Security Safeguards, and CMS IS policies, standards, and procedures, which are specifically incorporated herein.

## 9.3 Training and Awareness

**Both parties shall:**

- Have all users, including employees, contractors, and other authorized users, complete the information security and privacy awareness training on execution of this ISA and then annually thereafter; and

---

<sup>12</sup> The *CMS Business Partners System Security Manual* is located at: [http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/117\\_systems\\_security.pdf](http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/117_systems_security.pdf).

- Train, monitor, and audit staff on requirements related to the authorized use and sharing of PII with third parties, and on the consequences of unauthorized use or sharing of PII.

## 9.4 Personnel Changes / De-Registration

### Both parties shall:

- Provide notification to their respective BOs of the separation or long-term absence of their network owner or technical lead; and
- Provide notification to their respective BO of any changes in the ISSO or POC information.

## 10. Policies

### 10.1 Rules of Behavior

#### CMS shall:

- Ensure that all CMS system users with access to the CMS Network shall adhere to all current *HHS Rules of Behavior*.<sup>13</sup>

#### Beneficial shall:

- Require that all users with access to the Non-CMS Organization's system and its connection with the Hub, adhere to the terms of this ISA and the EDE Agreement executed between the Non-CMS Organization and CMS.
- Require the Non-CMS Organization's Rules of Behavior provide protections that are commensurate with current *HHS Rules of Behavior*.

### 10.2 Security Documentation

#### Both parties shall:

- Ensure that security is planned for, documented, and integrated into the System Life Cycle from the IT system's initiation to the system's disposal. For applicable guidance, please refer to CMS Target Life Cycle<sup>14</sup> and the *CMS Risk Management Handbook*.<sup>15</sup>

<sup>13</sup> Located at: <https://www.hhs.gov/sites/default/files/rules-of-behavior.pdf>.

<sup>14</sup> Located at: <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/TLC>.

<sup>15</sup> Located at: <https://security.cms.gov/learn/cms-security-and-privacy-handbooks#risk-management-handbook-rmh-chapters>.

**CMS shall:**

- Review the CMS System Security and Privacy Plan (SSP) for CMS information systems and the CMS network annually and update it when a major modification occurs, as required by the CMS SSP Procedures.

**Beneficial shall:**

- Maintain an SSP based on the *Non-Exchange Entity (NEE) System Security and Privacy Plan (SSP)* document<sup>16</sup> on the Non-CMS Organization's network and update annually or whenever there is a significant change;<sup>17</sup> and
- Make accessible to CMS all IS program documents including, but not limited to, those documents specified in Section 7.1.

## 11. Network Security

### 11.1 Network Management

**Both parties shall:**

- Ensure that this interconnection is isolated from all other customer / business processes to the greatest extent possible.

### 11.2 Material Network Changes

**Both parties shall:**

- Submit to the CMS CCIIO any proposed material changes to either network or the connecting medium accompanied by a valid business justification;
- Renegotiate this ISA before any material changes are implemented;
- Report planned technical changes to the network architecture that affect the interconnection to the CMS CCIIO Hub team;
- Conduct a risk assessment based on the new network architecture and modify and re-sign this ISA within one (1) month prior to implementation; and
- Notify the CMS CCIIO Hub team when access is no longer required.

<sup>16</sup> The *Non-Exchange Entity System Security and Plan (SSP)* is located at: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>.

<sup>17</sup> Per NIST SP 800-37, significant changes to an information system may include, for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include, for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.

## 11.3 New Interconnections

### Beneficial shall:

- List and define any new interconnections or updates to any existing interconnections, including any new updates in processes related to sharing, utilizing, and downloading data; and
- Notify CMS when new interconnections impact the security posture of the EDE Pathway or the Hub, unless expressly agreed in a modification to the relevant ISA and signed by both parties.

## 11.4 Network Inventory

### Beneficial shall:

- Maintain and make available to CMS on request a list of all Non-CMS Organization subnets connected to CMS's network, if applicable, and periodically update the information, including information on each owner, physical location, Internet Protocol (IP) address, host's name, hardware, operating system version, and applications.

## 11.5 Firewall Management

### CMS shall:

- Configure the CMS network perimeter firewall in accordance with CMS IS policy;
- Block all network traffic incoming from the Internet to CMS unless it is explicitly permitted; and
- Install a firewall between the perimeter (demarcation point) of the Non-CMS Organization's network and CMS's network if deemed necessary by CMS CCIIO Hub team.

### Beneficial shall:

- Maintain responsibility for configuring all Non-CMS Organization network perimeter firewalls in accordance with a policy at least as stringent as CMS IS policy as reflected in this ISA; and
- Provide to the CMS CCIIO Hub team a list of Non-CMS Organization authorized web HTTP, File Transfer Protocol (FTP), and Simple Mail Transport Protocol (SMTP) servers (identified individually as HTTP, FTP, and/or SMTP) on the Non-CMS Organization's network.

## 11.6 Penetration Test

### Beneficial shall:

- Execute a Rules of Engagement with their penetration testing team;



- Not target IP addresses used for the CMS and Non-CMS Organization connection;
- Conduct penetration testing in the lower environment that mirrors the production environment;
- Not conduct penetration testing in the production environment;
- Notify CMS designated technical counterparts on their annual penetration testing schedule; and
- Provide the following information to CMS a minimum of 5 business days prior to initiation of testing:
  - Period of testing performance (specific times for all testing should be contained in individual test plans);
  - Target environment resources to be tested (IP addresses, Hostname, URL); and
  - Any restricted hosts, systems, or subnets that are not to be tested.

## 12. Incident Prevention, Detection, and Response

### 12.1 Incident Handling

#### **CMS shall:**

- Handle and report incidents in accordance with the CMS Risk Management Handbook (RMH) Chapter 08: Incident Response.<sup>18</sup>

#### **Beneficialign shall:**

- Implement Breach and Incident Handling procedures that are consistent with CMS’s Incident and Breach Notification Procedures and incorporate these procedures in the Beneficialign’s own written policies and procedures.
- Implement specifications. Such policies and procedures would:
  - Identify the Beneficialign’s Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents<sup>19</sup> or Breaches<sup>20</sup>;

<sup>18</sup> Located at the CMS IS webpage, available at: <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response>.

<sup>19</sup> OMB Memorandum M-17-12 defines “incident” or “security incident” as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. OMB Memorandum M-17-12, Preparing for or Responding to A Breach of Personally Identifiable Information, January 3, 2017. Located at: [http://www.osec.doc.gov/opog/privacy/Memorandums/OMB\\_M-17-12.pdf](http://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-17-12.pdf).

<sup>20</sup> OMB Memorandum M-17-12 defines “breach” as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses



- Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes;<sup>21</sup> and
- Require reporting any Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at [cms\\_it\\_service\\_desk@cms.hhs.gov](mailto:cms_it_service_desk@cms.hhs.gov) within 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.

## 12.2 Intrusion Detection

### Both parties shall:

- Monitor intrusion detection activities and disseminate intrusion detection alerts to their respective BO counterparts for all networks within the scope of this ISA<sup>22</sup>;
- Report to both CMS and the Non-CMS Organization's BO any security incident that occurs on either organization's network within the scope of this ISA; and
- Block inbound and outbound access for any CMS or Non-CMS Organization information systems on the network within the scope of this ISA that are the source of unauthorized access attempts, or the subject of any security events, until the risk is remediated.

## 12.3 Disasters and Other Contingencies

### Both parties shall:

- Promptly notify their designated counterparts as defined in the information system contingency plan in the event of a disaster or other contingency that disrupts the normal operation of one or both connected networks.

## 13. Notice

### Both parties shall:

- Provide notice to all persons specifically required under this ISA in writing and shall be delivered as follows:

---

or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information for anything other than an authorized purpose.

<sup>21</sup> Please refer to *RMH Chapter 08 Incident Response Appendix K - Incident Report Template* located at: <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template>.

<sup>22</sup> Intrusion detection audit logs must be kept for purposes of forensic investigation in the case of an incident.

**If to Non-CMS Organization:**

Benefitalign LLC,  
2400 Louisiana Blvd NE,  
Building 3, Albuquerque,  
NM 87110

**Benefitalign LLC If to CMS:**

Centers for Medicare & Medicaid Services (CMS)  
Center for Consumer Information & Insurance Oversight (CCIIO)  
Room 739H 200 Independence Avenue, SW  
Washington, DC 20201

Notices sent by hand or overnight courier service, or mailed by certified or registered mail, shall be deemed to have been given when received, provided that notices not given on a business day (i.e., Monday – Friday excluding federal holidays) between 9:00 a.m. and 5:00 p.m. local time where the recipient is located shall be deemed to have been given at 9:00 a.m. on the next business day for the recipient. Either party to this Agreement may change its contact information for notices and other communications by providing thirty (30) days' written notice of such change in accordance with this provision.

## 14. Modifications

If any personnel changes occur involving the POCs listed in this ISA, the terms of this ISA shall remain in full force and effect, unless formally modified by both parties. Any modifications that materially change the security posture of the portion of the information system related to this ISA shall be in writing and agreed and approved in writing by both parties.

## 15. Compliance

Non-compliance with the terms of this ISA by either party or unmitigated security risks in violation of this ISA may lead to termination of the interconnection. CMS may block network access for the Non-CMS Organization if the Non-CMS Organization does not implement reasonable precautions to prevent the risk of security incidents spreading to CMS's network. CMS is authorized to audit the security of Non-CMS Organization's Network periodically by requesting that Non-CMS Organization provide documentation of compliance with the security requirements in this ISA (please refer to Section 22, Records). The Non-CMS Organization shall provide CMS reasonable access to its IT resources impacted by this ISA for the purposes of audits, subject to applicable legal requirements and policies.

## 16. Termination

Termination of this ISA will result in termination of the functionality and electronic interconnection(s) covered by this ISA. The termination of EDE Agreement and/or Issuer

Agreement and/or Web-broker Agreement will result in termination of this ISA. Termination of any of the agreements referenced in this provision will result in termination of DE Entity's ability of to use the EDE Pathway as allowed by this ISA.

## 17. Cost Considerations

Both parties agree to be responsible for their own systems and costs of the interconnecting mechanism and/or media. No financial commitments to reimburse the other party shall be made without the written concurrence of both parties. Modifications to either system that are necessary to support the interconnection are the responsibility of the respective system/network owners' organization. This ISA neither authorizes, requires, nor precludes any transfer of funds without the agreement of both parties.

## 18. Timeline

This Agreement becomes effective on the date the last of the two parties executes this Agreement and ends the day before the first day of the annual open enrollment period (OEP) for the benefit year beginning January 1, 2025.

## 19. Order of Precedence

In the event of an inconsistency between the terms and conditions of this ISA and the terms and conditions of any other agreement, memorandum of understanding, or acquisition between CMS and Non-CMS Organization, the terms and conditions of the EDE Agreement shall have precedence over this ISA. If the terms and conditions at issue are not otherwise covered in the EDE Agreement, the parties agree that the ISA will have precedence.

## 20. Confidentiality

Subject to applicable statutes and regulations, including the Freedom of Information Act, the parties agree that the terms and conditions (any proprietary information) of this ISA shall not be disclosed to any third party outside of the Government without the prior written consent of the other party.

Both parties may disclose the terms, conditions, and content of this ISA as reasonably necessary to their respective auditors, counsel, and other oversight agencies to respond to a properly authorized civil, criminal judicial process or regulatory investigation or subpoena or summons, issued by a federal or state authority having jurisdiction over either party for examination, compliance, or other purposes, as authorized by law. Any such disclosure may only be made after giving prior notice to the other party of the potential disclosure as soon as reasonably practical before such disclosure is required to be made. Either party, as a condition of its consent to disclosure, may require the other party to take sufficient measures to protect against the disclosure of information that could present significant risk to the security posture of the parties' systems, including the exposure of vectors of attack. Such measures include, but are not limited

to, obtaining a protective order from a court of competent jurisdiction, disclosing the ISA in redacted form, or disclosing the ISA subject to a non-disclosure agreement, as appropriate under the circumstances and applicable law.

## 21. Survival

The Non-CMS Organization's duty to protect and maintain the privacy and security of PII, as well as the confidentiality requirements under Section 20, shall survive the termination of this ISA.

## 22. Records

The Non-CMS Organization shall maintain all records that it may create in the normal course of its business in connection with activity under this ISA for the term of this ISA and for at least ten (10) years after the date this ISA terminates or expires in accordance with 45 C.F.R. §§ 155.220(c)(3)(i)(E) or 156.705(c), as applicable. Subject to applicable legal requirements and reasonable policies, such records shall be made available to CMS to ensure compliance with the terms and conditions of this ISA. The records shall be made available during regular business hours at Non-CMS Organization offices, and CMS's review shall not interfere unreasonably with the Non-CMS Organization business activities.

## 23. Assignment and Severability

This ISA may not be assigned to another party without the specific written consent of the other party. If any term or condition of this ISA becomes inoperative or unenforceable for any reason, such circumstances shall not have the effect of rendering the term or condition in question inoperative or unenforceable in any other case or circumstances, or of rendering any other term or condition contained in this ISA to be invalid, inoperative, or unenforceable to any extent whatsoever. The invalidity of a term or condition of this ISA shall not affect the remaining terms and conditions of this ISA.

## 24. Warranty

CMS does not warrant that Non-CMS Organization interconnection to the CMS network under this ISA will meet Non-CMS Organization requirements, expectations, or even the stated expected benefit of Non-CMS Organization interconnection to CMS (please refer to Provision 6, Statement of Requirements). Non-CMS Organization bears the entire risk regarding the quality and performance of its interconnection with the CMS, and Non-CMS Organization's exclusive remedy is to terminate this ISA in accordance with the terms and conditions herein.

CMS EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE WITH REGARD TO NON-ORGANIZATION'S INTERCONNECTION TO THE CMS.

## 25. Limitation of Liability

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL CMS BE LIABLE TO NON-CMS ORGANIZATION OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

## 26. Force Majeure

Non-CMS Organization's failure to comply with any term or condition of this ISA as a result of conditions beyond its fault, negligence, or reasonable control (such as, but not limited to, war, strikes, floods, governmental restrictions, riots, fire, other natural disasters, or similar causes beyond Non-CMS Organization control) shall not be deemed a breach of this ISA.

## 27. Signatures

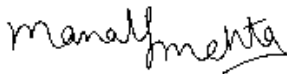
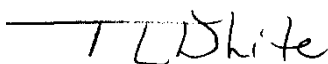
Both parties agree to work together to ensure the joint security of the connected networks and the data they store, process, and transmit, as specified in this ISA. Each party certifies that its respective network is designed, managed, and operated in compliance with this ISA, and all relevant federal laws, regulations, policies and the EDE System Security and Privacy Plan document. Each party attests that the information provided in this ISA is true, correct, and complete to the best of their knowledge. Each party also certifies that its respective network has been certified and accredited in accordance with NIST guidance.

By signing below, the parties agree to the terms and conditions of this ISA.

This “CMS INTERCONNECTION SECURITY AGREEMENT (ISA) BETWEEN CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) AND ENHANCED DIRECT ENROLLMENT ENTITY” has been signed and executed by:

### FOR EDE ENTITY

The undersigned is an authorized official of EDE Entity who is authorized to represent and bind EDE Entity for purposes of this ISA.

<b>Authorized Official for Benefitalign LLC</b>	<b>Chief Information Security Officer / Senior Officer of Privacy (equivalent) for Benefitalign LLC</b>
 _____ 10-19-2023	 _____ 10-19-2023
(Signature) (Date)	(Signature) (Date)
Manal Mehta CEO	Tamara White Sr. Director

### Benefitalign LLC

2400 Louisiana Blvd NE,  
Building 3, Albuquerque,  
NM 87110

Ph: **REDACTED**

**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Centers for Medicare & Medicaid Services

---

**FOR CMS**

**The undersigned are officials of CMS who are authorized to represent and bind CMS for purposes of this ISA.**

**Kevin A. Dorsey**  
-S

Digitally signed by Kevin A.  
Dorsey -S  
Date: 2023.10.17 09:03:47  
-04'00'

(Signature)

**Kevin Allen Dorsey**  
Senior Information Security Officer  
Center for Consumer Information and Insurance Oversight (CCIIO)  
Centers for Medicare & Medicaid Services (CMS)

**Brian M.**  
**James -S**

Digitally signed by Brian M.  
James -S  
Date: 2023.10.18 09:31:20  
-04'00'

(Signature)

**for Marc Richardson**  
Director of Marketplace Information Technology Group (MITG)  
Center for Consumer Information and Insurance Oversight (CCIIO)  
Centers for Medicare & Medicaid Services (CMS)

**Jeffrey Grant**  
S

Digitally signed by Jeffrey  
Grant -S  
Date: 2023.10.19 15:48:46  
-04'00'

(Signature)

**Jeffrey D. Grant**  
Deputy Director for Operations  
Center for Consumer Information and Insurance Oversight (CCIIO)  
Centers for Medicare & Medicaid Services (CMS)

**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Centers for Medicare & Medicaid Services

---

**Robert M.  
Wood -S**

Digitally signed by Robert M.  
Wood -S  
Date: 2023.10.30 01:20:05  
-04'00'

(Signature)

**Robert Wood**

Director Information Security and Privacy Group (ISPG)  
Chief Information Security Officer (CISO)  
Office of Information Technology (OIT)  
Centers for Medicare & Medicaid Services (CMS)

**George C.  
Hoffmann -S**

Digitally signed by George C.  
Hoffmann -S  
Date: 2023.10.30 07:12:49  
-04'00'

(Signature)

**George C. Hoffmann**

Deputy Chief Information Officer (Dep. CIO)  
Office of Information Technology (OIT)  
Centers for Medicare & Medicaid Services (CMS)



## Appendix A. Responsible Parties

### A.1 Authorizing Official

Table 1. System Authorizing Official

System Authorizing Official Information	Detail
Name	Manal Mehta
Title	CEO
Company / Organization	Benefitalign LLC
Address	2400 Louisiana Blvd NE, Building 3, Albuquerque, NM 87110
Phone Number	610-420-1213
Email Address	manal.mehta@benefitalign.com

### A.2 Other Designated Contacts

Table 2 and Table 3 identify the following individual(s) who possess in-depth knowledge of this system and/or its functions and operation.

Table 2. Information System Management Point of Contact

Information System Management POC	Detail
Name	Sonu Rajamma
Title	Infra Head
Company / Organization	Benefitalign LLC
Address	2400 Louisiana Blvd NE, Building 3, Albuquerque, NM 87110
Phone Number	301 775 0660
Email Address	sonu.sr@benefitalign.com

Table 3. Information System Technical Point of Contact

Technical POC	Detail
Name	Sonu Rajamma
Title	Infra Head
Company / Organization	Benefitalign LLC
Address	2400 Louisiana Blvd NE, Building 3, Albuquerque, NM 87110

Technical POC	Detail
Phone Number	301 775 0660
Email Address	sonu.sr@benefitalign.com

### A.3 Assignment of Security and Privacy Responsibility

The EDE Entity Information System Security Officer (ISSO) or equivalent, identified in Table 4, has been appointed in writing and is deemed to have significant cyber and operational role responsibilities.

**Table 4. EDE Entity Name Internal ISSO (or Equivalent) Point of Contact**

EDE Internal ISSO	Detail
Name	Biju Joseph
Title	Lead Infrastructure and Security
Company / Organization	Benefitalign LLC
Address	2400 Louisiana Blvd NE, Building 3, Albuquerque, NM 87110
Phone Number	505-917-3890
Email Address	biju.joseph@speridian.com

The EDE Entity Information System Official for Privacy, identified in Table 5, has been appointed in writing and is deemed to have significant privacy operational role responsibilities.

**Table 5. EDE Entity Internal Official for Privacy (or Equivalent) Point of Contact**

EDE Internal Official for Privacy POC	Detail
Name	Tamara White
Title	Senior Director
Company / Organization	Benefitalign LLC
Address	2400 Louisiana Blvd NE, Building 3, Albuquerque, NM 87110
Phone Number	305-725-4037
Email Address	tamara.white@benefitalign.com

Table 6 names the CMS Information System Security Officer responsible for providing assistance to the EDE Entity security and privacy officers.

Table 6. CMS ISSO Point of Contact

CMS ISSO POC	Detail
<b>Name</b>	CMS ISSOs
<b>Title</b>	ISSO
<b>Company / Organization</b>	CMS/Center for Consumer Information and Insurance Oversight/Marketplace IT Group
<b>Address</b>	7500 Security Blvd., Baltimore, MD 21244-1850
<b>Email Address</b>	directenrollment@cms.hhs.gov

## Appendix B. Primary EDE Entities Connection and Data Sharing with Upstream EDE Entities

The following Beneficial LLC update of Appendix B is maintained to record the annual description of the Primary EDE Entity and its upstream EDE Entities. This table must be updated to record any changes to Appendix B from the last submission.

**Table 7. Record of Changes for Appendix B**

Version	Date	Author / Owner	Description of Change	CR #
1.0	12/21/2018		Baselined	
1.1	01/10/2019		N/A	
1.2	03/27/2020		N/A	
1.3	10/16/2020	Head Infra	AvMed details added	
1.4	04/29/2021	Head Infra	Optima details added	
1.5	10/28/2021	Head Infra	Inshura details added	
1.6	08/17/2022	Head Infra	Modified Inshura data flow diagram	
1.7	10/16/2023	Head Infra	Removed Optima	

CR: Change Request

### B.1 Upstream EDE Entities Overview

Table 8 contains the following fields:

- **Upstream EDE Entity:** Document all known or unexpected EDE Entities and/or system name (if applicable).
- **Entity Type:** Document the Entity Type (e.g., issuer, web-broker, and agent/broker).<sup>23</sup>
- **Partner ID(s):** Provide the Partner ID(s) for the upstream EDE Entity.

**Table 8. Upstream EDE Entity Overview**

Upstream EDE Entity	Entity Type	Partner ID(s)
AvMed	Issuer	04.AVM.FL*.671.437
Inshura	Web-Broker	04.TCL.MD*.347.921

<sup>23</sup> Definitions of each entity type are available in [45 C.F.R. § 155.20](#).

## B.2 Data Connections

Table 9 contains the following fields:

- **ID:** Unique identifier for the row item to track items between Table 8 and Table 9, as applicable.
- **Information System Name:** IT system environment name for the EDE Environment Provider.
- **Upstream EDE Entity Organization Name:** Document all known or expected upstream entities and/or system name (if applicable).
- **Information Being Transmitted:** For example, personally identifiable information (PII) data elements, enrollment information, eligibility information, and 834s.
- **Data Sharing Agreement in Place:** Briefly describe terms of the Agreement (e.g., Memorandum of Understanding [MOU]) and Business Agreement), parties to the agreement, data covered, and protection requirements for the data.
- **Connection Type/Data Direction:** IPsec VPN, SSL, Secure File Transfer, API/Incoming, outgoing, or both.
- **Comments:** Any additional comments to describe the data connection.

Table 9. Interconnections and Data Exchange Between EDE Environment Provider and Upstream Entities

ID	Information System Name	Upstream EDE Entity Organization Name	Information Being Transmitted <sup>24</sup>	Data Sharing Agreement in Place	Connection / Data Direction	Comments
1	BrokerEngage	AvMed	SAML token with agent/member login information only	<p>AvMed has signed an extendable 3 years licensing and services agreement with Benefitalign/Speridian that includes the license to utilize Benefitalign's DE/EDE platform as an Upstream Issuer entity. The scope of this agreement is FFM on-exchange Individual and Family coverage offered by AvMed in the state of Florida.</p> <p>The agreement requires Benefitalign to comply with applicable CMS standards and requirements including the Privacy Rule, 45 C.F.R. Parts 160 and 164, subparts A and E, and the Security Rule, 45 C.F.R. Parts 160 and 164, subparts A and C, and the same may be modified or amended from time to time.</p> <p>The agreement covers Benefitalign's obligations concerning privacy and security, confidentiality and integrity of, and to prevent intentional or unintentional non-permitted or violating use or disclosure of, and to protect against unauthorized access to or unlawful destruction, loss or alteration</p>	SSL / Incoming	Hybrid Issuer – Agents & members signs into Benefitalign platform via SSO from AvMed.org, performs eligibility, enrollment & post enrollment activities [collects binder and ongoing payment, Notice retrieval & document upload

<sup>24</sup> **Note:** A primary EDE Entity adding any EDE Entity relationships must also follow the Change Notification Procedures for the Enhanced Direct Enrollment Entity Information Technology Systems process.

ID	Information System Name	Upstream EDE Entity Organization Name	Information Being Transmitted <sup>24</sup>	Data Sharing Agreement in Place	Connection / Data Direction	Comments
				of, the Personal data created for or received from or on behalf of the customer in connection with the services, functions, or transactions to be provided under on contemplated by this agreement. Benefitalign will neither utilize nor publicly release any information that could be linked to an individual in any manner that would reveal the PII and/or PHI. AvMed shall remain the sole owner of all the data and shall be utilized solely for the purposes set forth in this agreement.		
2	BrokerEngage	Inshura	Bearer Token with agent details	<p>Inshura has signed licensing and services agreement with Benefitalign that includes the license to utilize Benefitalign's DE/EDE platform as a Hybrid, non-issuer upstream entity. The scope of this agreement is FFM on-exchange individual and family coverage offered by Inshura in all the FFM states.</p> <p>The agreement requires Inshura to comply with applicable CMS standards and requirements regarding privacy and security.</p> <p>The agreement covers Benefitalign's and Inshura's obligations concerning privacy and security, confidentiality and integrity of, and to prevent intentional or unintentional non-permitted or violating use or disclosure of, and to protect against unauthorized</p>	SSL / Incoming	<p>Hybrid, non-issuer upstream entity.</p> <p>Inshura provides a free shopping and enrollment experience for agents, brokers and consumers. Inshura adds functionality to BenefitAlign's EDE environment by implementing an EDE program requirement instead of Benefitalign. Specifically, Inshura provides the agent/broker identity proofing implementation on its own system. Agents and brokers then use the primary EDE Entity's EDE</p>

ID	Information System Name	Upstream EDE Entity Organization Name	Information Being Transmitted <sup>24</sup>	Data Sharing Agreement in Place	Connection / Data Direction	Comments
				<p>access to or unlawful destruction, loss or alteration of, the personal data created for or received from or on behalf of the customer in connection with the services, functions, or transactions to be provided under on contemplated by this agreement. Benefitalign will neither utilize nor publicly release any information that could be linked to an individual in any manner that would reveal the PII and/or PHI.</p>		<p>environment to assist consumers.</p> <p>Inshura will further implement adding and storing the agents' carrier appointments within Inshura.</p> <p>Inshura allows the agents/ brokers to upload their current book of business and prospects through a bulk operation on the Inshura platform. This data will then be used on Benefitalign's EDE platform for creating quotes for new prospects or for renewing existing customers.</p> <p>Once the agents are logged into the Inshura platform they will be redirected to Benefitalign's EDE environment via single sign-on for the shopping, enrollment and post-enrollment experience.</p>



## B.3 Additional Functionality or Systems

Table 10 contains the following fields:

- **ID:** Unique identifier for the row item to track items between Table 9 and Table 10, as applicable.
- **Information System Name:** IT system environment name for the EDE Environment Provider.
- **Upstream EDE Entity Organization Name:** Document all known or expected upstream entities and/or system name (if applicable).
- **SSO Implementation:** If an EDE arrangement will involve SSO, the entity must describe the SSO implementation, including, at a minimum, the following information: which users will use the SSO implementation (i.e., consumers, agents, and brokers) and the process to and entity responsible for conducting identity proofing of consumers, agents, and brokers.
- **Additional Functionality/Systems:** For each applicable arrangement, indicate whether the primary EDE Entity’s environment integrates with any functionality or systems owned, controlled, managed, or accessed by the upstream EDE Entity that exists outside of the boundaries of the audited, primary EDE Entity’s EDE environment. For any such functionality or system, indicate the data transferred between the external environment and the EDE environment (e.g., data regarding data matching issues, special enrollment period verification issues, and enrollment status).
  - In the following sub-bullets, CMS provides several, non-exhaustive examples of potential additional functionality or systems:
    - Example Scenario 1: An upstream EDE Entity collects initial data from a consumer on its system for the purposes of completing an eligibility application or to display health insurance options or QHPs (e.g., plan selection), and then may redirect the consumer and/or their data to the primary EDE Entity for completing the eligibility application or enrollment experience.
    - Example Scenario 2: An upstream EDE Entity provides a plan selection and enrollment process separate from the primary EDE Entity’s EDE environment.
    - Example Scenario 3: An upstream entity provides the agent/broker identity proofing implementation on its own system. Agents and brokers then use the primary EDE Entity’s EDE environment to assist consumers.
    - Example Scenario 4: An upstream entity retrieves, stores, transfers, or manages consumer data obtained or collected through the primary EDE Entity’s EDE environment on the upstream entity’s own system (e.g., data stored in a customer relationship management software).
    - Example Scenario 5: An upstream entity implements a single sign-on solution with the primary EDE Entity’s EDE Environment.

- **QHP Display for EDE End-User Experience:** For each arrangement, indicate whether the primary EDE Entity or upstream EDE Entity provides the QHP display for the EDE End-User Experience. If both the primary and upstream EDE Entity provide the QHP display—such as at different parts of the EDE End-User Experience or for different pathways (e.g., agent/broker and consumer), describe the details of the arrangement for displaying QHPs in the End-User Experience for both agents/brokers and consumers.
  - For example, the upstream EDE Entity sends a selected QHP to the primary EDE Entity before a user completes the eligibility application, and the primary EDE Entity provides a post-application QHP shopping experience.
  - Another example, the upstream EDE Entity hosts a pre-application QHP display for agents/brokers and sends the QHP selection to the primary EDE Entity. The primary EDE Entity hosts the QHP display for consumers.
- **Comments:** Any additional comments to describe the data connection.

Table 10. Additional Functionality or Systems

ID	Information System Name	Upstream EDE Entity Organization Name	SSO Implementation <sup>25</sup>	Additional Functionality <sup>26</sup>	QHP Display for EDE End-User Experience <sup>27</sup>	Comments
1	BrokerEngage	AvMed	SSO SAML redirect Users: Agents & members ID Proofing done by Benefitalign.	NA	QHP display by Benefitalign	Upstream Issuer with all functions handled by Benefitalign platform like shopping, plan selection, ID proofing, Eligibility & Enrollment process, post enrollment process, document upload, notice retrieval, communication are handled by CMS audited Benefitalign platform.
2	BrokerEngage	Inshura	SSO Bearer Token with agent details  Agents & members ID Proofing done by Inshura.	Inshura adds functionality to BenefitAlign's EDE environment by implementing an EDE program requirement instead of Benefitalign.  Inshura provides the agent/broker identity proofing implementation on its own system.  Inshura will further implement adding and storing the agents' carrier appointments within Inshura.  Inshura allows the agents/brokers to upload their current book of business and prospects through a bulk operation on the	QHP display by Benefitalign	Inshura is a consumer and broker facing portal, and will use Benefitalign EDE platform for shopping, eligibility determination, submitting enrollments and performing post enrolment activities. Inshura's website will redirect the brokers & consumers to Benefitalign platform for quoting and enrollment

<sup>25</sup> CMS has added this new field to Table 10. Please review the instructions above to provide an appropriate response to this field.

<sup>26</sup> **Note:** A primary EDE Entity adding any EDE Entity relationships must also follow the Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems process.

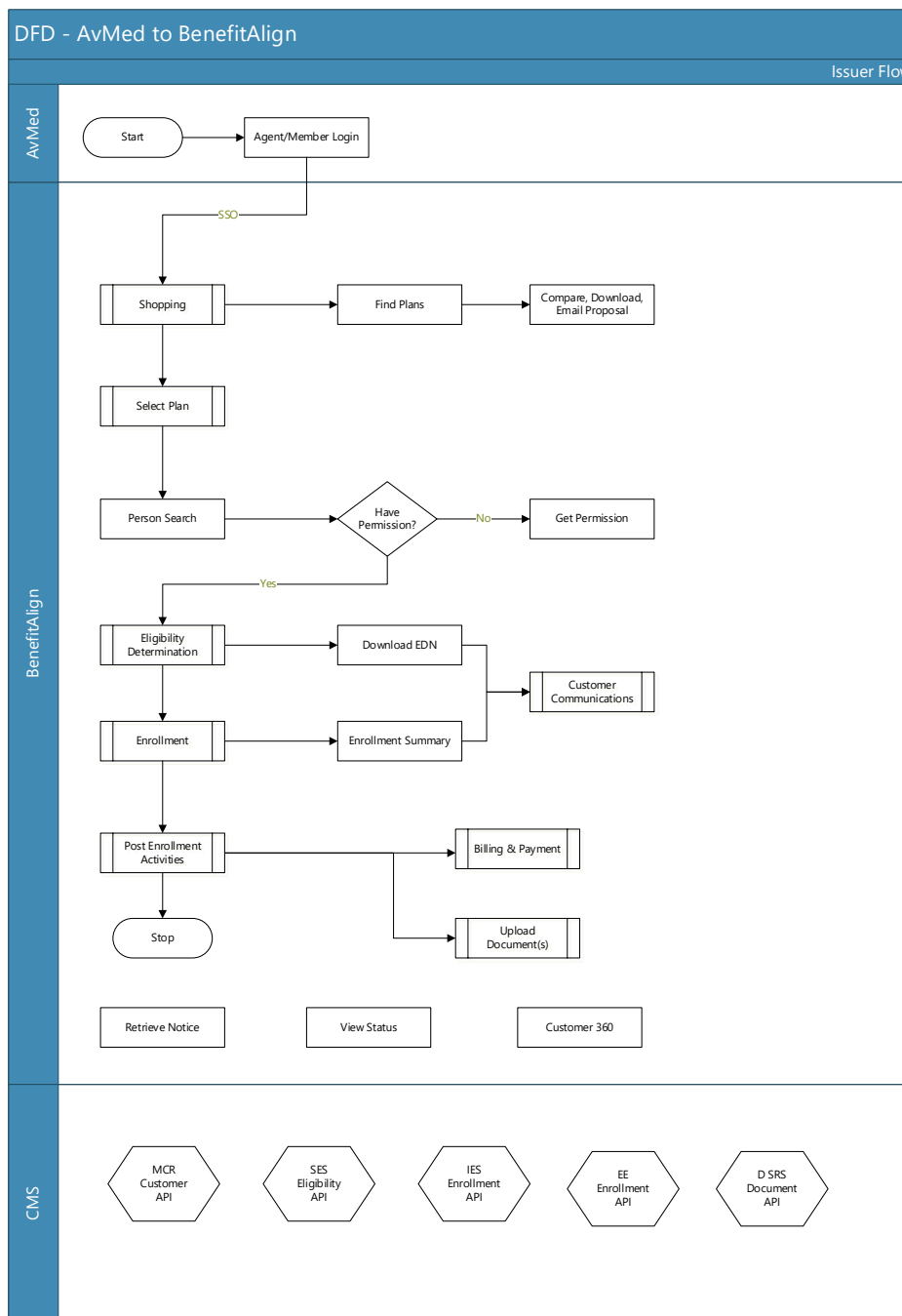
<sup>27</sup> CMS has revised the instructions for this field. Please carefully review the instructions above to provide an appropriate response to this field.

ID	Information System Name	Upstream EDE Entity Organization Name	SSO Implementation <sup>25</sup>	Additional Functionality <sup>26</sup>	QHP Display for EDE End-User Experience <sup>27</sup>	Comments
				<p>Inshura platform. This data will then be used on Benefitalign's EDE platform for creating quotes for new prospects or for renewing existing customers.</p> <p>Once the agents are logged into the Inshura platform they will be redirected to Benefitalign's EDE environment via single sign-on for the shopping, enrollment and post-enrollment experience.</p>		

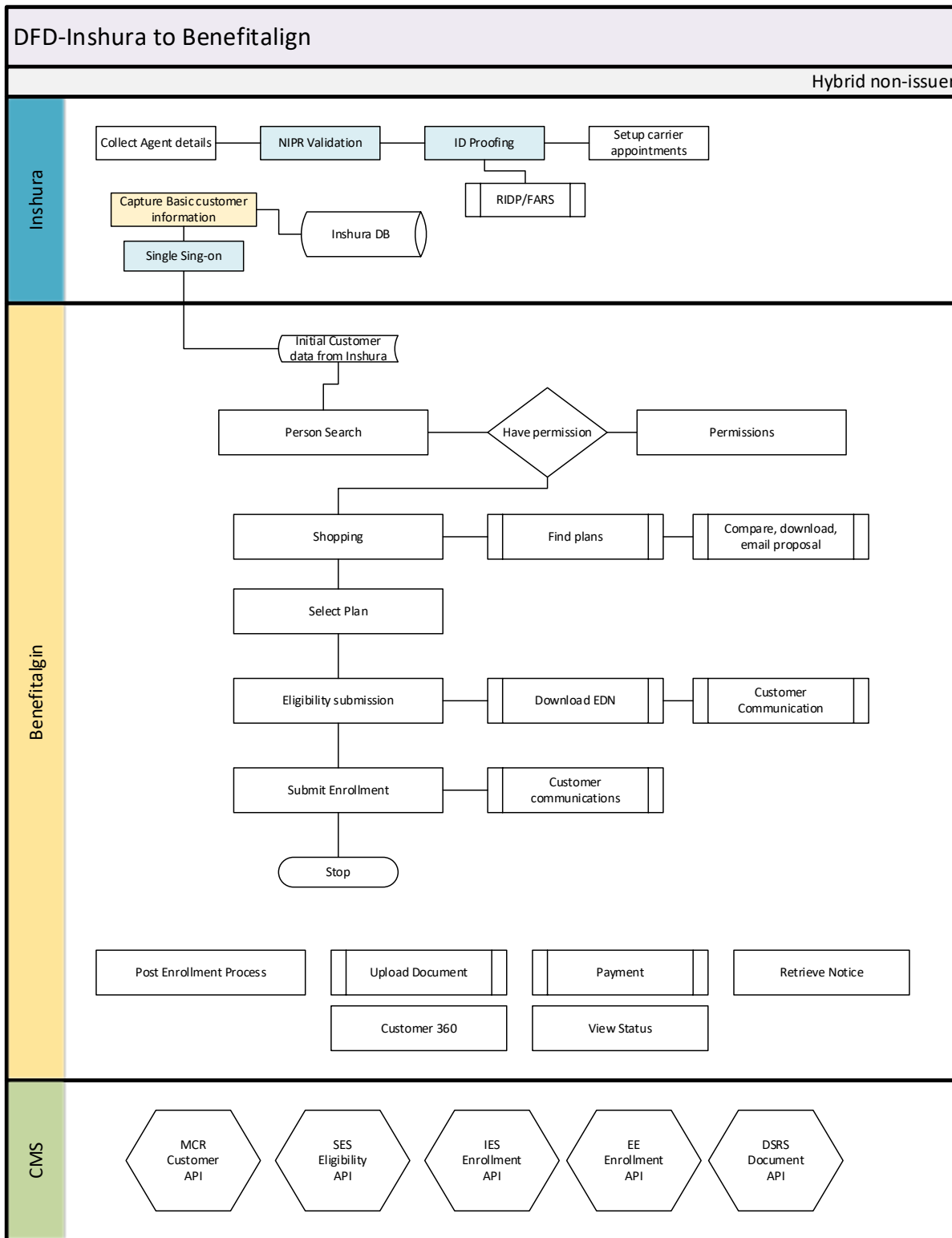
## B.4 Data Flow/Topological Diagram

Figure 2 represents the data flow in and out of the Primary EDE Environment and Additional Systems/Functionality system boundaries.

**Figure 2. AvMed Data Flow/Topological Diagram**



**Figure 3. Inshura Data Flow/Topological Diagram**



# Exhibit J

JUNE 09, 2021

## Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, find that it is appropriate to elaborate upon measures to address the national emergency with respect to the information and communications technology and services supply chain that was declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain). Specifically, the increased use in the United States of certain connected software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the Secretary of Commerce acting pursuant to Executive Order 13873 has defined to include the People's Republic of China, among others, continues to threaten the national security, foreign policy, and economy of the United States. The Federal Government should evaluate these threats through rigorous, evidence-based analysis and should address any unacceptable or undue risks consistent with overall national security, foreign policy, and economic objectives, including the preservation and demonstration of America's core values and fundamental freedoms.

By operating on United States information and communications technology devices, including personal electronic devices such as smartphones, tablets, and computers, connected software applications can access and capture vast swaths of information from users, including United States persons' personal information and proprietary business information. This data collection threatens to provide foreign adversaries with access to that information.



Foreign adversary access to large repositories of United States persons' data also presents a significant risk.

In evaluating the risks of a connected software application, several factors should be considered. Consistent with the criteria established in Executive Order 13873, and in addition to the criteria set forth in implementing regulations, potential indicators of risk relating to connected software applications include: ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities; use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data; ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary; ownership, control, or management of connected software applications by persons involved in malicious cyber activities; a lack of thorough and reliable third-party auditing of connected software applications; the scope and sensitivity of the data collected; the number and sensitivity of the users of the connected software application; and the extent to which identified risks have been or can be addressed by independently verifiable measures.

The ongoing emergency declared in Executive Order 13873 arises from a variety of factors, including the continuing effort of foreign adversaries to steal or otherwise obtain United States persons' data. That continuing effort by foreign adversaries constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. To address this threat, the United States must act to protect against the risks associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.

Additionally, the United States seeks to promote accountability for persons who engage in serious human rights abuse. If persons who own, control, or manage connected software applications engage in serious human rights abuse or otherwise facilitate such abuse, the United States may impose consequences on those persons in action separate from this order.

Accordingly, it is hereby ordered that:

Section 1. Revocation of Presidential Actions. The following orders are revoked: Executive Order 13942 of August 6, 2020 (Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain); Executive Order 13943 of August 6, 2020 (Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain); and Executive Order 13971 of January 5, 2021 (Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies).

Sec. 2. Implementation. (a) The Director of the Office of Management and Budget and the heads of executive departments and agencies (agencies) shall promptly take steps to rescind any orders, rules, regulations, guidelines, or policies, or portions thereof, implementing or enforcing Executive Orders 13942, 13943, or 13971, as appropriate and consistent with applicable law, including the Administrative Procedure Act, 5 U.S.C. 551 *et seq.* In addition, any personnel positions, committees, task forces, or other entities established pursuant to Executive Orders 13942, 13943, or 13971 shall be abolished, as appropriate and consistent with applicable law.

(b) Not later than 120 days after the date of this order, the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, and the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide a report to the Assistant to the President and National Security Advisor with recommendations to protect against harm from the unrestricted sale of, transfer of, or access to United States persons' sensitive data, including personally identifiable information, personal health information, and genetic information, and harm from access to large data repositories by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary. Not later than 60 days after the date of this order, the Director of National Intelligence shall provide threat assessments, and the Secretary of Homeland Security shall provide vulnerability assessments, to the Secretary of Commerce to support development of the report required by this subsection.

(c) Not later than 180 days after the date of this order, the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of

Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget, and the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide a report to the Assistant to the President and National Security Advisor recommending additional executive and legislative actions to address the risk associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.

(d) The Secretary of Commerce shall evaluate on a continuing basis transactions involving connected software applications that may pose an undue risk of sabotage or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States; pose an undue risk of catastrophic effects on the security or resiliency of the critical infrastructure or digital economy of the United States; or otherwise pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. Based on the evaluation, the Secretary of Commerce shall take appropriate action in accordance with Executive Order 13873 and its implementing regulations.

Sec. 3. Definitions. For purposes of this order:

(a) the term “connected software application” means software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the Internet;

(b) the term “foreign adversary” means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons;

(c) the term “information and communications technology or services” means any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display;

(d) the term “person” means an individual or entity; and

(e) the term “United States person” means any United States citizen, lawful permanent resident, entity organized under the laws of the United

States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 4. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

THE WHITE HOUSE,  
June 9, 2021.

# **Exhibit K**

**From:** Grant, Jeff (CMS/CCIIO) <REDACTED>  
**Sent:** Thursday, August 8, 2024 6:37 PM  
**To:** girish.panicker@REDACTED  
**Cc:** tamara.white@REDACTED, sonu.sr@benefitalign.com  
**Subject:** EDE/DE/EBP Suspension

CMS is suspending EDE/DE/EBP access for Inshura/TrueCoverage and Benefitalign due to potential anomalous activity. CMS will follow up with additional communication to provide next steps.

Jeffrey D. Grant  
Deputy Director for Operations  
Center for Consumer Information and Insurance Oversight  
Centers for Medicare & Medicaid Services

# **Exhibit L**

Thursday, September 19, 2024 at 10:22:19 Eastern Daylight Time

---

**Subject:** Re: CMS/Speridian  
**Date:** Thursday, August 15, 2024 at 6:43:13 AM Eastern Daylight Time  
**From:** Busby, Keith (CMS/OIT)  
**To:** Kalpit Dantara, Ashwini Deshpande, CMS CCIO Office of the Director, Montz, Ellen (CMS/CCIO), Grant, Jeff (CMS/CCIO), Girish Panicker, Manal Mehta, Sonu S. Rajamma, Shynihan Muhammed, REDACTED, Nettles, Leslie (CMS/OIT), Paradis, David (CMS/OIT), Dorsey, Kevin Allen (CMS/CCIO), Lyles, Darrin (CMS/CCIO), Kania, Michael (CMS/OIT)  
**Attachments:** image001.png

I can make 9 AM work. I know not everyone else has responded, but I will go ahead and schedule it for then and hope for the best.

Regards,

Keith Busby  
Acting Chief Information Security Officer  
Information Security & Privacy Group (ISPG)  
Office of Information Technology (OIT)  
Centers for Medicare and Medicaid Services (CMS)  
Mobile: REDACTED

---

**From:** Kalpit Dantara <[kalpit.dantara@speridian.com](mailto:kalpit.dantara@speridian.com)>  
**Date:** Wednesday, August 14, 2024 at 6:55 PM

REDACTED



**Subject:** Re: CMS/Speridian

Sure. 8am or 9am work for me.

Kalpit

Get [Outlook for iOS](#)

---

**From:** Busby, Keith (CMS/OIT) <REDACTED>



**Sent:** Wednesday, August 14, 2024 6:39:25 PM

**To:** Ashwini Deshpande <[ashwini.deshpande@Truecoverage.com](mailto:ashwini.deshpande@Truecoverage.com)>; CMS CCIIO Office of the Director

REDACTED  
REDACTED

**Subject:** Re: CMS/Speridian

You don't often get email from REDACTED [Learn why this is important](#)

This message has originated from an **External Source**. Please use proper judgment and caution before attending it. Please report it to [phishing.report@speridian.com](mailto:phishing.report@speridian.com) immediately if you suspect it's a suspicious email.

Good Evening,

We found a couple things that have led to additional questions. Would it be possible to setup a call for tomorrow morning to discuss our new questions?

Regards,

Keith Busby  
Acting Chief Information Security Officer  
Information Security & Privacy Group (ISPG)  
Office of Information Technology (OIT)  
Centers for Medicare and Medicaid Services (CMS)  
Mobile: REDACTED

---

**From:** Busby, Keith (CMS/OIT) <[Keith.Busby@cms.hhs.gov](mailto:Keith.Busby@cms.hhs.gov)>

**Date:** Wednesday, August 14, 2024 at 7:36 AM

**To:** Ashwini Deshpande <REDACTED

REDACTED

**Subject:** Re: CMS/Speridian

Please disregard my previous message. I was able to get in and download them.

Regards,

Keith Busby  
Acting Chief Information Security Officer  
Information Security & Privacy Group (ISPG)  
Office of Information Technology (OIT)  
Centers for Medicare and Medicaid Services (CMS)  
Mobile: REDACTED

---

**From:** Busby, Keith (CMS/OIT) <REDACTED>  
**Date:** Wednesday, August 14, 2024 at 7:34 AM  
**To:** Ashwini Deshpande <[ashwini.deshpande@Truecoverage.com](mailto:ashwini.deshpande@Truecoverage.com)>, REDACTED

REDACTED

**Subject:** Re: CMS/Speridian

Good Morning,

I can't access the folder. Can you adjust my permissions?

Regards,

Keith Busby  
Acting Chief Information Security Officer  
Information Security & Privacy Group (ISPG)  
Office of Information Technology (OIT)  
Centers for Medicare and Medicaid Services (CMS)  
Mobile: REDACTED

---

**From:** Ashwini Deshpande <REDACTED>  
**Date:** Tuesday, August 13, 2024 at 11:30 PM  
**To:** Busby, Keith (CMS/OIT) REDACTED

REDACTED

**REDACTED**

**Subject:** Re: CMS/Speridian

Good Evening

Following please find the DropBox link to the outstanding action items

 [Benefitalign Documents To CMS](#)

Access has been provided to all the CMS email recipients listed on this email .  
To access the documents, please use your email address when prompted.

Here are the list of files in the dropbox :

1. Cloudtrail IAM Access logs – 90 days: **CloudTrail-PROD-event\_history\_Logs.csv**
2. Fortigate geofence rules: **Fortigate Rule.png, Fortigate Rule.csv**
3. Guard duty events, unarchived finds: **Guard-duty-export\_Logs.json**
4. Previous Non-Compliance Remediation Evidence/Closure Information: **Benefitalign Attestation Letter 04192023.docx, Response Email from CMS.pdf**
5. A list of the WAF rules: **WAF-Rules.json**
6. A list of all public urls and load balancers: **URLs.docx**
7. All AWS config events over last 90 days for the WAF and load balancer: **WAF Config change.png, Internal ALB Config change.png, External ALB Config change.png**

Thanks

**Ashwini Deshpande**

Chief Executive Officer

[TrueCoverage, LLC](#)

Phone: **REDACTED**

---

**From:** Busby, Keith (CMS/OIT) <**REDACTED**>

**Date:** Tuesday, August 13, 2024 at 4:56 PM

**To:** CMS CCIO Office of the Director <[CCIOOfficeoftheDirector@cms.hhs.gov](mailto:CCIOOfficeoftheDirector@cms.hhs.gov)>, **REDACTED**

REDACTED

**Subject:** Re: CMS/Speridian

You don't often get email from REDACTED . [Learn why this is important](#)

This message has originated from an **External Source**. Please use proper judgment and caution before attending it. Please report it to [phishing.report@truecoverage.com](mailto:phishing.report@truecoverage.com) immediately if you suspect it's a suspicious email.

Thanks everyone for jumping on another call. As discussed, below are the outstanding action items.

Cloudtrail IAM Access logs – 90 days  
Fortigate geofence rules  
Guard duty events, unarchived finds  
Previous Non-Compliance Remediation Evidence/Closure Information

Can you also supply the following additional request:

A list of the WAF rules  
A list of all public urls and load balancers  
All AWS config events over last 90 days for the WAF and load balancer

Regards,

Keith Busby  
Acting Chief Information Security Officer  
Information Security & Privacy Group (ISPG)  
Office of Information Technology (OIT)  
Centers for Medicare and Medicaid Services (CMS)  
Mobile: REDACTED

---

**From:** [Keith.Busby](#) REDACTED  
**When:** 3:30 PM - 4:00 PM August 13, 2024  
**Subject:** CMS/Speridian  
**Location:** <https://cms.zoomgov.com/j/1602119654?pwd=RbZ0g15kA0lJG8mBATuh8EDbeXlnj.1>

Keith Busby is inviting you to a scheduled ZoomGov meeting.

Join ZoomGov Meeting

<https://cms.zoomgov.com/j/1602119654?pwd=RbZ0g15kA0lLjG8mBATuh8EDbeXlnj.1>

Meeting ID: 160 211 9654

Password: 278995

One tap mobile

REDACTED

Dial by your location

REDACTED

Meeting ID: 160 211 9654

Find your local number: <https://cms.zoomgov.com/u/adgOEqFlQz>

Join by SIP

Password: 278995

sip REDACTED

This meeting may be recorded. The host is responsible for maintaining any official recordings/transcripts of this meeting. If recorded, this meeting becomes an official record and shall be retained by the host in their files for 3 years or if longer needed for agency business. If a recording intends be fully transcribed or is being captured for the purpose of creating meeting minutes, the host shall retain the record in their files for 3 years or if no longer needed for agency business, whichever is later.

# Exhibit M

**From:** [Kalpit Dantara](#)  
**To:** [Paradis, David \(CMS/OIT\)](#); [Busby, Keith \(CMS/OIT\)](#); [CMS CCIIO Office of the Director](#); [Montz, Ellen \(CMS/CCIIO\)](#); [Grant, Jeff \(CMS/CCIIO\)](#); [Girish Panicker](#); [Manal Mehta](#); [Ashwini Deshpande](#); [Sonu S. Rajamma](#); [Shynihan Muhammed](#); [tamara.white@benefitalign.com](mailto:tamara.white@benefitalign.com); [Nettles, Leslie \(CMS/OIT\)](#); [Dorsey, Kevin Allen \(CMS/CCIIO\)](#); [Lyles, Darrin \(CMS/CCIIO\)](#); [Kania, Michael \(CMS/OIT\)](#)  
**Cc:** [Hunt, Patrick \(CMS/OIT\)](#); [Berry, Dawn \(CMS/OIT\)](#)  
**Subject:** RE: CMS/Speridian  
**Date:** Monday, August 19, 2024 12:04:28 AM  
**Attachments:** [image001.png](#)

---

Hi David,

Please see responses inline below. Files referenced are available in the dropbox folder shared for previous queries. Link [Benefitalign Documents To CMS](#)

Appreciate if we can get on a call sometime tomorrow to discuss and bring this to a logical conclusion.

-Kalpit

---

**From:** Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>

**Date:** Friday, August 16, 2024 at 2:08 PM

**To:** Kalpit Dantara <kalpit.dantara@Truecoverage.com>, **REDACTED**

[REDACTED]

**Subject:** RE: CMS/Speridian

This message has originated from an **External Source**. Please use proper judgment and caution before attending it. Please report it to [phishing.report@truecoverage.com](mailto:phishing.report@truecoverage.com) immediately if you suspect it's a suspicious email.

Kalpit,

Thank you for the additional information!

- Please provide the VPN logs for the other two VPN's

>> As mentioned in previous email, the other hosted VPN is a backup VPN and has not been used and does not have any relevant logs. Log from Palo Alto VPN is available in the dropbox. Filename 'PaloAltoVPN Log.csv'

- Why do you only maintain three weeks of VPN logs

>> 3 weeks is the current retention policy. Having said that, open to suggestions on an optimal retention policy. Happy to make the necessary changes once we have an agreement.

- Please provide any Geofencing rules applied to all VPN solutions

>> Screenshot Of VPN Geofencing rules available in dropbox. Filenames 'FortiClient - VPN Geo fencing.png', 'Palo Alto - VPN Geo Fencing 1.png', 'Palo Alto - VPN Geo Fencing 2.png', 'Palo Alto - VPN Geo Fencing 3.png', 'Palo Alto - VPN Geo Fencing 4.png'

- Please provide ruleset from VPNs

>> Ruleset provided in dropbox. Filename 'SPAWSFWL-0001.conf' and 'Palo Alto - Geo Fencing rule.png'

- Please provide any logs with destinations on 158.73.0.0/16, 198.179.4.0/24 or 198.179.3.0/24

>> Having looked at our logs, we don't see any access to the above IP ranges. If you have any further specifics on this request including timeframe in question, happy to dig in further. Screenshots of our search provided in dropbox. Filename 'Logs to Destination Ips.docx'

- Does BenefitAlign/True Coverage have monitoring in place for users utilizing VPN services or accessing resources from OCONUS? If so what is it and can a log be provided?

>> Our firewall is configured to serve as a VPN gateway with geofencing capabilities, allowing only employees located in the U.S. region to connect to the VPN and access resources.



- Based on the original description of the issue, one of the things we will want to see is queries generated by the CRM platform that target CMS data in EDE - including the source IP address and username the query originated from.

>> There are no queries from CustomerEngage [Our CRM Platform] that can access any EDE data within BrokerEngage [EDE Platform]. There are entities that reside outside the EDE Object Model that can be created or updated from CustomerEngage. Below use case will help you understand the interactions:

1. Agent gets a call [Lead] and this creates a Lead record in CustomerEngage [CRM].
2. The Lead is nurtured and if it is disposed as an "Opportunity", it creates a Customer Record [basic profile information like name, phone # etc] and a related Opportunity record in CustomerEngage.
3. The customer record is synced into BrokerEngage [EDE].
4. The agent can navigate to BrokerEngage and see the newly created Customer Record.
5. The agent then can create Quotes/Proposals in BrokerEngage.
6. If the customer wants to enroll, the EDE Flow is initiated in BrokerEngage by the agent.
7. When the application is completed and submitted, the BrokerEngage Customer Record Status is updated to reflect the enrolled status.
8. This customer status is synced back to CustomerEngage and the opportunity is updated to Sold status.

If it is helpful, we can setup a demo to walk you through the sales workflow.

- Please provide an explanation of your firewall configuration rules in Fortigate to better understand whether or not the rules are correctly configured to prevent access from OCONUS, and where exactly this firewall sits in their network.

>> Our VPN configuration enforces stringent geofencing policies, blocking all connection attempts from IP addresses located outside the United States. VPN authentication is restricted to users within the U.S. region. Upon successful authentication, the firewall applies rules that permit traffic exclusively from these validated users, ensuring that only U.S.-based entities can access the network resources through the VPN. VPN and WAF firewalls sit at the perimeter level.

- Have you enabled a WAF rule to block VPN and proxy traffic <https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-ip-rep.html#aws-managed-rule-groups-ip-rep-anonymous> and can you provide evidence of such?

>> No, the IP reputation anonymous rule is not enabled on our WAF. Again, we are happy to work with your team on any recommendations.

# **Exhibit N**

**From:** [Manal Mehta](#)  
**To:** [Paradis, David \(CMS/OIT\)](#)  
**Cc:** [Nettles, Leslie \(CMS/OIT\)](#); [Lyles, Darrin \(CMS/CCIIO\)](#); [Ashwini Deshpande.](#); [Hunt, Patrick \(CMS/OIT\)](#); [Busby, Keith \(CMS/OIT\)](#); [Montz, Ellen \(CMS/CCIIO\)](#); [Kania, Michael \(CMS/OIT\)](#); [Sonu S. Rajamma](#); [Dorsey, Kevin Allen \(CMS/CCIIO\)](#); [Girish Panicker](#); [Tamara White](#); [Berry, Dawn \(CMS/OIT\)](#); [Kalpit Dantara](#); [Grant, Jeff \(CMS/CCIIO\)](#); [CMS CCIIO Office of the Director](#); [Shynihan Muhammed](#)  
**Subject:** Re: CMS/Speridian  
**Date:** Thursday, August 22, 2024 10:25:53 AM  
**Attachments:** [image002.png](#)

---

Hello David:

Please find attached responses to your questions below.

Files referenced are available in the dropbox folder shared for previous queries. Link [Benefitalign Documents To CMS](#)

We believe it would be better to have a call sometime today if you have additional questions.

Thanks,  
Manal.

---

**From:** Paradis, David (CMS/OIT) <**REDACTED**>  
**Date:** Tuesday, August 20, 2024 at 3:29 PM

**To:** Kalpit Dantara <[kalpit.dantara@Truecoverage.com](mailto:kalpit.dantara@Truecoverage.com)>, **REDACTED**  
**REDACTED**

**Cc:** **REDACTED**

**Subject:** RE: CMS/Speridian

This message has originated from an **External Source**. Please use proper judgment and caution before attending it. Please report it to [phishing.report@truecoverage.com](mailto:phishing.report@truecoverage.com) immediately if you suspect it's a suspicious email.

Kalpit,

Thank you for the additional information – the teams have some additional questions and requests for data;

- **To confirm, where is the CRM physically located? Please provide evidence of it's physical location.**

>> The CRM application is hosted in the AWS data center located in the US-EAST-1 region. Evidence of physical location in dropbox. Filename – 'CRM location evidence.png'

- **What steps does a CRM operator take to input data into the EDE?**

>> The licensed agent who is EDE ID Proofed is himself/herself the CRM operator [CRM Operator] and has to login with credentials into BrokerEngage [EDE] and be authenticated first. Both CustomerEngage [CRM] and BrokerEngage [EDE] are separate platforms, have separate credentials and each needs their own authorizations.

Once authenticated in BrokerEngage, the agent has to complete ID Proofing [Experian] before the EDE component is enabled or can be accessed as part of initial setup. BrokerEngage is also integrated with NIPR and agents state licensing information is automatically set up/updated in BrokerEngage. Agents cannot quote or see plans for states that they are not licensed in. Additional controls/authorization rules;

- There are two Roles in BrokerEngage: Producer Role and Agency Admin Role. Producers can only view / manage their own Book of Business [BoB], i.e. their own customers. Agency Admin can view and manage the BoB of all producers within the agency.
- Irrespective of Role, EDE is only enabled if the user is ID Proofed.
- Additionally, FFM certified agents who are actively servicing marketplace customers are required to link their FFM account [OKTA linking] with the platform account for security.
- Only one active user per credentials is allowed. If a user tries to login while another session is active, the old session is terminated after prompting the user.
- Inactivity timeouts are set to 5 mins by default. Users can configure it to different times but cannot exceed 30 mins.
- Additionally, agents can enable 2 factor authentication for added security.

- **Where does a CRM operator get the data to input into EDE?**

>> The licensed agent who is EDE ID Proofed [CRM Operator] gets the data to input into EDE from the customer. The customer is typically on the phone and customer consent is obtained prior to working on and prior to submitting their application. See file: BrokerEngage: Customer Consent

- **Is there any data processing, collection or trending occurring for this effort outside of the CONUS?**

>> There is no data processing, collection or trending occurring for this effort outside of the CONUS. BrokerEngage [EDE] cannot be accessed from outside the US.

- **Please explain in detail all methodologies to access your AWS console to include any connection requirements.**

>> Access to AWS infrastructure is restricted to authorized employees in CONUS with whitelisted IP addresses. Users access the AWS console via a web browser, where they must log

in using their unique credentials. To further enhance security, multi-factor authentication is enforced for all users, requiring an additional verification code generated by an authentication app, in addition to their password.

- **Please provide evidence of ownership behind AWS Account ID 26280443682 - BenefitAlign, True Coverage, Speridian or other?**

>> Above Account ID is owned by Benefitalign. Evidence of same is provided in dropbox. Filename – ‘Evidence of ownership.png’

- **Provide a description for FortiClient VPN, Palo Alto VPN, and the backup solution and their specific use cases?**

>> We have implemented VPN solution with whitelisted IP addresses for securing our AWS infrastructure, particularly when employees are working from home. This approach offers robust protection by insulating our network from the public internet. FortiClient is used for our current primary and backup VPN service, and we are in the process of transitioning to Palo Alto's VPN solution as part of our cloud-first strategy. This shift is driven by the advanced security features offered by Palo Alto, which provide more comprehensive protection that better aligns with our evolving security requirements.

- **Please provide the full logs for BOTH FortiClient VPN's and the PA VPN in raw form.**

>> Full logs of all VPN's available in dropbox. Foldername – ‘Activity Log’

- **Where you have indicated that the third VPN is used for backup, we require evidence that this third VPN is not receiving any traffic**

>> Screenshot of activity log provided in dropbox. Filename – ‘Backup FortiClient VPN Logs.png’

- **Why do we see a user logging into the AWS console on June 30 from one VPN endpoint, and then a different VPN endpoint on August 13?**

>> The user, who is a member of the AWS Infrastructure Admin team was evaluating an alternate VPN service, and has not been used since.

- **Do you have any VPN/proxy/anonymizer access disabled through all of your VPN solutions?**

>> Yes. Evidence provided in screenshot available in dropbox. Foldername - ‘VPN Security’

- **Please explain in detail how your geofencing restrictions are implemented across all available VPN platforms**

>> FortiClient VPN applies geofencing at the VPN gateway level within the SSL VPN settings,

allowing connections only from US-based IP addresses. To safeguard against proxies and anonymizers, application security has been implemented in the FortiClient application, blocking proxy traffic at the host level.

Palo Alto VPN applies geofencing at both the security policy and gateway levels. Only traffic originating from US-based IP addresses will be allowed to connect through the gateway.

Both security policy and proxy block rule screenshot available in dropbox. Foldername: 'VPN Security'

- **Do you handle CMS data via email? If so, what data?**

>> The BrokerEngage [EDE] Platform does send out emails triggered based on different events in quoting and enrollment process. Typically, these emails include quotes/proposals, plan comparisons, enrollment confirmations etc. We have attached a document with screenshots & notes that describes the events and the emails. We are not sure about the question about what constitutes CMS data but the document includes email examples generated from the BrokerEngage EDE Platform. Filename: BrokerEngage: Agent Experience & Communications

- **When CMS data requires emailing, who receives it and at what email addresses? Please provide evidence.**

>> The emails generated from the BrokerEngage EDE Platform are sent to the related customer and/or to the Agent on Record. Filename: BrokerEngage: Agent Experience & Communications and BrokerEngage: Customer Consent

- **When CMS data requires emailing, who sends it and from what email addresses? Please provide evidence.**

>> All emails that are sent from the platform are systematically generated and go out from noreply@benefitalign.com. Please see attached document for samples. Filename: BrokerEngage: Agent Experience & Communications and BrokerEngage: Customer Consent

- **Do you use any O365 technologies to handle, process or direct CMS data?**

>> The BrokerEngage EDE Platform does not use any O365 technologies to handle, process or direct any emails that are sent from the platform.

Again, we believe it would be better to have a call to go over any additional questions you may have. Thank you.

Regards,

-Dave

---

**David V. Paradis**  
**Primary contact #** **REDACTED**

# Exhibit O

**From:** [Paradis, David \(CMS/OIT\)](#)  
**To:** [Manal Mehta](#)  
**Cc:** [Nettles, Leslie \(CMS/OIT\)](#); [Lyles, Darrin \(CMS/CCIIO\)](#); [Ashwini Deshpande.](#); [Hunt, Patrick \(CMS/OIT\)](#); [Busby, Keith \(CMS/OIT\)](#); [Montz, Ellen \(CMS/CCIIO\)](#); [Kania, Michael \(CMS/OIT\)](#); [Sonu S. Rajamma](#); [Dorsey, Kevin Allen \(CMS/CCIIO\)](#); [Girish Panicker](#); [Tamara White](#); [Berry, Dawn \(CMS/OIT\)](#); [Kalpit Dantara](#); [Grant, Jeff \(CMS/CCIIO\)](#); [CMS CCIIO Office of the Director](#); [Shynihan Muhammed](#); [Paradis, David \(CMS/OIT\)](#)  
**Subject:** RE: CMS/Speridian  
**Date:** Wednesday, August 28, 2024 12:13:02 PM  
**Attachments:** [image001.png](#)

---

All,

Thank you for your continued support. Can you please provide the below?

- Please provide all available VPC Flow Logs for all AWS accounts under the control of Speridian/BenefitAlign/True Coverage in raw form with no filters applied.
- Speridian/True Coverage previously indicated that access to AWS infrastructure is restricted to authorized employees in CONUS with whitelisted IP addresses. CMS SOC has determined that IP addresses associated with anonymizing VPN services have been considered allowed traffic. Please provide a list of all whitelisted IP addresses and documentation on the standard procedure to verify and vet IP addresses to whitelist.
- Speridian/True Coverage previously indicated that the VPN services they operate apply geofencing controls to prevent users who are OCONUS from accessing the VPN. Please provide details on any controls in place that disallow the use of anonymizing VPN services that mask the true geolocation of the user who is attempting to connect to your VPN.
- Please provide details and documentation on the implementation of geographic restrictions for all traffic exiting the VPN, if any are in place.
- Please provide details and policy on the acceptable use of TeamViewer within your environment, if any exist.

Regards,  
-Dave

---

**David V. Paradis**

**Primary contact #** **REDACTED**

*INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW: This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.*

---

**From:** Manal Mehta **REDACTED**  
**Sent:** Thursday, August 22, 2024 10:25 AM  
**To:** Paradis, David (CMS/OIT) **REDACTED**



UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

BENEFITALIGN, LLC, et al.,

Plaintiffs,

v.

CENTERS FOR MEDICARE & MEDICAID  
SERVICES, et al.,

Defendants.

Civil Action No. 24-2494 (JEB)

**DECLARATION OF JEFF WU**

I, Jeff Wu, pursuant to 28 U.S.C. § 1746, and based upon my personal knowledge, information I have reviewed in the records of the U.S. Department of Health and Human Services (HHS) and its subsidiary agencies, or on information provided to me by HHS employees and contractors, hereby make the following declaration with respect to the above-captioned matter:

1. I currently serve as the Deputy Director for Policy in the Center for Consumer Information & Insurance Oversight (CCIIO) at the Centers for Medicare & Medicaid Services (CMS), a component within HHS. In my role as a CCIIO Deputy Director, I oversee policy for the commercial health insurance market, including the Federally-facilitated Exchange (FFE) and State-based Exchanges on the Federal Platform (SBE-FPs) (collectively, “Exchange”).

2. I graduated from Harvard College in 1992 with a bachelor's degree in economics, and from Stanford Business School and Stanford Law School in 2001 with a master's degree in business administration and a juris doctor degree, respectively. In 2011, I joined CCIIO as a health insurance specialist, and I have served in various policy roles at CCIIO since then. I am currently

the senior member of the career staff responsible for overseeing CCIIO's policy and regulatory activities, including policymaking with respect to the Affordable Care Act.

3. I am aware of, and familiar with, the amended complaint and amended motion for temporary restraining order and preliminary injunction filed by BenefitAlign, LLC and TrueCoverage, LLC, captioned *BenefitAlign, LLC v. Centers for Medicare & Medicaid Services*, Case No. 24-02494 (JEB) (D.D.C.) (filed Sept. 6, 2024). On August 8, 2024, CMS suspended the Speridian Companies'<sup>1</sup> ability to transact information with the Exchange after CMS's internal analysis identified a serious lapse in the security posture of the Speridian Companies' platforms, namely that the Speridian Companies' platforms may be accessed by non-CMS approved systems outside of the United States, in violation of the Speridian Companies' Agreements with CMS. On September 2, 2024, CMS sent the Speridian Companies a formal written notice explaining the basis of the suspension. The notice also explained that the suspension would remain in place while CMS conducts an audit of the Speridian Companies and until CMS is satisfied that the issues described in the notice are remedied or sufficiently mitigated. Exhibit A is a true copy of the email notice that CMS sent to Speridian [email dated 09/02/24 from Jeff Grant, CCIIO Deputy Director for Operations to Girish Panicker, Tamara White, Manal Mehta, Sarika Balakrishnan, and Ashwini Deshpande].

- a. Transmitting and storing sensitive, personal data or government-related data to foreign entities constitutes a breach of the privacy and security standards set forth in OMB A-130.2 This directive mandates that federal agencies protect information resources and ensure that sensitive data, especially consumer personally identifiable information (PII) such as full names, date of births, and social security numbers, is not exposed to unauthorized entities. At the conclusion of CMS's audit, CMS will advise the Speridian Companies of its findings and the Speridian Companies will have the opportunity to rebut those findings and challenge and final agency action, if any is imposed.

---

<sup>1</sup> The Speridian Companies encompass Speridian Global Holdings, LLC; Speridian Technologies, LLC; BenefitAlign, LLC; TrueCoverage, LLC; and True Coverage, LLC dba Inshura.com.

- b. The unauthorized transmission of sensitive data, including consumer PII, increases the risk of identity theft and financial fraud. Consumers whose data is compromised could face significant financial losses, damage to their credit, and long-term difficulties in reclaiming their identity and restoring their financial standing. CMS has an obligation to protect consumers from this type of harm occurring from improper practices in its programs and through the Exchange.
  - c. Such unauthorized transmissions of data may also result in the unauthorized use of consumer data, including PII, which may result in consumers being unknowingly disenrolled from their current Exchange plan, newly enrolled in an Exchange plan, or switched to a new Exchange plan altogether without their knowledge or consent. Such changes can affect how much consumers must pay towards their premiums, coinsurance, copays, and deductibles for every visit and doctor type, as well as the amount of financial assistance consumers may or may no longer qualify for. This can result in serious health care impacts (for example, not receiving life-saving medication or necessary medical procedures) as well as unexpected financial responsibility burdens for the consumers.
  - d. The mishandling of sensitive data undermines consumer trust in the organizations responsible for safeguarding their information. This loss of trust can have wide-reaching consequences, including reluctance to engage in online transactions – particularly in relation to the Exchange, potentially resulting in loss of access to needed health care.
4. Agents and brokers who previously utilized the BenefitAlign direct enrollment platform may submit enrollments to the Exchange through other avenues, and the impact on these agents' and brokers' ability to assist consumers with Exchange enrollments will be modest.
- a. While BenefitAlign's direct enrollment platform remains suspended, agents and brokers that previously utilized the BenefitAlign direct enrollment platform may elect to use another Enhanced Direct Enrollment (EDE) Entity's approved platform, the Exchange Call Center, or HealthCare.gov itself to assist consumers. Accordingly, the suspension of Speridian Companies' ability to transact information with the Exchange does not present a significant risk to consumers' ability to enroll in, maintain, or make changes to their Exchange coverage.
  - b. Consumers may elect to be assisted by any agent or broker of their choosing at any point in time or elect to enroll in Exchange coverage without agent or broker support through HealthCare.gov or an alternative EDE consumer pathway. Through an EDE consumer pathway, consumers create their own

account on the EDE partner's website, undergo identity proofing, complete the Exchange eligibility application, and are able to enroll in a plan. The application questions and eligibility determination will be the same on an EDE partner's website as on HealthCare.gov, but the EDE partner's website often offers additional, streamlined features on their user interface. Consumers may also work with the Exchange Call Center to speak with a consumer service representative for support, with or without the assistance of an agent, broker, Navigator, or other assister.

- c. There are many other enrollment assisters and channels available to consumers who would like assistance applying for or enrolling in Exchange coverage, including approved direct enrollment platforms (11 others), web-brokers (12), health insurance agencies, independent agents and brokers (approximately 79,795 completed training and registration), Navigators (approximately 2,316 funded by the FFE), and other assisters (approximately 5,970) that are available to consumers who would like assistance applying for or enrolling in Exchange coverage.

5. CMS is pursuing a compliance audit to reach conclusive findings in order to make a final determination regarding Speridian Companies' actions and ability to transact information with the Exchange. The Speridian Companies have a history of noncompliance with CMS regulations and agreements dating back to 2018 and it is imperative for CMS to have confidence in the security of the Speridian Companies' systems for the benefit and safety of millions of Exchange consumers and their data.

- a. On April 19, 2018, TrueCoverage had its 2018 CMS agreements terminated, which ended their ability to transact information with the Exchange, due to the severe nature of their suspected and, in some cases, admitted violations of CMS regulations. The Speridian Companies admitted that their agents and brokers submitted false Social Security Numbers in connection with Exchange eligibility applications, and CMS had reasonable, un rebutted suspicions of other fraud, improper enrollments, and misconduct by the Speridian Companies. CMS's termination applied only for Plan Year 2018.
- b. On October 3, 2022, CMS suspended TrueCoverage dba Inshura.com for noncompliance for failing to implement procedures to verify consumer identity as required by the CMS EDE guidelines. The suspension was lifted when True Coverage dba Inshura.com instituted complaint procedures for consumer identity proofing.

- c. On April 6, 2023, CMS suspended BenefitAlign for attempting to access the CMS software testing environment for the Exchange from India on March 8, 2023. This suspension was lifted after BenefitAlign submitted a corrective action plan to remediate the issue.
  
- d. CMS has also corresponded with the Speridian Companies on a near monthly basis on a variety of noncompliance issues that did not rise to the level of requiring a system suspension but nonetheless raised consumer protection and other concerns on the part of CMS.

I declare under penalty of perjury under the law that the foregoing is true and correct.

Jeffrey C. Wu -S<sub>S</sub> Digitally signed by Jeffrey C. Wu -  
Date: 2024.09.20 17:53:38 -04'00'

---

Jeff Wu

Dated: September 20, 2024

# **Exhibit A**

**From:** Grant, Jeff (CMS/CCIIO) [REDACTED]

**Date:** Monday, September 2, 2024 at 5:32 PM

**To:** [REDACTED]

**Cc:** Bierer, Brett (HHS/OGC) <[REDACTED]> Tischbein, Cory (HHS/OGC)

**Subject:** Notice of Suspension and Audit

Please see the attached Notice of Immediate Suspension and Audit.

Jeffrey D. Grant  
Deputy Director for Operations  
Center for Consumer Information and Insurance Oversight  
Centers for Medicare & Medicaid Services

DEPARTMENT OF HEALTH AND HUMAN SERVICES  
Centers for Medicare & Medicaid Services  
Center for Consumer Information and Insurance Oversight  
200 Independence Avenue SW  
Washington, DC 20201



September 2, 2024

**VIA ELECTRONIC MAIL AND UNITED STATES POSTAL SERVICE:**

TrueCoverage LLC  
c/o Ashwini Deshpande  
2400 Louisiana Blvd NE  
Building 3, Suite 100  
Albuquerque, NM 87110

TrueCoverage LLC dba Inshura  
c/o Ms. Sarika Balakrishnan  
2400 Louisiana Blvd NE  
Building 3, Suite 100  
Albuquerque, NM 87110

BenefitAlign LLC  
c/o Manal Mehta and Tamara White  
2400 Louisiana Blvd NE  
Building 3  
Albuquerque, NM 87110

**RE: Suspensions of Web-broker and Enhanced Direct Enrollment Entity Activities  
and Notice of Compliance Audit**

Dear Ashwini Deshpande, Sarika Balakrishnan, Manal Mehta, and Tamara White:

The Centers for Medicare & Medicaid Services (CMS), on behalf of the Department of Health and Human Services (HHS), administers the program under which licensed web-brokers may operate non-Marketplace websites or information technology (IT) platforms. Using these websites and platforms, agents and brokers may assist with consumer health insurance enrollments through the Federally-facilitated Marketplaces (FFMs) and State-based Marketplaces on the Federal Platform (SBM-FPs) (collectively, Marketplace or Marketplaces).

Pursuant to 45 C.F.R. §§ 155.220(c)(4)(ii) and 155.221(e), and attributable to credible allegations of misconduct described in this notice, CMS is immediately suspending True Coverage LLC's, TrueCoverage dba Inshura's, and BenefitAlign's (collectively, the Speridian



Companies<sup>1</sup>) ability to transact information with the Marketplaces. CMS is also suspending the Speridian Companies' ability to make its non-Marketplace websites available to other agents and brokers to transact information with the Marketplaces. Pursuant to 45 C.F.R. § 155.220(c)(5) and section X.m. of the executed Enhanced Direct Enrollment (EDE) Agreement, section X.l. of the executed Web-Broker Agreement, and section 15 of the executed Interconnection Security Agreement (ISA), CMS also notifies the Speridian Companies of its intent to conduct a compliance review and audit.

## Background

CMS operates a program through which approved web-brokers registered with CMS may host an application for Marketplace coverage on their own websites. Such entities operate as Direct Enrollment (DE) or EDE entities<sup>2</sup> and must comply with the requirements of section 1312(e) of the Patient Protection and Affordable Care Act and associated regulations, including 45 C.F.R. §§ 155.220 and 155.221.

In accordance with federal requirements, the Speridian Companies voluntarily executed the following agreements with CMS to participate in the Marketplace as an approved web-broker and DE/EDE partner, effective for plan years 2022, 2023, and 2024 (collectively, the CMS Agreements):

- Agreement Between Web-Broker TrueCoverage, LLC and CMS for the Individual Market FFM and SBM-FP;
- Agreement Between Web-Broker BenefitAlign, LLC and CMS for the Individual Market FFM and SBM-FP;
- EDE Agreement between EDE Entity BenefitAlign LLC and CMS for the Individual Market FFM and SBM-FP;
- EDE Agreement between EDE Entity TrueCoverage dba Inshura and CMS for the Individual Market FFM and SBM-FP; and

---

<sup>1</sup> Speridian Global Holdings LLC has common ownership and control of TrueCoverage, Inshura, and BenefitAlign, and their IT platforms for participating in the Marketplaces operate on the same IT infrastructure. This suspension notice collectively addresses all three entities as the Speridian Companies.

<sup>2</sup> "Direct Enrollment is a service that allows approved Qualified Health Plan (QHP) issuers and third-party web-brokers (online insurance sellers) to enroll consumers in Exchange coverage, with or without the assistance of an agent/broker, directly from their websites. In the 'Classic' DE experience ... consumers start on a DE entity's (e.g., issuer or web-broker) website by indicating they are interested in Exchange coverage. The issuer or web-broker redirects users to HealthCare.gov to complete the eligibility application portion of the process. After completing their eligibility application, HealthCare.gov redirects the user back to the issuer or web-broker website to shop for a plan and enroll in Exchange coverage.... The Enhanced Direct Enrollment user experience goes well beyond the plan shopping and enrollment experience that is available via Classic DE. EDE is a service that allows approved EDE entities (e.g., QHP issuers and web-brokers approved to participate in EDE) to provide a comprehensive consumer experience including the eligibility application, Exchange enrollment, and post-enrollment year-round customer service capabilities for consumers and agents/brokers working on behalf of consumers, directly on issuer and web-broker websites. Through EDE, approved EDE Entities build and host a version of the HealthCare.gov eligibility application directly on their websites that securely integrates with a back-end suite of FFE application programming interfaces (APIs) to support application, enrollment and more. " *Direct enrollment and enhanced direct enrollment*. CMS.gov. (n.d.). <https://www.cms.gov/marketplace/agents-brokers/direct-enrollment-partners>

- ISA between EDE Entity BenefitAlign LLC and CMS for the Individual Market FFM and SBM-FP.

The Speridian Companies signed and executed the CMS Agreements, thus voluntarily agreeing to accept and abide by the terms of the CMS Agreements and the federal regulations governing Marketplace web-brokers and DE/EDE partners at 45 C.F.R. §§ 155.220 and 155.221.<sup>3</sup> These terms and regulations provide, in relevant part, the right for CMS or its designee to conduct compliance reviews and audits, including the right to interview employees, contractors, and business partners of an EDE Entity and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of the web-broker's and EDE Entity's compliance with applicable requirements.<sup>4</sup>

### **The Speridian Companies' Previous Record of Noncompliance with CMS Regulations and Agreements**

The Speridian Companies have a history of noncompliance with CMS regulations and agreements dating back to 2018. On April 19, 2018, TrueCoverage had its 2018 CMS agreements terminated, which ended their ability to transact information with the Marketplace, due to the severe nature of its suspected and, in some cases, admitted violations of CMS regulations.<sup>5</sup> After the termination, the Speridian Companies were not registered with the Exchanges or permitted to assist with or facilitate enrollment of qualified individuals through the Exchange, including direct enrollment. The Speridian Companies admitted that their agents and brokers submitted false Social Security Numbers in connection with Marketplace eligibility applications, and CMS had reasonable suspicions of other fraud, improper enrollments, and misconduct by the Speridian Companies. The Speridian Companies regained their connection to CMS in 2019 after CMS, satisfied with the good-faith evidence provided, entered into Exchange agreements in Plan Year 2019.

On October 3, 2022, CMS suspended TrueCoverage dba Inshura for noncompliance for failing to implement procedures to verify consumer identity as required by the CMS EDE guidelines.<sup>6</sup> The suspension was lifted when True Coverage dba Inshura instituted procedures for consumer identity proofing. On April 6, 2023, CMS suspended BenefitAlign for attempting to access the FFM's software testing environment from India on March 8, 2023. This suspension was lifted after BenefitAlign submitted a corrective action plan to remediate the issue. Since then, we have corresponded with Speridian Companies on a near monthly basis on a variety of noncompliance issues that did not rise to the level of requiring a system suspension but nonetheless raised consumer protection and other concerns on the part of CMS.

### **The August 8, 2024 Suspension**

CMS began a review of the Speridian Companies' DE platforms after CMS received an

<sup>3</sup> 45 C.F.R. §§ 155.220(a) and 155.221(a)(2). *See also* definition of "web-broker" at 45 C.F.R. § 155.20; EDE Agreement, section II and section III; Web-Broker Agreement section II.

<sup>4</sup> EDE Agreement at section X.m.; Web-Broker Agreement at section X.l.; ISA at section 15

<sup>5</sup> C.F.R. § 155.285(a)(1)(i). Also see 45 C.F.R. § 155.220(d)(3) and (j)(2)(ii). A termination here is distinct from a suspension. When an entity is terminated from the Marketplace its CMS Agreements are voided and the entity cannot assist or facilitate consumer enrollment. The only way to get back onto the Marketplace is to re-apply (if permitted, as was the case with True Coverage's suspension in 2018). A suspension also blocks an entity's ability to interact with the Marketplace, but can be ended if CMS's concerns are remediated.

<sup>6</sup> 45 C.F.R. § 155.221(e) and Section V.C of the EDE Business Agreement

unconfirmed report on July 24, 2024 that the TrueCoverage and BenefitAlign technical teams were based overseas, and allegedly were able to access the True Coverage and BenefitAlign platforms, including consumer PII submitted to those platforms, in violation of CMS rules.<sup>7</sup> ~~BenefitAlign~~ Speridian Companies' DE platforms' technical infrastructure.

On August 6, 2024, CMS began an initial risk assessment of the connection between the Speridian Companies and the Marketplace. This assessment concluded that there existed critical risk to CMS infrastructure and consumers. This assessment was based on the evaluation of five factors: Foreign Ownership, Control, or Influence; Significant Adverse Information; Supply Chain Tier Structure Concerns; Company Product Related Concerns; and the Company Cyber Vulnerabilities.

The Speridian Companies use a hybrid onsite/offshore delivery model, which means that a portion of the software development work and IT support is conducted from overseas locations. This is acceptable, provided that CMS data and consumer PII reside in the United States. Multiple domains tied to the Speridian Companies, however, are based in India, where they operate a large, dedicated data center, and CMS reasonably believes that CMS data, including consumer PII, is processed and/or stored in this location. The company has subsidiaries and operations in Canada, India, Pakistan, Saudi Arabia, Singapore, and the UAE. There may be other locations and subsidiaries that CMS has not yet discovered.

Further, the Speridian Companies, BenefitAlign and True Coverage dba Inshura, are defendants in a pending lawsuit, filed by private parties in 2024, alleging that they engaged in a variety of illegal practices, including violations of the RICO Act, misuse of consumer PII, and insurance fraud that they allegedly carried out by misusing BenefitAlign's access to the Marketplace. Plaintiffs in the lawsuit likewise claim that BenefitAlign allows access to the Exchange from abroad and houses CMS data overseas.

CMS suspended the Speridian Companies' ability to transact information with the Marketplace on August 8, 2024, after a CMS analysis identified a serious lapse in the security posture of the Speridian Companies' platforms; namely, that the Speridian Companies' platforms could be accessed by non-CMS-approved systems outside of the United States. Under CMS's requirements, Marketplace data must always reside in the United States to eliminate the possibility that foreign powers might obtain access to CMS data and information.<sup>8</sup> In addition, the EDE agreement states that EDE entities or their delegated entities, including employees and contracted agents, "cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to EDE Entity's systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America.... This includes any such connection through virtual private networks (VPNs)." <sup>9</sup>

On August 13, 2024, OIT met with the Speridian Companies to discuss CMS's concerns about Marketplace data being accessed or accessible from outside the continental United States (OCONUS). During these meetings and afterward, CMS requested information relevant to its

---

<sup>7</sup> EDE Agreement at section X.n.

<sup>8</sup> "CMS system owners must ensure that CMS data is not processed, transmitted, transferred, or stored outside the United States and its territories." *BR-SAAS-8*, CMS.gov. (n.d.).  
[https://www.cms.gov/tra/Infrastructure\\_Services/IS\\_0250\\_SaaS\\_Business\\_Rules.htm](https://www.cms.gov/tra/Infrastructure_Services/IS_0250_SaaS_Business_Rules.htm).

<sup>9</sup> EDE Agreement, Section X.n.

concerns, including information regarding who could access the platforms and from what geographic locations. CMS sent an initial data request to the Speridian Companies on August 13, 2024, the first of seven requests for data. The Speridian Companies' responses each time either led to more questions or were incomplete, with the August 16, 2024 response omitting some of the requested VPN access logs altogether.

CMS reviewed the data the Speridian Companies provided between August 19 and 28, 2024. CMS identified several issues of continued concern, including concerns that there appeared to be VPN usage which could indicate a party's intent to hide the fact that its systems could be accessed from outside the United States. The review also identified additional concerns regarding connections to internet protocol (IP) addresses in India and Pakistan. The review also revealed that all IP addresses associated with the Speridian Companies indicated that their primary IT infrastructure was operated in India.

By August 28, 2024, CMS made a number of concerning discoveries, including that multiple users logging onto the Speridian Companies' systems with company-provided credentials had been identified as connecting to IP addresses that were geolocated to India. Similarly, multiple users had been recorded as sending traffic to multiple IP addresses that corresponded to resources geolocated overseas, including in Hong Kong, India, Ireland, Japan, Pakistan, and Sweden. CMS requested further information from the Speridian Companies regarding this activity on August 28, 2024, and has yet to receive a response.

Due to these critical concerns, as well as an absence of requested information that the Speridian Companies have failed to provide to CMS, CMS has determined that continuing the August 8, 2024 suspension of the Speridian Companies is necessary and appropriate. Thus far, the data and information provided do not allay CMS suspicions that Marketplace data, including consumer PII, was transferred outside the United States, or that EDE and/or FFM systems are being accessed from outside of the United States.

### **Notice of Intent to Conduct a Compliance Review and Audit**

Pursuant to CMS's authorities at 45 C.F.R. § 155.220(c)(5) and as specified in the CMS Agreements<sup>10</sup>, CMS intends to conduct a compliance review and audit ("Audit") of the Speridian Companies.

On April 12, 2024, private parties filed a civil action in U.S. District Court, *Turner v. Enhance Health, LLC*, Case No.:24-cv-60591 (S.D. Fla.) on behalf of a class of consumers and a class of agents. The pleadings in that case, including the complaint, a motion for expedited discovery, and witness declarations submitted under penalty of perjury, allege that the Speridian Companies committed various acts (described below) that, if true, would constitute noncompliance with the web-broker and DE/EDE program regulations and CMS Agreements,

CMS has a reasonable suspicion, based on credible evidence it has considered, that the Speridian Companies directed its employees and other agents to change Marketplace enrollees' coverage

---

<sup>10</sup> section X.m. of the EDE Agreement, section X.l. of the Web-Broker Agreement, and section 15 of the executed Interconnection Security Agreement



and enroll insured and uninsured consumers without the enrollees' consent; design, publish, and/or clear misleading advertisements; and utilize agents' and brokers' national producer numbers without the agents' or brokers' consent. These circumstances pose unacceptable risk to the accuracy of the Marketplace's eligibility determinations, Marketplace operations, and Marketplace IT systems. These allegations are independent from, but in addition to, the other IT issues mentioned above, in particular the allegations of unauthorized transmission of consumer PII overseas. Any of these allegations, if true, would constitute noncompliance with the web-broker and DE/EDE program regulations and CMS Agreements.

This Audit would build upon the review CMS initiated on August 6, 2024, and would address issues that may or may not have been evaluated or relevant to the OIT review Pursuant to the CMS Agreements, the Speridian Companies are expected to provide reasonable access to their information, employees, and facilities during the course of the Audit.<sup>11</sup> The Speridian Companies are also responsible for ensuring cooperation with the Audit by its downstream and delegated entities, including subcontractors.<sup>12</sup>

The Audit will cover the Speridian Companies' activities beginning on or after October 10, 2020 to the present. The Audit's scope will include, but will not be limited to, a review of the Speridian Companies' business relationships with agents and brokers who are not agents or brokers for a Speridian Company, a review of any call scripts used by Speridian Companies' agents, records of commission payments, IT records and practices, business processes and records, relationships with current and former business partners, and any related issues to these topics that may arise as part of the review of the Speridian Companies' compliance with applicable federal regulations and the CMS Agreements. CMS will follow up with additional information on when the Audit will begin and who will conduct it.

Given the serious risk to the Marketplace and consumers and other circumstances underlying CMS's suspicions, these suspensions will remain in effect until CMS completes its investigation and is satisfied that the issues described in this notice have been remedied or sufficiently mitigated as authorized by 45 C.F.R. §§ 155.220(c)(4)(ii) and 155.221(e). During this suspension and audit period, the Speridian Companies may not offer its non-Marketplace website for use by agents or brokers assisting consumers with Marketplace applications for, and enrollments in, insurance affordability programs or to enroll consumers in a QHP offered through any FFM, FF-Small Business Health Options Program (SHOP), SBM-FP, or SBM-FP-SHOP. Similarly, the Speridian Companies, and any of their upstream DE partners will be unable to transact information with Marketplace systems through Speridian Companies' DE/EDE platforms during this suspension and audit period.

### **CMS System Access Can Only Be Restored Once Concerns are Resolved**

As explained above, pursuant to its obligations to protect the privacy and security of consumer information and CMS IT systems, CMS will not lift the suspensions and restore the Speridian Companies' ability to transact information with the Marketplaces or its ability to make its non-

---

<sup>11</sup> EDE Agreement at section X.m.; Web-Broker Agreement at section X.l.; ISA at section 15.

<sup>12</sup> EDE Agreement, section X.m. Web-Broker Agreement at section X.l.; ISA at section 15. "A QHP issuer direct enrollment technology provider that provides technology services or provides access to an information technology platform to a QHP issuer will be a downstream or delegated entity of the QHP issuer that participates or applies to participate as a direct enrollment entity." 45 C.F.R. § 155.20.

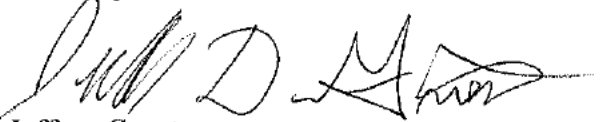
Marketplace website available until the security issues described above have been remedied or sufficiently mitigated to CMS's satisfaction. Further, during this temporary suspension and audit period, the Speridian Companies may not offer its non-Marketplace website for use by agents or brokers assisting consumers with Marketplace applications for, and enrollments in, insurance affordability programs or to enroll consumers in a QHP offered through any FFM, FF-Small Business Health Options Program (SHOP), SBM-FP, or SBM-FP-SHOP. Similarly, Speridian Companies, and any of their upstream DE partners will be unable to transact information with Marketplace systems through Speridian Companies' DE/EDE platforms during this suspension and audit period.

### **Personally Identifiable Information (PII) Protection and Record Retention Requirements**

This suspension does not alter the Speridian Companies' legal obligation to protect and maintain the privacy and security of PII collected in connection with Marketplace applications and enrollments; that obligation remains in full force and effect until such PII is destroyed at the end of the required record retention period. Refer to 45 C.F.R. § 155.260(b) and your CMS Agreements for more information on the obligation to protect the privacy and security of, as well as the accompanying record retention requirements for, PII to which the Speridian Companies gained access to, collected, used, or disclosed in the course of facilitating enrollments through the FFMs, FF-SHOPS, SBM-FPs, and SBM-FP-SHOPS during the term of your CMS Agreements.

Please respond to [REDACTED] if you have any questions or would like to discuss this issue further.

Sincerely,



Jeffrey Grant  
Deputy Director for Operations  
Centers for Medicare & Medicaid Services  
Center for Consumer Information and Insurance Oversight

cc: Speridian Global Holdings LLC

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

BENEFITALIGN, LLC, et al.,

Plaintiffs,

v.

CENTERS FOR MEDICARE & MEDICAID  
SERVICES, et al.,

Defendants.

Civil Action No. 24-2494 (JEB)

**DECLARATION OF JEFFREY GRANT**

I, Jeffrey Grant, pursuant to 28 U.S.C. § 1746, and based upon my personal knowledge and information made known to me in the course of my employment, hereby make the following declaration with respect to the above-captioned matter:

1. I currently serve as the Director for Operation in the Center for Consumer Information and Insurance Oversight (CCIIO) at the Centers for Medicare & Medicaid Services (CMS). In my role as the Deputy Director for Operations, I oversee operations for the Federally-facilitated Exchanges (FFE) and State-based Exchanges on the Federal Platform (SBE-FPs) (hereinafter “Exchanges” or “Exchange”).

2. I obtained a BA in History from the University of Michigan and a Masters of Public Administration from the George Washington University. I then spent 22 years of service as a Navy Reservist. I have over 30 years of experience as an entrepreneurial manager of major health programs in the federal sector, leading the implementation of Affordable Care Act, Medicare Advantage and Medicare Prescription Drug Benefit payment policies, operations, and systems.

3. The Exchanges are a centralized, cloud-based federal platform that manages all data and information related to applications for and enrollments in qualified health plans (QHPs) through the Exchanges. The Exchanges are the authoritative source for all data on the Exchanges: records for QHP enrollees, QHPs, and associated agents and brokers (if any), alongside other personally identifiable information (PII), are stored in the Exchange system.

4. Consumers have the option of working with agents and brokers in the application, enrollment, and post-enrollment processes. Most agents and brokers use the Classic Direct Enrollment (Classic DE) or Enhanced Direct Enrollment (EDE) pathways, which involve private web sites that are connected to the Exchanges. An agent or broker must adhere to CMS registration, licensure, and training requirements in order to utilize an approved Classic DE or EDE platform. When agents and brokers assist consumers in purchasing a plan, the agent or broker's National Producer Number (NPN) is associated with that enrollment and provided to the health insurance issuer so that the agent or broker can receive a commission and other compensation for the sale from the health insurance issuer, subject to agreement between the issuer and the agent or broker.

5. Agents and brokers are required by CMS to search for consumers in the Exchange system prior to creating a new application for that consumer. If a consumer record already exists in the Exchanges, agents and brokers are expected to update the existing application and enrollment, rather than creating a duplicate record. In cases where duplicate records are created, the Exchange system will identify overlapping policies, and the applicable Exchange will end coverage as necessary to prevent duplicate enrollments. Duplicate applications are not deleted.

6. EDE partners are third-party organizations that interface with the Exchanges to streamline the health insurance enrollment process. They integrate their platforms with the Exchanges, allowing consumers to compare, select, and enroll in QHPs directly through their



websites, similar to how HealthCare.gov works. For agents and brokers that use EDE platforms, the platforms include consumer search functionality. To become an EDE partner, a company must submit to a security audit and sign an EDE Agreement, which defines acceptable information technology, privacy, and business practices. Primary EDE partners connect directly to the Exchanges. They can also allow “upstream” partners to use their systems to access the Exchanges indirectly.

7. There are currently eleven active primary EDE partners and seventy-two upstream EDE entities that facilitate enrollments through the FFEs and SBE-FPs. Some agents and brokers work with multiple EDE partners to facilitate enrollments.

8. Web-brokers provide online platforms for agents and brokers (and sometimes, consumers) to compare, select, and enroll in health insurance plans, either by building their own Classic DE or EDE platforms or by functioning as upstream entities. For example, BenefitAlign is a Primary EDE Partner and Web Broker, while TrueCoverage is an Upstream Web Broker Entity of BenefitAlign.

9. EDE Partner platforms sometimes offer non-ACA plans like dental, vision, supplemental, life, disability, and short-term medical insurance. Enrollment into these plans do not require a link to the Exchanges.

10. Agents, brokers, and agencies, including TrueCoverage’s agents, will continue to be able to serve consumers, even while BenefitAlign and TrueCoverage platforms are suspended. Unless contractually restricted, agents and brokers generally can affiliate with multiple insurance agencies simultaneously. They may also work with consumers independently, without association with an insurance agency. Similarly, agents, brokers, and agencies do not lose their book of business or ability to receive commissions or other compensation on existing enrollments when

they move to a different EDE partner: consumer contact information, plan information, and the agent or broker's NPN are stored in the Exchange's system and can be accessed by an agent or broker, so long as the agent or broker has a consumer's written consent to access their information in the Exchange's system.

11. Consumers can remain with their chosen agents or brokers, maintaining continuity and trust in their relationship, regardless of the EDE platform that the agent or broker chooses to use. If a consumer purchased non-ACA services through the Speridian Companies they should still be able to use those services, as they do not require a connection to the FFE. Furthermore, consumers can turn to the Federally-managed Exchange Call Center for support. The Exchange Call Center can access the applications and enrollments of all consumers enrolled through the Exchanges, regardless of whether the enrollment was submitted by an active or suspended EDE partner.

12. Consumers' health insurance coverage and access to care will be unaffected by the Speridian Companies' suspensions. When a consumer enrolls in a QHP through the Exchanges, the insurance issuer receives a notification and the consumer's relevant information. All plan information is captured by the issuer's system. A healthcare provider's office verifies coverage through the insurance issuer, not the consumer's agent or broker: all insurance issuers provide a dedicated phone line and sometimes system portals to healthcare providers so they can verify a consumer's coverage eligibility and details on their plan benefits.

\* \* \*

I declare under penalty of perjury under the law that the foregoing is true and correct.

**JEFFREY GRANT -S** Digitally signed by JEFFREY  
GRANT -S  
Date: 2024.09.20 17:19:51 -04'00'

---

Jeffrey Grant

Dated: September 20, 2024