

UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

BENEFITALIGN, LLC; AND
TRUECOVERAGE, LLC,

Plaintiffs,

v.

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

Defendants.

Case No.: 1:24-cv-02494-JEB

**AMENDED MOTION FOR PRELIMINARY INJUNCTION AND REQUEST FOR
EXPEDITED HEARING**

Plaintiffs Benefitalign, LLC and TrueCoverage, LLC (“Plaintiffs”) move this Court for both a Temporary Restraining Order and a Preliminary Injunction enjoining the Centers for Medicare and Medicaid Services (“CMS”) from suspending Plaintiffs’ access to CMS’ Data Services Hub (“CMS Network”). Plaintiffs request leave to withdraw their prior Motion for Temporary Restraining Order and Preliminary Injunction (ECF No. 2).

Dated: September 6, 2024

Respectfully submitted,

/s/ Amy E. Richardson

Amy E. Richardson, Esq. (DC Bar # 472284)

Patrick P. O’Donnell (DC Bar # 459360)

Walter E. Anderson, Esq. (DC Bar # 975456)

HWG LLP

1919 M Street NW, 8th Floor

Washington, DC 20036

Tel.: 202-730-1329

Email: arichardson@hwglaw.com

*Counsel for Plaintiffs Benefitalign, LLC and
TrueCoverage, LLC*

**UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA**

BENEFITALIGN, LLC,
TRUECOVERAGE, LLC
Plaintiffs,

v.

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

Defendant.

Case No.: 1:24-cv-02494-JEB

**MEMORANDUM IN SUPPORT OF PLAINTIFFS' AMENDED MOTION FOR
TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION AND
REQUEST FOR EXPEDITED HEARING**

Dated: September 6, 2024

Amy E. Richardson, Esq. (DC Bar # 472284)
Patrick P. O'Donnell (DC Bar # 459360)
Walter E. Anderson, Esq. (DC Bar # 975456)
HWG LLP
1919 M Street NW, 8th Floor
Washington, DC 20036
Tel.: 202-730-1329
Email: arichardson@hwglaw.com

*Counsel for Plaintiffs Benefitalign, LLC and
TrueCoverage, LLC*

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY OF ARGUMENT 1

STATEMENT OF FACTS..... 3

ARGUMENT..... 9

I. CMS’s Arbitrary Suspension Is Lawless in at Least Three Different Ways..... 9

1. CMS Violated the Administrative Procedure Act by Violating HHS Regulations..... 9

2. The Relevant Information Security Requirement Pertains Specifically to Information Systems that Connect or Transmit Data to the Marketplace or Its Testing Environments..... 10

3. CMS Does not, and Cannot, Establish that the EDE Platform Violates Any Requirement..... 11

4. CMS Merely Feels the Possibility of a Violation by Plaintiffs..... 13

5. CMS’s Indefinite Suspension of Plaintiffs Based on Generalized Suspicions Violates its Own Regulations 15

6. CMS Cites Only Unfounded Claims in a Lawsuit to Justify Expanding Its Suspension to TrueCoverage’s Web-Broker Activities..... 16

7. CMS’s Decision is Arbitrary and Capricious. 17

8. CMS Violated the Due Process Clause of the Constitution. 19

II. CMS’s Suspension Threatens Immediate, Irreparable Harm to TrueCoverage and Beneficialign. 20

III. The Balance of Equities Favors a Preliminary Injunction to Maintain the Status Quo, and CMS’s Suspension Undermines the Public Interest by Chilling Consumers’ Ability to Access Affordable Healthcare Plans and Receive Service for Current Health Plans. 22

CONCLUSION 25

TABLE OF AUTHORITIES

Cases

Aamer v. Obama, 742 F.3d 1023 (D.C. Cir. 2014)..... 9

Am. Wild Horse Pres. Campaign v. Perdue, 873 F.3d 914 (D.C. Cir. 2017)..... 17

Elevance Health, Inc. v. Becerra, No. CV 23-3902 (RDM), 2024 WL 2880415
(D.D.C. June 7, 2024) 16

Gen. Elec. Co. v. Jackson, 610 F.3d 110 (D.C. Cir. 2010)..... 19

Judulang v. Holder, 565 U.S. 42 (2011)..... 17, 18

Mathews v. Eldridge, 424 U.S. 319 (1976)..... 19

Michigan v. EPA, 576 U.S. 743 (2015) 17

Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463
U.S. 29 (1983)..... 17

N. Am. Butterfly Ass’n v. Wolf, 977 F.3d 1244 (D.C. Cir. 2020)..... 19

Pursuing Am.’s Greatness v. Fed. Election Comm’n, 831 F.3d 500 (D.C. Cir.
2016) 9

U.S. Lines, Inc. v. Fed. Mar. Comm’n, 584 F.2d 519 (D.C. Cir. 1978)..... 16

Statutes

42 U.S.C. § 18032(e) 18

5 U.S.C. § 706(2)(A)..... 9, 17

5 U.S.C. § 706(2)(D)..... 9

Regulations

45 C.F.R. § 155.220(c)(4)(ii) 6, 10, 15, 18

45 C.F.R. § 155.221(e)..... 6, 10, 15, 18

Other Authorities

A quick guide to the Health Insurance Marketplace, HealthCare.gov 7

About Us, Speridian Technologies..... 12

An Overview for New and Existing Web-brokers, CMS..... 3

Consumer Information and Insurance Oversight, CMS..... 3

Direct Enrollment and Enhanced Direct Enrollment, CMS..... 4

Entities Approved to Use Enhanced Direct Enrollment, CMS..... 2, 16

Getting Started with Remote Access to the CMS Network, CMS 12

Health Insurance Marketplaces, CMS 3

Need health insurance?, HealthCare.gov 3

INTRODUCTION AND SUMMARY OF ARGUMENT

On August 8, 2024, the Centers for Medicare and Medicaid Services (“CMS”) cut off Plaintiffs’ access to the CMS databases that underlie healthcare.gov, with no meaningful notice or explanation, in violation of its own regulations. For the next three weeks, in hopes of achieving a swift resolution, Plaintiffs fully cooperated with all CMS requests for information. Yet, CMS maintained the suspension, and it still did not offer a cogent explanation as to why. On August 29, 2024, their businesses threatened with insolvency, Plaintiffs filed their Complaint and sought emergency relief from this Court. On September 2, 2024, after Plaintiffs sought relief, CMS delivered a letter to Plaintiffs attempting to address the suspension in writing. CMS’s *post hoc* notice, however, does not meet CMS’s own standards for an ongoing suspension. Because the ongoing suspension is unlawful and is guaranteed to shutter Plaintiffs’ businesses, Plaintiffs seek emergency relief.

CMS’s arbitrary and indefinite suspension violates HHS regulations, the Administrative Procedure Act (“APA”), and the Due Process Clause. CMS attempted to cure these violations with a letter asserting data-security concerns, but its claims—offered without any evidence at all—do not satisfy the requirements for a suspension under either of the regulations it invokes. *See Ex. 1 at 4* (“Suspension Notice”). CMS’s rationale would deny data access to a platform operated by any company (1) whose corporate parent has international operations wholly unconnected to, and firewalled from, the company’s ACA exchange business; (2) whose employees access the company’s servers using virtual private networks (“VPN”) to ensure secure network connections; or (3) whose employees access overseas websites, while they are working. CMS’s rationale would also permit suspension of any brokerage based on unproven allegations in a private lawsuit. In short, CMS has not alleged, much less demonstrated, any violation of CMS rules. Instead, CMS has described activities that are commonplace across corporate

America, including among Plaintiffs' competitors, none of whom CMS has suspended to date.

See Entities Approved to Use Enhanced Direct Enrollment, CMS (Aug. 9, 2024),

<https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance->

[Marketplaces/Downloads/EDE-Approved-Partners.pdf](https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/EDE-Approved-Partners.pdf) (last visited September 6, 2024).

The suspension is an imminent threat to Plaintiffs' existence because the overwhelming majority of Plaintiffs' revenue comes from operating business platforms that rely on access to the ACA exchanges. Plaintiffs have already lost a substantial number of customers and agents. *See Panicker Am. Decl.* ¶ 22. If CMS continues the suspension into the period immediately preceding the ACA's open enrollment period, Plaintiffs are almost certain to lose their remaining customers and agents and very unlikely to get them back. *See Panicker Am. Decl.* ¶ 22. That would have dire consequences: Plaintiffs will be unable to repay bank loans, pay employees, or cover other expenses—in other words, continue to operate their businesses. *Panicker Am. Decl.* ¶ 29. Plaintiffs' only hope of salvaging their businesses is to regain access to CMS data in very short order, both to prevent the mass customer and agent exodus, and to give Plaintiffs time to prepare for ACA open enrollment season, which begins November 1, 2024. *Panicker Am. Decl.* ¶ 23. CMS's suspension does not just threaten Plaintiffs' businesses; it has a significant impact on third parties, including consumers. Every day that the suspension continues denies consumers the ability to use Plaintiffs' EDE Platform to access to affordable healthcare plans, prevents brokers and agents from doing so to access customer records for existing insurance plans, and denies insurance carriers and doctors the ability to confirm the existence and scope of customers' health coverage through those platforms. *Panicker Am. Decl.* ¶ 30.

CMS's suspension is plainly unlawful in several ways, threatens irreparable harm to Plaintiffs, and causes substantial harm to the public interest. Accordingly, under applicable law, both a temporary restraining order and preliminary injunction are warranted.

STATEMENT OF FACTS

The Affordable Care Act, among other things, sought to create a competitive private health insurance market through the creation of exchanges or "Health Insurance Marketplaces." *See Health Insurance Marketplaces*, CMS, <https://www.cms.gov/marketplace/about/overview-exchanges> (last visited Aug. 13, 2024). Through the website [healthcare.gov](https://www.healthcare.gov), consumers, agents, and brokers can search these marketplaces for qualified health plans eligible for tax credits that subsidize the consumer's healthcare costs. *See Need health insurance?*, HealthCare.gov, <https://www.healthcare.gov/get-coverage/> (last visited Aug. 13, 2024). CMS, a component of HHS, oversees implementation of the ACA and operation of the marketplaces. *See Consumer Information and Insurance Oversight*, CMS, <https://www.cms.gov/marketplace/about/oversight> (last visited Aug. 13, 2024).

A thicket of jargon has grown from the soil of the Affordable Care Act, including two terms particularly relevant to this case: Federally Facilitated Marketplaces ("FFMs") and State-based Marketplaces on the Federal Platform ("SBM-FPs"). Because the distinction between the two is not relevant to this motion, we refer to them as Marketplace or Marketplaces for the sake of readability, as does CMS. *See Suspension Notice* at 1.

In addition to making [healthcare.gov](https://www.healthcare.gov) available, HHS allows private entities to access the Marketplace. Some entities, known as "web brokers," provide websites that allow consumers to select and enroll in qualified health plans. *See An Overview for New and Existing Web-brokers*, CMS (Oct. 2017) <https://www.cms.gov/files/document/processes-becoming-web-broker.pdf> (last visited Sept. 5, 2024). Other entities, known as "direct enrollment" or "enhanced direct

enrollment” entities, build their own platforms that allow consumers, agents, and brokers to access the ACA Marketplaces. *See Direct Enrollment and Enhanced Direct Enrollment*, CMS, <https://www.cms.gov/marketplace/agents-brokers/direct-enrollment-partners> (last visited Aug. 13, 2024). A “direct enrollment” entity builds a web interface that redirects users to healthcare.gov to complete an application, whereas an “enhanced direct enrollment” entity can access CMS’s data directly, thereby avoiding the need to redirect users to healthcare.gov. *Id.*

CMS approved Plaintiff Benefitalign as an “enhanced direct enrollment” entity. Panicker Am. Decl. ¶ 4. It delivers end-to-end technology solutions for Benefits Administration and Customer Relationship Management across all lines of business for carriers, agencies, brokers, and employers. Panicker Am. Decl. ¶ 4. Benefitalign offers its BrokerEngage™ EDE Platform as a white-labelled solution to carriers, agencies, and agents/brokers. Panicker Am. Decl. ¶ 4. Plaintiff TrueCoverage, through its “Inshura” brand, has CMS approval to offer a free, white-labelled health plan-quoting and enrollment version of Benefitalign’s BrokerEngage™ Platform to agencies and agents/brokers. Panicker Am. Decl. ¶ 5. TrueCoverage d/b/a Inshura markets this offering as the Inshura EDE Platform. Panicker Am. Decl. ¶ 5.

Plaintiff TrueCoverage, operating as TrueCoverage, offers a private health insurance venue for individuals, families, and employers. It is a “One-Stop-Insurance Shop” where consumers and agents (on behalf of consumers) can shop, compare, and enroll in qualified health insurance plans under the Affordable Care Act. TrueCoverage offers insurance plans from more than 600 top carriers across the country. Panicker Am. Decl. ¶ 5. TrueCoverage is an approved web-broker pursuant to 45 C.F.R. § 155.220. Panicker Am. Decl. ¶ 5.

After business hours on August 8, 2024, an official at CMS sent the following two-sentence email to Benefitalign and Inshura/TrueCoverage: “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.” Panicker Am. Decl., Ex.

A. CMS offered no other reason for, or information about, its decision.

For the next three weeks, Plaintiffs engaged with CMS staff and attempted to identify and resolve any concerns. Panicker Am. Decl. ¶¶ 15–19. Plaintiffs answered multiple questions from CMS staff and provided all data that they requested. Panicker Am. Decl. ¶ 16. Plaintiffs’ platforms, however, remained cut off from EDE access for the entire three-week period, with no explanation, and no end in sight. Panicker Am. Decl. ¶ 19.

On August 29, 2024, facing the imminent collapse of their businesses, Plaintiffs could wait no longer and sought relief from this Court. Four days later, CMS, for the first time, sent a written notice attempting to explain the suspension. That notice asserts that “[p]ursuant 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” Plaintiffs. *See* Suspension Notice at 1.¹ Further, the Suspension Notice apparently expanded the suspension to cover “web broker” activities” (not just “EDE/DE/EBP” activities) and TrueCoverage itself (not just TrueCoverage d/b/a Inshura, as the August 8 email did). Suspension Notice at 1.

The Suspension Notice then goes on to discuss a litany of “concerns,” “suspicions,” “allegations,” and allegations that CMS “reasonably believes” about possible overseas access to CMS data. The letter does not, however, include evidence of any actual violation, citing limited facts that are themselves entirely innocuous and commonplace, as explained below. In short,

¹ The Suspension Notice also claims that “the Speridian Companies have a history of noncompliance with CMS regulations and agreements dating back to 2018” citing events from April 2018, October 2022 and April 2023. Suspension Notice at 3. CMS’s summaries of those events, however, are incomplete, often inaccurate, and deeply misleading. None of them are alleged to be ongoing, however, and so they are irrelevant to this motion.

CMS's allegations rely on drawing unsupported and unreasonable inferences from a "hybrid" business model that CMS itself admits is generally proper, and from activity, such as use of VPN connections, that CMS itself publicly endorses.

CMS's technical allegations against Plaintiffs' EDE Platform are either unsupported and conclusory, or they highlight innocuous conduct that is commonplace in a wide swath of businesses. None of the allegations, either alone or taken together, amount to "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), or a "security or privacy incident or breach," 45 C.F.R. § 155.220(c)(4)(ii).

In an apparent attempt to justify expanding its suspension to TrueCoverage's web-broker activities, the Suspension Notice also includes a gratuitous reference to a complaint filed in federal court in Florida. A mere unsupported court complaint cannot justify a company-killing suspension, especially considering that TrueCoverage has not even responded to the complaint.

Plaintiffs' attempts to come to a resolution with CMS have thus far been unsuccessful. On September 4, Plaintiffs proposed a potential interim agreement with Defendants to avoid the need for further litigation. *See* Ex. 2 (Proposed Interim Agreement). In that proposal, Plaintiffs committed to continue their existing practice regarding authorizing only users in the United States to access the EDE Platform and continue segregating the EDE Platform from any overseas IT systems. *Id.* at 1. In addition, Plaintiffs proposed to incorporate a range of additional technical solutions and restrictions to assuage any potential concerns regarding EDE access or PII, and to provide CMS with daily logs for access to the EDE Platform. *Id.* at 2. CMS stated in response that the proposals did not resolve CMS's concerns, but it did not describe what steps

would do so or make any counterproposal. *See* Ex. 3 (Email from B. Bierer to P. O'Donnell, dated Sept. 6, 2024).

CMS's unjustified suspension creates an existential crisis for Plaintiffs, who rely heavily on revenues from supporting entities that participate in the ACA Marketplace. Without access to the healthcare exchanges and the data stored on them, Plaintiffs' businesses cannot function. And if they cannot function, they cannot generate any revenue. Panicker Am. Decl. ¶ 8. They are, in effect, out of business for as long as CMS maintains its cutoff. This abrupt halt imperils the companies, and it hurts the brokers, agents, and customers who access the ACA marketplaces through Plaintiffs. Panicker Am. Decl. *passim*.

Indeed, brokers, agencies, and agents have begun switching to functioning platforms and brokerages. Panicker Am. Decl. ¶ 22. Insurance carriers are likely to do the same. Panicker Am. Decl. ¶ 25. With open enrollment quickly approaching, that trend will accelerate if Plaintiffs are not reinstated. Panicker Am. Decl. ¶ 23. As revenue evaporates, Plaintiffs risk being unable both to pay debt and to compensate employees, either of which will force Plaintiffs to cease operations. Panicker Am. Decl. ¶ 29.

To avoid a mass exodus of brokers, agencies, and agents in advance of open enrollment season—indeed, to have any hope of salvaging their businesses—Plaintiffs need to regain access to CMS data now. ACA open enrollment season begins on November 1, 2024. *See A quick guide to the Health Insurance Marketplace*, HealthCare.gov, <https://www.healthcare.gov/quick-guide/dates-and-deadlines/> (last visited Sept. 6, 2024). If Plaintiffs can retain, regain, or secure new relationships in time for open enrollment, then they have a chance to survive. Panicker Am. Decl. ¶ 23. That all requires regaining access to CMS data immediately. Panicker Am. Decl. ¶ 23. Otherwise, any remaining brokers, agencies, and agents will migrate to functioning

platforms and brokerages, and Plaintiffs will not have time to regain the relationships needed to participate meaningfully in open enrollment. Panicker Am. Decl. ¶ 23.

CMS's proposed remedy is no remedy at all. In the notice, CMS has initiated an audit of Plaintiffs and has decided to leave the suspension in place for the duration of the audit.

Suspension Notice at 6. CMS has still not even begun its audit as of the date of this filing, and audits take months. Panicker Am. Decl. ¶ 18. But months might as well be eternity: absent some change in course, Plaintiffs will be shuttered in weeks. Panicker Am. Decl. ¶ 18. If CMS proceeds with this course of action, there will be no one left standing to audit, and the irreparable harm will be complete. Panicker Am. Decl. ¶ 18.

CMS's arbitrary suspension harms more than just Plaintiffs. With Plaintiffs' platforms shut down, brokers, agencies, and carriers have lost access to a key tool that, for years, has allowed them to help consumers shop for and enroll in affordable healthcare plans. Panicker Am. Decl. ¶ 35. Moreover, consumers who already purchased plans through Plaintiffs' platforms have lost access to their customer records, which will prevent brokers from answering important questions about the scope of consumers' coverage under their existing plans. Panicker Am. Decl. ¶ 37. Consumers will also lose the ability to ask their brokers to make changes to their existing plans or to obtain documentation proving that they have health coverage. Panicker Am. Decl. ¶ 37. Likewise, insurance carriers will not be able to verify that a particular consumer is actively enrolled in one of the carrier's health plans, nor will the carrier be able to answer questions about services that are covered by their plan. Panicker Am. Decl. ¶ 38.

CMS's suspension of Plaintiffs' platforms is unlawful. It is threatening Plaintiffs' very existence. And it is needlessly depriving consumers, brokers, agents, and carriers access to

Plaintiffs' platforms. Plaintiffs seek immediate relief in order to resume providing these essential services to Americans who need affordable health insurance.

ARGUMENT

A plaintiff seeking a temporary restraining order or preliminary injunctive relief “must establish [1] that he is likely to succeed on the merits, [2] that he is likely to suffer irreparable harm in the absence of preliminary relief, [3] that the balance of equities tips in his favor, and [4] that an injunction is in the public interest.” *Aamer v. Obama*, 742 F.3d 1023, 1038 (D.C. Cir. 2014). Where, as here, a government agency is a defendant, the last two factors merge and are “one and the same, because the government’s interest *is* the public interest.” *Pursuing Am. ’s Greatness v. Fed. Election Comm’n*, 831 F.3d 500, 511 (D.C. Cir. 2016). Each of these factors justifies both a temporary restraining order and a preliminary injunction.

I. CMS’s Arbitrary Suspension Is Lawless in at Least Three Different Ways.

CMS’s suspension is unlawful in at least three different ways. First, the suspension contradicts CMS’s own regulations, which violates the Administrative Procedure Act (“APA”). Second, the suspension is arbitrary and capricious, which also violates the APA. Third, the suspension deprives Plaintiffs of property in a manner that violates the Due Process clause. Because the law and facts are clear, Plaintiffs will succeed on each of these claims.

1. CMS Violated the Administrative Procedure Act by Violating HHS Regulations.

The APA provides that courts must “hold unlawful and set aside agency action” that is “not in accordance with law” or is “without observance of procedure required by law.” 5 U.S.C. §§ 706(2)(A), (D). After Plaintiffs were forced to seek emergency relief from this Court, CMS invoked two regulations as authorizing the extraordinary action it had already taken against Plaintiffs: 45 C.F.R. §§ 155.220(c)(4)(ii) and 155.221(e). Suspension Notice at 1.

The first regulation provides 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.

45 C.F.R. § 155.220(c)(4)(ii) (emphasis added). Under the second regulation, CMS may suspend a direct enrollment entity only if it “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). But CMS’s purported “credible allegations of misconduct described in this notice” do not satisfy either standard. Suspension Notice at 1.

2. *The Relevant Information Security Requirement Pertains Specifically to Information Systems that Connect or Transmit Data to the Marketplace or Its Testing Environments.*

As the foundation for an alleged violation of the broad regulatory standards, CMS identifies only one specific requirement: a contract term providing that Plaintiffs

[C]annot remotely connect or transmit data to the [Marketplace] or its testing environments, nor remotely connect or transmit data to [Plaintiffs’] systems that maintain connections to the [Marketplace] 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).

Suspension Notice at 4 and n. 9 (citing § X.n of the Enhanced Direct Enrollment Agreements (“EDE Agreements”) between CMS and the Plaintiffs) (emphasis added). *See also* Ex. 4 (Benefitalign’s EDE Agreement); Ex. 5 (TrueCoverage’s EDE Agreement) (collectively “EDE Agreements”). This obligation breaks down into two closely related requirements: (1) Plaintiffs “cannot remotely connect or transmit data *to the [Marketplace]* or its testing environments . . . from locations outside of the United States or its territories, embassies, or military installations”

nor (2) “remotely connect or transmit data to [Plaintiffs’] systems that maintain connections *to the [Marketplace]* or its testing environments” from such foreign location. Suspension Notice at 4. (emphasis added).

CMS does not, however, claim that Plaintiffs actually committed either possible breach, let alone provide evidence of one. Instead, CMS fixates on one overarching fact: Plaintiffs obtain substantial software and other IT services from affiliates in India—an uncontested fact that violates no regulatory or contractual obligation at all. Under the regulations and the contracts, Plaintiffs are free to maintain systems with overseas connections so long as those systems do not connect or transmit data *to the Marketplace* or its testing environments.

CMS concedes this point. It writes that Plaintiffs “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.*” Suspension Notice at 4 (emphasis added).

3. *CMS Does not, and Cannot, Establish that the EDE Platform Violates Any Requirement.*

Despite this recognition, CMS asserts that it still “reasonably believes that CMS data, including consumer PII, is processed and/or stored in” India. *Id.* Over the past month, however, Plaintiffs have repeatedly shown CMS that the EDE Platform—*i.e.*, Plaintiffs’ *only* system that connects to the Marketplaces—is not interconnected with overseas computers at all. Panicker Am. Decl. ¶ 45. To the extent CMS offers any facts, none of them show, or even provide a reasonable basis to suspect, that Plaintiffs process and/or store “CMS data” overseas, or that anyone outside the United States can connect or transmit data to Plaintiffs’ EDE Platform. Rather, CMS’s factual support consists of anodyne assertions that apply to vast numbers of businesses.

Indeed, Plaintiffs do rely on some “technical teams . . . based overseas,” and members of such teams are “able to access” some of “TrueCoverage and BenefitAlign platforms” Suspension Notice at 4. It’s true that “[m]ultiple domains tied to [Plaintiffs] . . . are based in India, where they operate a large, dedicated data center” *Id.* But, as Plaintiffs have made clear to CMS, that overseas data center does not support the EDE Platform; Plaintiff’s data center used for EDE Platform development is based in the United States. Panicker Am. Decl. ¶ 45. Plaintiffs make no secret of their affiliates’ “operations in Canada, India, Pakistan, Saudi Arabia, Singapore, and the UAE,” *id.*, and would be pleased to take CMS officials to tour them. Plaintiffs are equally happy to discuss any “other locations and subsidiaries that CMS has not yet discovered.” *Id.* Much can be learned about the global operations of Plaintiffs’ affiliate, Speridian Technologies, through its webpage, *About Us*, Speridian Technologies, <https://www.speridian.com/about-speridian/>, (last visited Sept. 6, 2024), and in particular by the drop-down box that opens at the top of that page labeled “Global/US.”

Further, there is indeed “VPN usage” by Plaintiffs’ personnel. Suspension Notice at 5. CMS speculates that “VPN usage . . . could indicate a party’s intent to hide the fact that its systems could be accessed from outside the United States.” *Id.* But VPN usage is so commonplace that CMS itself publishes a web page intended to “assist you with remotely accessing the Centers for Medicare & Medicaid Services (CMS) network infrastructure . . . through a Virtual Private Network (VPN).” *See Getting Started with Remote Access to the CMS Network*, CMS (July 23, 2012), <https://www.cms.gov/files/document/getting-started-remote-access-1pdf> (last visited Sept. 5, 2024).

Plaintiffs also have “connections to internet protocol (IP) addresses in India and Pakistan,” and “the Speridian Companies . . . primary IT infrastructure was operated in India.”

Suspension Notice at 5. Plaintiffs’ personnel have also sent internet “traffic to multiple IP addresses that corresponded to resources geolocated overseas, including in Hong Kong, India, Ireland, Japan, Pakistan, and Sweden.” *Id.* Given the far reach of the internet for even the most mundane information, it would be remarkable if traffic out of any entity—even a government agency—did not show personnel accessing IP addresses “that corresponded to resources geolocated overseas.” *Id.* CMS’s suggestion of something improper about that fact is more remarkable, still.

None of these rather humdrum facts say anything about the only system that matters: the EDE Platform, which is Plaintiffs’ *only* system that “maintains connections to the [Marketplaces], or their testing environments,” EDE Agreements, § X.n. *All* of CMS’s factual recitations pertain to “Speridian Companies’ platforms” or “Speridian Companies’ systems” generally; no specific factual allegations appear at all about the EDE Platform. Suspension Notice at 4. And as discussed above, Plaintiffs have repeatedly shown CMS that the EDE Platform is inaccessible from outside the United States. Panicker Am. Decl. ¶ 45.

4. *CMS Merely Fears the Possibility of a Violation by Plaintiffs.*

After a month-long review, CMS has found no facts showing a security violation regarding the EDE Platform. If it had, one would expect CMS to have cited such facts in its Suspension Notice.

Instead, reflecting the absence of relevant facts, the Suspension Notice’s assertions are caveated expressions of fear about what might be. They start with a seemingly alarming statement that “TrueCoverage and BenefitAlign technical teams . . . *allegedly* were able to access the True Coverage and BenefitAlign platforms, including consumer PII submitted to those platforms,” but admit that the allegation is based on an “*unconfirmed* report.” Suspension Notice at 4 (citing § X.n of the EDE Agreements between CMS and the Plaintiffs) (emphasis added).

CMS has also never shared its “report,” making it impossible to assess its credibility. CMS claims that “Speridian Companies’ platforms *could be* accessed by non-CMS-approved systems outside of the United States,” but again do not assert, let alone provide reason to think, that this is true of the EDE Platform. *Id.* (emphasis added). CMS expressed to Plaintiffs its “*concerns* about Marketplace data being accessed or accessible from outside the continental United States” *Id.* (emphasis added). CMS has developed “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.” *Id.* at 5 (emphasis added). CMS concludes by justifying its devastating cutoff of Plaintiffs not by citing any evidence that would support a finding that there has been any foreign breach of the Marketplace’s data, but by its unresolved and perhaps unresolvable fears:

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 *suspensions* 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.

Id. at 5 (emphasis added).²

The Suspension Notice contains only one uncaveated allegation: “CMS reasonably believes that CMS data, including consumer [personally identifiable information], is processed and/or stored” in India, where Plaintiffs’ affiliates maintain a data center and from which

² Despite the assertion that Plaintiffs have not provided information requested by CMS, and the assertion that CMS had “yet to receive a response” to the information it requested on August 28, 2024, Suspension Notice at 5, Plaintiffs responded to CMS’s last pending request at 7:52 PM Eastern Time on Friday, August 30, 2024. *See* Ex. 6 at 1 (Email from M. Mehta to D. Paradis, dated Aug. 30, 2024).

Plaintiffs procure software development and IT support services. Suspension Notice at 4. Before and after this assertion, CMS cites § X.n of the EDE Agreements between CMS and the Plaintiffs. *See* Suspension Notice at 4 nn. 7, 9. The only “CMS data” even potentially relevant to a violation, however, is data from the EDE Platform described in § X.n of the Enhanced Direct Enrollment Agreement. Yet CMS provides no reasons for what it “reasonably believes,” that pertain to the EDE Platform. Suspension Notice at 4. Instead, it references routine facts common to any of the many American companies that take advantage of overseas, particularly Indian, information technology assets, which CMS concedes “is acceptable.” Suspension Notice at 4.

5. *CMS’s Indefinite Suspension of Plaintiffs Based on Generalized Suspicions Violates its Own Regulations*

CMS plainly fails to satisfy the first regulation it cites, asserting the right to suspend “if HHS discovers a security and privacy incident or breach.” 45 C.F.R. § 155.220(c)(4)(ii). As explained above, it has neither “discovered” nor even referenced one.

Under the second cited regulation, CMS may suspend a direct enrollment entity only if it “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). In the absence of any facts at all about the EDE Platform—the subject of the only potentially relevant obligation—CMS’s basis boils down to generalized suspicion of the foreign operations of plaintiffs’ affiliates and of entirely routine activity.

Being owned by a parent company that has international business operations, requiring employees to access company systems through VPNs while out of the office, and allowing personnel to access public websites hosted outside the United States cannot possibly create “unacceptable risks.” Otherwise, virtually every business’s IT infrastructure would create

“unacceptable risks.” That includes Plaintiffs’ competitors, and CMS does not appear to have suspended any of them. *See Entities Approved to Use Enhanced Direct Enrollment*, CMS (Aug. 9, 2024) <https://www.cms.gov/media/595041>. In any event, Plaintiffs have provided CMS with extensive evidence demonstrating that it is impossible for anyone outside the United States to access Plaintiffs’ EDE Platform, which debunks CMS’s claim. Panicker Am. Decl. ¶ 45.

CMS also cannot base a finding of “unacceptable risks” on the unfounded allegations contained in a court complaint. Suspension Notice at 6. That is especially so when the allegations do not relate to the security of Plaintiffs’ platforms themselves. Otherwise, an entire business’s owners, employees, and customers could suffer greatly simply because someone makes a set of salacious allegations, no matter how baseless.

Accordingly, no relevant regulation authorizes a suspension under the circumstances that CMS has described, and the decision is unlawful under HHS’s own regulations. That violates the APA. *See Elevance Health, Inc. v. Becerra*, No. CV 23-3902 (RDM), 2024 WL 2880415, at *9 (D.D.C. June 7, 2024) (noting that an agency “is not free to ignore or violate its regulations while they remain in effect.”) (quoting *U.S. Lines, Inc. v. Fed. Mar. Comm’n*, 584 F.2d 519, 526 n.20 (D.C. Cir. 1978)).

6. *CMS Cites Only Unfounded Claims in a Lawsuit to Justify Expanding Its Suspension to TrueCoverage’s Web-Broker Activities.*

The vast majority of the Suspension Notice focuses on requirements applicable to the EDE platforms. As noted above, however, CMS also apparently expanded the suspension to include TrueCoverage’s web-broker activities as well. Suspension Notice at 1. The only possible support for this action, however, is a citation to a complaint filed in Florida. Suspension Notice at 5. TrueCoverage, however, has not even responded to that complaint yet, and there is no record evidence to support the meritless allegations in the lawsuit. Thus, CMS has identified

no basis for its sudden expansion of its suspension beyond the technical issues on which it mainly relies.

7. *CMS's Decision is Arbitrary and Capricious.*

Under the APA, a court must “hold unlawful and set aside agency action” that is arbitrary or capricious or otherwise not in accordance with law or contrary to the Constitution. 5 U.S.C. § 706(2)(A). The Supreme Court has “frequently reiterated that an agency must cogently explain why it has exercised its discretion in a given manner” *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 48 (1983). And a court “must reverse an agency policy when [it] cannot discern a reason for it.” *Judulang v. Holder*, 565 U.S. 42, 64 (2011).

“[A]gency action is lawful only if it rests on a ‘consideration of the relevant factors’” and “important aspect[s] of the problem.” *Michigan v. EPA*, 576 U.S. 743, 750–52 (2015) (quoting *Motor Vehicle Mfrs. Ass’n*, 463 U.S. at 43) (requiring “reasoned decisionmaking”). This means agencies must “examine all relevant factors and record evidence.” *Am. Wild Horse Pres. Campaign v. Perdue*, 873 F.3d 914, 923 (D.C. Cir. 2017). In doing so, an agency cannot “entirely fail[] to consider an important aspect of the problem.” *Motor Vehicle Mfrs. Ass’n*, 463 U.S. at 43; *see also Am. Wild Horse*, 873 F.3d at 931 (“[T]he Service’s Finding of No Significant Impact not only failed to take a ‘hard look’ at the consequences of the boundary change, it averted its eyes altogether.”).

The suspension decision is arbitrary and capricious for at least three independently sufficient reasons.

First, CMS’s initial justification for a suspension that lasted more than three weeks—“potential anomalous activity”—is so vague as to be meaningless and to constitute no reason at all. *See Panicker Am. Decl., Ex. A*. Then, (only after facing a lawsuit and motion for TRO), CMS

provided a written notice that does little more than identify innocuous and widespread corporate practices, accompanied by bald and conclusory allegations, topped off with unproven allegations in a court complaint. Put simply, the Defendants have not offered any explanation based on record evidence as to the reasoning behind Plaintiffs' suspension. Panicker Am. Decl. ¶ 16. That remains so, even after Plaintiffs worked diligently to respond to all of CMS's questions and provided all requested data. Panicker Am. Decl. ¶¶ 15–16.

Second, the regulations governing suspension are itself so vague as to invite and encourage arbitrary and capricious decision making. If CMS asserts that “a security and privacy incident or breach” or “unacceptable risk” are to be defined without regard to specific security requirements, and that the purported “discovery” of facts that are entirely commonplace can justify such a finding, then it argues for essentially boundless discretion. *See* 45 C.F.R. §§ 155.220(c)(4)(ii), 155.221(e). But an agency decision is arbitrary and capricious when “at base everything hangs on the fortuity of an individual official's decision.” *Judulang*, 565 U.S. at 58.

Third, the decision to suspend on the unintelligible basis of “potential anomalous activity,” followed by a *post-hoc* explanation that does not justify a suspension, fails to consider an important aspect of the problem: participation in the ACA system will be deterred once other enrollment platform providers, brokers, agents, and carriers learn that CMS can and will simply turn off access for hundreds of thousands of insured customers for any or no reason. This undermines rather than serves the statutory requirement that HHS establish procedures to allow agents and brokers to enroll eligible participants. *See* 42 U.S.C. § 18032(e).

For each of these independently sufficient reasons, the suspension decision violates the Administrative Procedure Act's prohibition on arbitrary and capricious decisions.

8. *CMS Violated the Due Process Clause of the Constitution.*

“A procedural due process violation under the Fifth Amendment occurs when a government official deprives a person of property without appropriate procedural protections” *N. Am. Butterfly Ass’n v. Wolf*, 977 F.3d 1244, 1265 (D.C. Cir. 2020). When evaluating a procedural due process claim, courts first consider “whether the plaintiff has been deprived of a protected interest in ‘liberty’ or ‘property.’” *Gen. Elec. Co. v. Jackson*, 610 F.3d 110, 117 (D.C. Cir. 2010). If so, courts then determine whether the government’s attendant procedures comport with principles of due process. *Id.* That inquiry turns to the familiar three-factor balancing test set forth in *Mathews v. Eldridge*, 424 U.S. 319 (1976), which considers: (1) “the private interest that will be affected by the official action,” (2) “the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards,” and (3) “the Government’s interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.” *Id.* at 335.

Here, Plaintiffs plainly have a property interest in their businesses, which CMS’s unjustified suspension imperils. By summarily suspending Plaintiffs without any prior warning, and without providing a legitimate explanation, even after Plaintiffs responded to all questions and provided all requested data, CMS’s conduct will erroneously destroy Plaintiffs’ business. CMS has exacerbated this issue by refusing to reinstate Plaintiffs until they complete a full audit. Because Plaintiffs cannot survive the duration of a complete audit, this “remedy” is akin to a commercial death penalty. Simply giving cogent pre-deprivation notice of the reason for the suspension, with a meaningful process allowing Plaintiffs to address any such reason before they are forced to cease operations, would be a minimally burdensome “substitute” procedure over a wholly unjustified suspension.

Accordingly, CMS is depriving Plaintiffs of a protected property interest, and the *Matthews v. Eldridge* factors demonstrate that CMS's suspension did not comport with Due Process.

II. CMS's Suspension Threatens Immediate, Irreparable Harm to TrueCoverage and Benefitalign.

Plaintiffs' platforms serve critical health insurance functions, and the revenue they generate is critical to the companies' ongoing operations. CMS's ongoing suspension of these platforms' EDE access administered by CMS has already ground Plaintiffs' business to a halt. Each day of ongoing suspension jeopardizes their ability to stay in business. Panicker Am. Decl. ¶ 20.

The CMS suspension threatens practically all of the revenue generated by TrueCoverage and Benefitalign. Panicker Am. Decl. ¶ 21. The platforms form the foundation for brokers and agencies to sell healthcare plans to new customers and serve existing customers. Panicker Am. Decl. ¶ 21. Benefitalign and TrueCoverage worked with over 5,000 such brokers and agencies, each of whom cannot perform these functions if they do not have access to the platforms where all relevant information resides. Panicker Am. Decl. ¶ 21. Indeed, many brokers and agencies who used Plaintiffs' platforms have now transitioned to other EDE platforms to service and enroll customers. Panicker Am. Decl. ¶ 22. With open enrollment rapidly approaching, that trend will only accelerate in the coming days. Panicker Am. Decl. ¶ 22.

TrueCoverage's brokerage faces the same predicament as the brokers, with whom its Inshura platform works, as TrueCoverage itself is a purveyor of healthcare plans and uses the Benefitalign platform to enroll new customers and service existing customers. Panicker Am. Decl. ¶ 24. TrueCoverage works with, and provides support to, over 150,000 customers, fielding at least 300 customer calls each day. Locked out of its platforms, the ability to support

customers is in jeopardy. Panicker Am. Decl. ¶ 24. Each day that the platforms remain non-functional means that TrueCoverage cannot provide its services, resulting in ongoing loss of revenue. Panicker Am. Decl. ¶ 24.

The same is true for the health insurance carriers, such as AvMed Health Plans, that use the Benefitalign and Inshura platforms and whose operations are severely affected by the suspension of these platforms. Panicker Am. Decl. ¶ 25. Without access to platform-based records showing which customers have health insurance plans with the carrier and what their plans cover, the carriers are hamstrung in their ability to serve existing customers. Panicker Am. Decl. ¶ 25.

CMS's suspension, and brokers and carriers' imminent termination of their relationships with Benefitalign and TrueCoverage, will lead to cascading and irreversible harm. The ongoing suspension risks initiating a torrent of license termination proceedings against TrueCoverage from state insurance departments. Panicker Am. Decl. ¶ 26. Separately, TrueCoverage has a \$20 million loan from its banking partners, and is required to demonstrate a revenue stream each month to sustain that loan. But because CMS's suspension virtually destroys all revenues that TrueCoverage and Benefitalign receive, the suspension will render TrueCoverage unable to satisfy the requirements of its loan. Panicker Am. Decl. ¶ 27. In addition, TrueCoverage works with over 100 employees whose ongoing employment is jeopardized by the CMS suspension. As revenues plummet while brokers and carriers turn to EDE platform alternatives, TrueCoverage's ability to retain its employee base will rapidly diminish. Panicker Am. Decl. ¶ 28.

Plaintiffs have only one more chance to salvage their business. If they can be reinstated immediately, they can potentially stave off the mass departure of their remaining brokers and

agencies. They can also secure relationships with agencies and brokers who either do not currently have access to a platform, or who are looking to switch away from another platform, in advance of the ACA open enrollment period. Panicker Am. Decl. ¶ 23. To have any chance of success, however, Plaintiffs must regain access to CMS data now. Panicker Am. Decl. ¶ 23.

III. The Balance of Equities Favors a Preliminary Injunction to Maintain the Status Quo, and CMS's Suspension Undermines the Public Interest by Chilling Consumers' Ability to Access Affordable Healthcare Plans and Receive Service for Current Health Plans.

CMS's suspension has far-reaching effects beyond its calamitous impact on TrueCoverage and Benefitalign's ability to remain in business. The platforms are important tools for consumers, often low-income individuals, who seek timely access to affordable healthcare. These platforms aggregate information about different carriers' health plan offerings and serve as a search engine to identify health plans available to that individual. Panicker Am. Decl. ¶ 31. Health insurance brokers use the platforms to input information about potential customers who need access to healthcare, determine what health insurance plan offerings the customer is eligible for, determine if the customer is eligible for any subsidy, and enroll the customer in their chosen health plan. Panicker Am. Decl. ¶ 31. Since CMS's suspension, brokers have been unable to access either platform and have thus been unable to sell health insurance to new customers who need it to afford healthcare. Panicker Am. Decl. ¶ 32. With each day that passes, more potential customers will be rebuffed in their efforts to enroll in health insurance. Panicker Am. Decl. ¶ 32.

The ongoing suspension also has drastic impact on customers who are already enrolled in a health plan and who require service on that plan. The platforms serve as a virtual "filing cabinet" of customer records. Panicker Am. Decl. ¶ 33. These records help determine, for example, what medical care is and is not covered by the enrolled customer's health insurance

plan. Panicker Am. Decl. ¶ 33. Brokers cannot service current customers without access to those customer records. Panicker Am. Decl. ¶ 33. For example, customers call brokers with questions about the scope of their existing coverage under their current health plan. Without access to the customer's records, brokers cannot confirm for a customer whether or not a particular medical care is covered by their plan. Panicker Am. Decl. ¶ 34. Customers may also seek to alter their health plans—for example, they may wish to add a dependent to their plan. With open enrollment soon, many customers will look to change their health coverage. But without access to customer records, brokers cannot honor customers' requests for change. Panicker Am. Decl. ¶ 34. Similarly, health plan enrollees are often required to submit documentation proving their health plan coverage, which is impossible without access to the platforms containing those records. Panicker Am. Decl. ¶ 34.

CMS's suspension imposes considerable burdens on new consumers looking to access affordable health coverage, while existing consumers are hampered in understanding and taking advantage of their current benefits. Panicker Am. Decl. ¶ 35. While brokers can eventually turn to other EDE platforms to sell and service customers, that is neither easy nor cost-free. In the meantime, new customers remain unenrolled and current customers remain unserved. And if Benefalign and TrueCoverage cannot participate in the upcoming open enrollment period, consumers will have fewer choices for their health coverage needs. Panicker Am. Decl. ¶ 36.

As noted above, several health insurance carriers use Plaintiffs' platforms to do business, and their ability to serve current customers is severely impacted by the platforms' abrupt unavailability. Panicker Am. Decl. ¶ 38. To provide one common example, patients are required to submit insurance documentation prior to a medical appointment. The medical office commonly contacts the health insurance carrier's Provider Services line to verify coverage so

that the patient can be treated. But without access to customer records stored on the platforms, carriers cannot verify whether a particular individual is actively enrolled in one of that carrier's health plan offerings, which impacts the patient's ability to receive medical treatment from the contacting medical office. Panicker Am. Decl. ¶ 39. Similarly, an individual may contact the carrier's Member Services line to inquire about their health insurance coverage—and without access to the customer's records, the carrier cannot provide that information. Panicker Am. Decl. ¶ 40. Enrolled customers may also contact TrueCoverage directly to request this information—TrueCoverage receives approximately 300 such calls each day. Without access to the customer's records, TrueCoverage cannot respond to the customers' inquiries. Panicker Am. Decl. ¶ 41.

TrueCoverage also works with multiple downline agencies that license the Benefitalign and Inshura platforms. In these instances, TrueCoverage acts as an intermediary between the health insurance carrier and the downline broker agency: TrueCoverage facilitates the carrier appointments, and the revenue from the downline agencies' sales of that carrier's health plans passes to TrueCoverage, which passes it along to the downline agency that made the sale. Panicker Am. Decl. ¶ 42. The downline agencies with which TrueCoverage works have approximately 200,000 customers they support, and their ability to support these customers without access to the platforms is in jeopardy. Panicker Am. Decl. ¶ 43. CMS's lawless suspension will thus lead to carriers in turn suspending payments, and any suspension of payments by carriers to TrueCoverage will impact TrueCoverage's ability to transmit payment to downline agencies. Most such agencies are small to mid-size organizations that could not survive for more than a month if their payments are not timely released. Panicker Am. Decl. ¶

44. These agencies employ hundreds of individuals whose ongoing employment will be jeopardized by the suspension. Panicker Am. Decl. ¶ 44.

CONCLUSION

For the reasons stated herein, Plaintiffs respectfully request that this Court enter a temporary restraining order and preliminary injunction enjoining CMS from enforcing its arbitrary and unwarranted suspension.

Dated: September 6, 2024

Respectfully submitted,

/s/ Amy E. Richardson

Amy E. Richardson, Esq. (DC Bar # 472284)

Patrick P. O'Donnell (DC Bar # 459360)

Walter E. Anderson, Esq. (DC Bar # 975456)

HWG LLP

1919 M Street NW, 8th Floor

Washington, DC 20036

Tel.: 202-730-1329

Email: arichardson@hwglaw.com

*Counsel for Plaintiffs Benefitalign, LLC and
TrueCoverage, LLC*

Exhibit 1

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:

ashwini.deshpande@truecoverage.com; Sarika.balakrishnan@truecoverage.com;
manal.mehta@benefitalign.com; tamara.white@benefitalign.com, girish.panicker@speridian.com

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

Companies¹) 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 entities² 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

¹ 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.

² "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 155.221.³ 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.⁴

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.⁵ 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.⁶ 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

³ 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.

⁴ EDE Agreement at section X.m.; Web-Broker Agreement at section X.l.; ISA at section 15

⁵ 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.

⁶ 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.⁷ ~~○~~~~○~~~~○~~ 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.⁸ 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)." ⁹

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

⁷ EDE Agreement at section X.n.

⁸ "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.

⁹ 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 Agreements¹⁰, 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

¹⁰ 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.¹¹ The Speridian Companies are also responsible for ensuring cooperation with the Audit by its downstream and delegated entities, including subcontractors.¹²

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-

¹¹ EDE Agreement at section X.m.; Web-Broker Agreement at section X.l.; ISA at section 15.

¹² 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 directenrollment@cms.hhs.gov 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

Exhibit 2



HWG LLP
1919 M STREET NW
WASHINGTON, DC 20036
TEL: +1 202 730 1300 | HWGLAW.COM

September 4, 2024

By email: Stephanie.Johnson5@usdoj.gov
Stephanie R. Johnson, Esq.
Assistant United States Attorney
United States Attorney's Office
District of Columbia
601 D Street, NW
Washington, DC 20530

By email: Brett.Bierer@hhs.gov
Brett Bierer, Esq.
Office of General Counsel
Department of Health and Human Services
7500 Security Blvd.
Baltimore, MD 21244-1849

Re: Proposed Interim Agreement, *TrueCoverage LLC et al. v. Becerra et al.*, United States District Court for the District of Columbia, 1:24-cv-02494

Dear Ms. Johnson and Mr. Bierer:

As we indicated in our telephone conversation earlier this week, our clients TrueCoverage LLC and Benefitalign LLC (each individually, a Company, and together, the Companies) continue to wish to explore every possibility of amicably resolving the above matter and to avoid the need for interim relief from the Court, if possible. To that end, the Companies propose an interim agreement between the parties, followed by a joint request to stay the above matter pending final resolution.

Specifically, the Companies propose the following interim commitments in exchange for the agreement of the Centers for Medicare & Medicaid Services (CMS), on behalf of the Department of Health and Human Services (HHS) to restore the Companies' ability to transact information with Federally facilitated Marketplaces (FFMs) and State-based Marketplaces on the Federal Platform (SBM-FPs) (collectively, Marketplace or Marketplaces), for themselves and their customer agents and brokers:

The Companies' system that "maintains connections to the FFE, SBE-FP, or their testing environments,"¹ is "Benefitalign BrokerEngage™ - Primary EDE Host," which also operates as "Inshura - Hybrid Non-Issuer Upstream EDE Entity" (collectively, the EDE Platform). For the life of the proposed interim agreement, the Companies will commit to:

1. Continue their existing practice of authorizing only users based in the United States of America to access the EDE Platform, enforced by unique user credentials.
2. Continue their existing practice of allowing users to remotely access the EDE Platform only through a firewall configured to:

¹ See EDE Agreement between EDE Entity BenefitAlign LLC and CMS for the Individual Market FFM and SBM-FP, § X.n and EDE Agreement between EDE Entity TrueCoverage dba Inshura and CMS for the Individual Market FFM and SBM-FP, § X.n. See also Letter from Jeffrey Grant, September 2, 2024 at 4 nn. 7 and 9.

September 4, 2024

Page 2 of 2

- a. “Geofence” the IP addresses from which the EDE Platform can be accessed so that it may be accessed only from locations within the United States of America; and
 - b. Prohibit access through any Virtual Private Network (VPN) that anonymizes the original internet protocol (IP) address of the user’s internet connection.
3. Continue their existing practice of segregating all of the Companies’ overseas Information Technology (IT) systems from the EDE Platform so that no information can be exchanged electronically between the EDE Platform and any overseas IT system of either Company.
 4. Institute a further segregation of the EDE Platform by moving it to a dedicated Virtual Private Cloud (VPC) containing none of the Companies’ other platforms.
 5. Institute new restrictions that prevent brokers and agents from downloading their book of business from the EDE Platform that may contain any personally identifiable information (PII) about their own applicants or customers, and continuing existing restrictions that prevent brokers and agents from accessing from the EDE Platform any PII about individuals who are not their applicants or customers.
 6. Provide CMS with daily logs for the EDE Platform’s VPC, VPN, and Amazon Web Services (AWS) Management Console, to include the IP address of each user and activities within the relevant infrastructure.

We are hopeful you will agree that this is a reasonable and constructive proposal. Although the Companies dispute the assertions made in Jeffrey Grant’s letter of September 2, 2024, to which they will separately respond more fully, the proposed commitments address all of the technical concerns expressed in that letter. This proposal is without prejudice to the newly announced audit by CMS, with which the Companies will cooperate fully.

As you know, the Court has imposed a deadline of September 6, 2024, for the Companies to amend their Complaint in the above matter. Given the urgent and ongoing threat to the Companies’ existence, and the need to meet the Court’s deadline, we request a response by tomorrow, September 5, 2024.

We are, of course, available to discuss this matter with you at any time.

Sincerely,



Patrick O'Donnell
Amy Richardson
Counsel for TrueCoverage LLC and Benefitalign LLC

Exhibit 3

Re: Call re: TRO in 24-cv-2494

Amy E. Richardson <ARichardson@hwglaw.com>

Fri 9/6/2024 12:45 PM

To: Bierer, Brett (HHS/OGC) <Brett.Bierer@hhs.gov>; Johnson, Stephanie (USADC) <Stephanie.Johnson5@usdoj.gov>; Balderston, Robert (HHS/OGC) <Robert.Balderston@HHS.GOV>

Cc: Patrick O'Donnell <podonnell@hwglaw.com>; Amy E. Richardson <ARichardson@hwglaw.com>

Brett,

Thank you for your response. Our clients remain committed to working collaboratively with CMS and are remain open to considering any counterproposal from CMS. Does your client have any proposal to offer short of indefinite suspension? It would helpful to have a call among counsel to discuss.

Thanks in advance.

Amy

From: "Bierer, Brett (HHS/OGC)" <Brett.Bierer@hhs.gov>

Date: Friday, September 6, 2024 at 9:15 AM

To: Patrick O'Donnell <podonnell@hwglaw.com>, "Stephanie R. Johnson" <Stephanie.Johnson5@usdoj.gov>

Cc: Amy Richardson <ARichardson@hwglaw.com>, "Balderston, Robert (HHS/OGC)" <Robert.Balderston@HHS.GOV>

Subject: RE: Call re: TRO in 24-cv-2494

Thank you. CMS has considered your proposal, but it does not allay the concerns that CMS raised in its suspension notice.

From: Patrick O'Donnell <podonnell@hwglaw.com>

Sent: Wednesday, September 4, 2024 5:42 PM

To: Johnson, Stephanie (USADC) <Stephanie.Johnson5@usdoj.gov>; Bierer, Brett (HHS/OGC) <Brett.Bierer@hhs.gov>

Cc: Amy E. Richardson <ARichardson@hwglaw.com>

Subject: Re: Call re: TRO in 24-cv-2494

Importance: High

Stephanie and Brett –

As we briefly discussed yesterday, our client remains willing to consider any reasonable step to give your client very strong protections so that it can restore our clients' access while we work through the dispute and the new audit. To that end, we've prepared the attached proposal, requesting a response tomorrow given the Friday deadline to amend our complaint.

Feel free to call either of us to discuss it. My cell is [REDACTED]. Amy's is [REDACTED].

Patrick O'Donnell
HWG LLP
1919 M Street, NW
8th Floor
Washington, D.C. 20036

From: Amy E. Richardson <ARichardson@hwglaw.com>
Date: Tuesday, September 3, 2024 at 10:30 AM
To: Johnson, Stephanie (USADC) <Stephanie.Johnson5@usdoj.gov>
Cc: Patrick O'Donnell <podonnell@hwglaw.com>
Subject: Re: Call re: TRO in 24-cv-2494

Stephanie –

Do you have time for a quick chat before our call at 11:30 with the Court? We had time to review the letter from CMS last night and have some thoughts we would like to discuss prior to talking to the Court. We are available any time between and 11:30. Just let us know.

Amy

From: " Stephanie R. Johnson " <Stephanie.Johnson5@usdoj.gov>
Date: Monday, September 2, 2024 at 9:54 PM
To: Amy Richardson <ARichardson@hwglaw.com>
Subject: RE: Call re: TRO in 24-cv-2494

Yes, that would work. Thank you.

Sincerely,

Stephanie R. Johnson

Assistant United States Attorney
United States Attorney's Office
District of Columbia
601 D Street, NW
Washington, DC 20530
Office Phone: [REDACTED]
Work Cell Phone: [REDACTED]
Email: Stephanie.Johnson5@usdoj.gov

Preferred Pronouns: She, Her, Hers

From: Amy E. Richardson <ARichardson@hwglaw.com>
Sent: Monday, September 2, 2024 8:46 PM
To: Johnson, Stephanie (USADC) <SJohnson4@usa.doj.gov>
Subject: [EXTERNAL] Re: Call re: TRO in 24-cv-2494

Stephanie – I think you can add one person and I can add one person. Do you want to call me at 11:20 and then we can each try to add in our respective parties.

From: " Stephanie R. Johnson " <Stephanie.Johnson5@usdoj.gov>
Date: Saturday, August 31, 2024 at 10:45 AM
To: Amy Richardson <ARichardson@hwglaw.com>
Subject: RE: Call re: TRO in 24-cv-2494

Okay, thank you. Agency counsel also wants to join the call so if I am only able to add one person then you or your colleague may need to call the court.

Sincerely,

Stephanie R. Johnson

Assistant United States Attorney
United States Attorney's Office
District of Columbia
601 D Street, NW
Washington, DC 20530
Office Phone: [REDACTED]
Work Cell Phone: [REDACTED]
Email: Stephanie.Johnson5@usdoj.gov

Preferred Pronouns: She, Her, Hers

From: Amy E. Richardson <ARichardson@hwglaw.com>
Sent: Friday, August 30, 2024 10:37 PM
To: Johnson, Stephanie (USADC) <SJohnson4@usa.doj.gov>
Subject: [EXTERNAL] Re: Call re: TRO in 24-cv-2494

Thanks Stephanie. I am not sure if I will cover the call or if one of colleagues will. I will email you Monday evening.

From: "Johnson, Stephanie (USADC)" <Stephanie.Johnson5@usdoj.gov>
Date: Friday, August 30, 2024 at 8:29 PM
To: Amy Richardson <ARichardson@hwglaw.com>
Subject: RE: Call re: TRO in 24-cv-2494

Hi Amy,

My telephone numbers are in my signature but the best number to reach me will be my work cell phone number. If you want, I can give you a call on Tuesday and then I call chambers on three-way. Please just let me know and provide your number.

Sincerely,

Stephanie R. Johnson

Assistant United States Attorney
United States Attorney's Office
District of Columbia
601 D Street, NW
Washington, DC 20530
Office Phone: [REDACTED]
Work Cell Phone: [REDACTED]
Email: Stephanie.Johnson5@usdoj.gov

Preferred Pronouns: She, Her, Hers

From: Russell Bogue <Russell_Bogue@dcd.uscourts.gov>

Sent: Friday, August 30, 2024 8:10 PM

To: arichardson@hwglaw.com; Johnson, Stephanie (USADC) <SJohnson4@usa.doj.gov>

Subject: [EXTERNAL] Call re: TRO in 24-cv-2494

Amy and Stephanie,

CJ Boasberg would like to discuss the pending TRO motion in the above-captioned case via phone at 11:30 a.m. on Tuesday, September 3. Please exchange telephone numbers and call the Chambers line ([REDACTED]) with both parties on the line. If this time does not work for you, let us know as soon as possible so that we can find a different window.

Thank you!

Russell C. Bogue

Law Clerk to the Honorable James E. Boasberg

U.S. District Court for the District of Columbia

Russell_Bogue@dcd.uscourts.gov

[REDACTED]

Exhibit 4

**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”)¹ 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.

¹ 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,² 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;

² 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.³

³ 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.⁴
- 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

⁴ 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 Entity⁵ 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

⁵ 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 CMS⁶. 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.⁷ 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.⁸

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,⁹ 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,¹⁰ 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

⁶ 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>.

⁷ 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.

⁸ This document is available at the following link: <https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf>.

⁹ This document is available at the following link within the Privacy and Security Templates Resources: <https://zone.cms.gov/document/privacy-and-security-audit>.

¹⁰ 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. 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.¹¹ 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

¹¹ 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.¹² 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

¹² 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.¹³

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

¹³ 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.¹⁴ 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.¹⁵ The ORR, and

¹⁴ 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.

¹⁵ 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).¹⁶ 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,¹⁷ Enhanced Direct Enrollment API Companion Guide,¹⁸ and FFE UI Application Principles for Integration with FFE APIs.¹⁹ 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

¹⁶ 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.”

¹⁷ See *supra* note 8.

¹⁸ The document Enhanced Direct Enrollment API Companion *Guide* is available at the following link: <https://zone.cms.gov/document/api-information>.

¹⁹ 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.²⁰ 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.²¹ 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

²⁰ 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>.

²¹ 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.²² 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.

²² 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.²³
- 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.

²³ 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. 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.²⁴ 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

²⁴ 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.”²⁵
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.²⁶
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

²⁵ 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>.

²⁶ 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 Redirect²⁷, 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.²⁸
- 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.²⁹
- 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.

²⁷ 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>.

²⁸ EDE APIs technical documentation is available on CMS zONE at the following link: <https://zone.cms.gov/document/api-information>.

²⁹ 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

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 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

505-585-2792

EDE Entity Contact Number

FOR CMS

The undersigned are officials of CMS who are authorized to represent and bind CMS for purposes of this Agreement.

Jeffrey D. Grant

Date

Deputy Director for Operations
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services

George C. Hoffmann

Date

Deputy CIO and 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”)³⁰ and Section A³¹ 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

³⁰ The NEE SSP template is located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

³¹ 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.³²

(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

³² 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.

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 REQUIREMENTS³³

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
Consumer Identity Proofing Implementation	<ul style="list-style-type: none"> ▪ <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.³⁴ 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"> – <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. – <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 (https://zone.cms.gov/document/api-information).

³³ 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."

³⁴ 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
Consumer Identity Proofing Implementation (continued)	<ul style="list-style-type: none"> – 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. – 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. ▪ Review Standard: <ul style="list-style-type: none"> – If an EDE Entity uses the Exchange RIDP service, the Auditor must verify that the EDE Entity has successfully passed testing with the Hub.³⁵ – 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"> The ID proofing service is FICAM TFS-approved, and The EDE Entity has implemented the service correctly. – 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. – EDE Entity’s inclusion of the appropriate Consumer User ID fields in the EDE and Fetch Eligibility API calls.

³⁵ 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
Agent and Broker Identity Proofing Verification	<ul style="list-style-type: none"> ▪ <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"> – EDE Entity must integrate with IDM-Okta³⁶ 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. – 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"> Use the Exchange-provided RIDP/FARS APIs to remotely ID proof Agents and Brokers; OR Manually ID proof Agents and Brokers following the guidelines outlined in the document “Acceptable Documentation for Identity Proofing” available on CMS zONE EDE webpage (https://zone.cms.gov/document/api-information). 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. – 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 its EDE environment. – 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. – 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).

³⁶ 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
Agent and Broker Identity Proofing Verification (continued)	<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"> – 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. – 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. – EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3. ▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> – 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. – EDE Entity’s process for ID proofing an Agent or Broker prior to allowing an Agent or Broker to use its EDE environment. – 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. – 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. – 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.
Phase-dependent Screener Questions (EDE Phase 1 and 2 EDE Entities Only)	<ul style="list-style-type: none"> ▪ <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]. ▪ <i>Review Standard:</i> The Auditor must verify the following: <ul style="list-style-type: none"> – 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. – The EDE Entity’s EDE environment facilitates moving Consumers to one of the alternative enrollment pathways described immediately above.

Review Category	Requirement and Audit Standard
Accurate and Streamlined Eligibility Application User Interface (UI)	<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 (https://zone.cms.gov/document/eligibility-information). Auditors will need to access the FFE Application UI Principles document to conduct the audit.</p> <ul style="list-style-type: none"> – 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"> 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. – 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. <ul style="list-style-type: none"> ▪ <i>Review Standard:</i> The Auditor must review and certify the following: <ul style="list-style-type: none"> – The FFE Application UI has been implemented in EDE Entity's environment in accordance with the Exchange Application UI Principles document. – The FFE Application UI displays all appropriate eligibility questions and answers from the Application UI Toolkit, including any questions designated as optional. – 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"> 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. – 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.

Review Category	Requirement and Audit Standard
Post-eligibility Application Communications	<ul style="list-style-type: none"> ▪ <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"> – EDE Entity must provide Consumers with required UI messaging tied to API functionality and responses as provided in the EDE API Companion Guide³⁷. – 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.

³⁷ 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
Post-eligibility Application Communications (continued)	<ul style="list-style-type: none"> – 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. – 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. – 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. – 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). – 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. – 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. ▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> – The EDE Entity’s EDE environment is compliant with the requirements contained in the Communications Toolkit and API Companion Guide. – 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. – 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. – 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. – The EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI. – The EDE Entity must have a means for providing critical communications to the Consumer consistent with the standards above. – The EDE Entity must support all DMLs and SVIs in its post-eligibility application and post-enrollment functionality.

Review Category	Requirement and Audit Standard
Accurate Information about the Exchange and Consumer Communications	<ul style="list-style-type: none"> ▪ <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. ▪ <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.
Documentation of Interactions with Consumer Applications or the Exchange	<ul style="list-style-type: none"> ▪ <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,³⁸ as well as the Upstream EDE Entity users, of a Primary EDE Entity's EDE environment. ▪ <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"> – 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. – 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. – 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. – 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. – The EDE Entity's environment stores this information for 10 years.

³⁸ 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
Eligibility Results Testing and SES Testing	<ul style="list-style-type: none"> ▪ <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"> – 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 https://zone.cms.gov/document/business-audit. ▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> – 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. – 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).
API Functional Integration Requirements	<ul style="list-style-type: none"> ▪ <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 (https://zone.cms.gov/document/api-information). ▪ <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"> – 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. – 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.
Application UI Validation	<ul style="list-style-type: none"> ▪ <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. ▪ <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.

Review Category	Requirement and Audit Standard
Section 508-compliant UI	<ul style="list-style-type: none"> ▪ <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)). ▪ <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"> – 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. – 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.
Non-English-language Version of the Application UI and Communication Materials	<ul style="list-style-type: none"> ▪ <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.³⁹ 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.⁴⁰ ▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> – 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. – The Auditor must verify that the application UI has the same meaning as its English-language version. – The Auditor must also verify that EDE Entity has met all EDE communications translation requirements released by CMS in the Communications Toolkit. – 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.

³⁹ 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.

⁴⁰ 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
EDE Change Management Process	<ul style="list-style-type: none"> ▪ <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"> – A process that incorporates all elements of the Change Notification SOP as referenced in Section XI.A.i, EDE Entity-initiated Change Request Process; – 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; – A process for defining regression testing scope and developing or identifying applicable testing scenarios; – A process for conducting regression testing; – A process for identifying and correcting errors discovered through regression testing and re-testing the correction; – A process for maintaining separate testing environments and defining the purposes and releases for each environment; – 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 – 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. ▪ <i>Review Standard:</i> The Auditor must evaluate the EDE Entity's change management plan for compliance with the elements and criteria defined above.
Health Reimbursement Arrangement (HRA) Offer Required UI Messaging	<ul style="list-style-type: none"> ▪ <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.⁴¹ ▪ <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.

⁴¹ 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.⁴² 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)⁴³ 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.

⁴² “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.”

⁴³ 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>Notice of Intent to Participate and Auditor Confirmation</p>	<ul style="list-style-type: none"> ▪ 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"> – Prospective EDE Entity Name – Auditor Name(s) and Contact Information (Business Requirements and Privacy and Security, if different) – A copy of the executed contract with the Auditor(s) (pricing and proprietary information may be redacted) – EDE Phase (1, 2, or 3) – 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 – Prospective EDE Entity Technical POC name, email, and phone number. The Technical POC should be a person 	<ul style="list-style-type: none"> ▪ The Prospective Primary and Prospective Phase Change EDE Entity must email directenrollment@cms.hhs.gov ▪ Subject line should state: “Enhanced DE: Intent.” 	<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"> – who manages technical development – 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.⁴⁴ – CMS-issued Hub Partner ID 			
DE Entity Documentation Package—Privacy Questionnaire (or attestation, if applicable, see Submission Requirements column)	<ul style="list-style-type: none"> ▪ CMS has provided the privacy questionnaire as part of the DE Entity Documentation Package available on CMS zONE. ▪ EDE Entity must populate the privacy questionnaire and return it to CMS for review. 	<ul style="list-style-type: none"> ▪ Submit via the DE/EDE Entity PME Site ▪ 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. – The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents. 	Prospective Primary EDE Entities	Submit with audit submission

⁴⁴ 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.

Document	Description	Submission Requirements	Entity Responsible	Deadline
<p>DE Entity Documentation Package—Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements column)</p>	<ul style="list-style-type: none"> ▪ 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. ▪ 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. 	<ul style="list-style-type: none"> ▪ Submit via the DE/EDE PME Site ▪ 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"> – The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents 	<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
EDE Business Agreement	<ul style="list-style-type: none"> ▪ 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). ▪ 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. 	<ul style="list-style-type: none"> ▪ Submit via the DE/EDE Entity PME Site 	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>
DE Entity Documentation Package—Operational and Oversight Information	<ul style="list-style-type: none"> ▪ EDE Entities must submit the operational and oversight information to CMS to use the EDE pathway. This form must be filled out completely. ▪ The form is an Excel file that the EDE Entity will complete and submit to CMS. 	<ul style="list-style-type: none"> ▪ Submit via the DE/EDE Entity PME Site ▪ Prospective Primary EDE Entities will receive an encrypted, pre-populated version of the form from CMS ▪ Prospective Upstream EDE Entities will complete a blank version of the form that is available on CMS zONE 	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
Business Audit Report and Toolkits	<ul style="list-style-type: none"> EDE Entities must submit the Business Requirements Audit Report Template and all applicable toolkits completed by its Auditor(s). See Section VI.B.ii, Business Requirements Audit Resources, Exhibit 5, for more information. 	<ul style="list-style-type: none"> The EDE Entity and its Auditor(s) must submit the different parts of the Auditor resources package via the DE/EDE Entity PME Site 	Prospective Primary EDE Entities, Prospective Phase Change EDE Entities, and their Auditors	April 1 -July 1 (3:00 AM ET)
Training	<ul style="list-style-type: none"> EDE Entities (and their Auditors) must complete the trainings as outlined in Section VIII, Required Auditor and EDE Entity Training. The trainings are located on REGTAP (located at the following link: https://www.regtap.info/). 	<ul style="list-style-type: none"> The person taking the training must complete the course conclusion pages at the end of each module 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 	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>
HUB Onboarding Form	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Follow instructions on the Hub Onboarding Form (located at the following link: https://zone.cms.gov/document/hub-onboarding-form) Send to HubSupport@sparksoftcorp.com 	Prospective Primary and Prospective Upstream EDE Entities	Prior to accessing the EDE APIs

Document	Description	Submission Requirements	Entity Responsible	Deadline
Application Technical Assistance and Mini Audit Testing Credentials	<ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ Follow instructions on the EDE UI Eligibility Technical Assistance Credentials Form Template on CMS zONE: https://zone.cms.gov/document/eligibility-information 	Prospective Primary EDE Entities and Prospective Phase Change EDE Entities	Submit with audit submission date

Document	Description	Submission Requirements	Entity Responsible	Deadline
Interconnection Security Agreement (ISA)	<ul style="list-style-type: none"> ▪ A Prospective Primary EDE Entity must submit the ISA to use the EDE pathway. ▪ CMS will countersign the ISA after CMS has reviewed and approved the EDE Entity's business requirements audit and privacy and security audit. 	<ul style="list-style-type: none"> ▪ A Prospective Primary EDE Entity must submit the ISA via the DE/EDE Entity PME Site. ▪ The ISA contains Appendices that must be completed in full for an EDE Entity to be considered for approval. ▪ Appendix B of the ISA must detail: <ol style="list-style-type: none"> (1) all arrangements with Upstream EDE Entities and any related data connections or exchanges, (2) any arrangements involving Web-brokers, and (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. ▪ 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. 	<ul style="list-style-type: none"> ▪ Prospective Primary EDE Entities 	<ul style="list-style-type: none"> ▪ Submit with the audit submission

Document	Description	Submission Requirements	Entity Responsible	Deadline
Security Privacy Controls Assessment Test Plan (SAP)	<ul style="list-style-type: none"> ▪ This report is to be completed by the Auditor and submitted to CMS prior to initiating the audit. ▪ The SAP describes the Auditor's scope and methodology of the assessment. The SAP includes an attestation of the Auditor's independence. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the SAP completed by its Auditor via the DE/EDE Entity PME Site. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ At least thirty (30) Days before commencing the privacy and security audit; during the planning phase
Security Privacy Assessment Report (SAR)	<ul style="list-style-type: none"> ▪ This report details the Auditor's assessment findings of the Prospective EDE Entity's security and privacy controls implementation. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the SAR completed by its Auditor via the DE/EDE Entity PME Site. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ April 1 – July 1 (3:00 AM ET)

Document	Description	Submission Requirements	Entity Responsible	Deadline
Plan of Action & Milestones (POA&M)	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity must submit a POA&M if its Auditor identifies any privacy and security compliance issues in the SAR. ▪ The POA&M details a corrective action plan and the estimated completion date for identified milestones. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the POA&M in conjunction with the SAR via the DE/EDE Entity PME Site. ▪ POA&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&M, but must submit an update monthly to CMS until all significant or major findings are resolved. Thereafter, quarterly POA&M submissions are required as part of the ISCM activities. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Initial: April 1 – July 1 (3:00 AM ET) ▪ Monthly submissions, as necessary, if outstanding findings. ▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit quarterly POA&Ms by the last business Day of March, July, September, and December.

Document	Description	Submission Requirements	Entity Responsible	Deadline
Risk Acceptance Form	<ul style="list-style-type: none"> ▪ The Risk Acceptance Form records the weaknesses that require an official risk acceptance from the organization's Authorizing Official. ▪ Before deciding to accept the risks, the relevant NEE's authorities should rigorously explore ways to mitigate the risks. 	<ul style="list-style-type: none"> ▪ 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&M. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ The Risk Acceptance Form should be submitted with the POA&M during the regular POA&M submission schedule.
Privacy Impact Assessment (PIA)	<ul style="list-style-type: none"> ▪ The PIA will detail the Prospective EDE Entity's evaluation of its controls for protecting PII. 	<ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Before commencing the privacy and security audit as part of the NEE SSP
Non-Exchange Entity System Security and Privacy Plan (NEE SSP)	<ul style="list-style-type: none"> ▪ The NEE SSP will include detailed information about the Prospective EDE Entity's implementation of required security and privacy controls. 	<ul style="list-style-type: none"> ▪ 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. ▪ The implementation of security and privacy controls must be completely documented in the NEE SSP before the audit is initiated. 	<ul style="list-style-type: none"> ▪ Prospective Primary and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Before commencing the privacy and security audit

Document	Description	Submission Requirements	Entity Responsible	Deadline
Incident Response Plan and Incident/Breach Notification Plan	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity is required to implement Breach and Incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures. ▪ A Prospective EDE Entity must incorporate these procedures into its own written policies and procedures.⁴⁵ 	<ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Before commencing the privacy and security audit as part of the NEE SSP

⁴⁵ <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf>.

<p>Annual Penetration Testing</p>	<ul style="list-style-type: none"> ▪ The penetration test must include the EDE environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10. ▪ 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 and must provide the following information to CMS, a minimum of five (5) business Days using the CMS-provided form⁴⁶, prior to initiation of the penetration testing: <ul style="list-style-type: none"> – Period of testing performance (specific times for all penetration 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. ▪ 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 mirrors the production environment. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the Penetration Test results with the SAR via the DE/EDE Entity PME Site. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Initial: April 1 – July 1 (3:00 AM ET) ▪ 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.
------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Document	Description	Submission Requirements	Entity Responsible	Deadline
<p>Vulnerability Scan</p>	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity is required to conduct monthly Vulnerability Scans. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the last three months of their Vulnerability Scan Reports, in conjunction with POA&M and SAR via the DE/EDE Entity PME Site. ▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&M. ▪ Similar findings can be consolidated. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities. 	<ul style="list-style-type: none"> ▪ Initial: April 1 – July 1 (3:00 AM ET) ▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit Vulnerability Scans annually.

⁴⁶ 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	832-287-5647
Auditor 1 Contact Email Address	sgupta@absurance.com
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.⁴⁷ 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
Phase 1: Host Simplified Application + EDE API Suite	<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"> ▪ Application filer (and others on application, if applicable) resides in the application state and all dependents have the same permanent address, if applicable ▪ 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 ▪ 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 ▪ No household members are full-time students aged 18-22 ▪ No household member is pregnant ▪ All Applicants are U.S. citizens ▪ All Applicants can enter Social Security Numbers (SSNs) ▪ No Applicants are applying under a name different than the one on his/her Social Security cards ▪ No Applicants were born outside of the U.S. and became naturalized or derived U.S. citizens ▪ No Applicants are currently incarcerated (detained or jailed) ▪ No household members are American Indian or Alaska Native ▪ No Applicants are offered health coverage through a job or COBRA ▪ No Applicants are offered an individual coverage health reimbursement arrangement (HRA) or qualified small employer health reimbursement arrangement (QSEHRA) ▪ No Applicants were in foster care at age 18 and are currently 25 or younger ▪ All dependents are claimed on the Application filer's federal income tax return for the coverage year ▪ All dependents are the Application filer's children who are single (not married) and 25 or younger ▪ No dependents are stepchildren or grandchildren ▪ No dependents live with a parent who is not on the Application filer's federal income tax return 	<p>Lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.</p>

⁴⁷ 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
Phase 2: Host Expanded Simplified Application + EDE API Suite	<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"> ▪ All scenarios covered by Phase 1 ▪ Full-time student ▪ Pregnant application members ▪ Non-U.S. citizens ▪ Naturalized U.S. citizens ▪ Application members who do not provide an SSN ▪ Application members with a different name than the one on their SSN cards ▪ Incarcerated application members ▪ Application members who previously were in foster care ▪ Stepchildren 	<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>
Phase 3: Host Complete Application + EDE API Suite	<p>EDE Entity hosts an application that supports all application scenarios (equivalent to existing HealthCare.gov):</p> <ul style="list-style-type: none"> ▪ All scenarios covered in Phase 2 ▪ American Indian and Alaskan Native household members ▪ Application members with differing home addresses or residing in a State separate from where they are applying for coverage ▪ Application members with no home address ▪ Application members not planning to file a tax return ▪ Married application members not filing jointly ▪ 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) ▪ Application members offered coverage through their job, someone else's job, or COBRA ▪ Application members with dependent children who are over age 25 or who are married ▪ Application members with dependent children living with a parent not on their federal income tax return ▪ Dependents who are not sons/daughters ▪ Applicants who are offered an individual coverage HRA or QSEHRA 	<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 5

**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”)¹ 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.

¹ 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,² 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;

² 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.³

³ 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.⁴
- 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

⁴ 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 Entity⁵ 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

⁵ 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 CMS⁶. 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.⁷ 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.⁸

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,⁹ 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,¹⁰ 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

⁶ 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>.

⁷ 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.

⁸ This document is available at the following link: <https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf>.

⁹ This document is available at the following link within the Privacy and Security Templates Resources: <https://zone.cms.gov/document/privacy-and-security-audit>.

¹⁰ 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. 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.¹¹ 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

¹¹ 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.¹² 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

¹² 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.¹³

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

¹³ 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.¹⁴ 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.¹⁵ The ORR, and

¹⁴ 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.

¹⁵ 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).¹⁶ 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,¹⁷ Enhanced Direct Enrollment API Companion Guide,¹⁸ and FFE UI Application Principles for Integration with FFE APIs.¹⁹ 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

¹⁶ 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.”

¹⁷ See supra note 8.

¹⁸ The document Enhanced Direct Enrollment API Companion *Guide* is available at the following link: <https://zone.cms.gov/document/api-information>.

¹⁹ 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.²⁰ 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.²¹ 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

²⁰ 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>.

²¹ 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.²² 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.

²² 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.²³
- 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.

²³ 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. 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.²⁴ 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

²⁴ 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.”²⁵
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.²⁶
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

²⁵ 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>.

²⁶ 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 Redirect²⁷, 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.²⁸
- 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.²⁹
- 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.

²⁷ 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>.

²⁸ EDE APIs technical documentation is available on CMS zONE at the following link: <https://zone.cms.gov/document/api-information>.

²⁹ 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

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 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.

Ashwini Deshpande

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

04.TCL.MD*.347.921

EDE Entity Name

EDE Entity Partner IDs

Sarika Balakrishnan

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

505-585-2783

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”)³⁰ and Section A³¹ 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

³⁰ The NEE SSP template is located on CMS zONE at the following link: <https://zone.cms.gov/document/privacy-and-security-audit>.

³¹ 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.³²

(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

³² 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.

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 REQUIREMENTS³³

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
Consumer Identity Proofing Implementation	<ul style="list-style-type: none"> ▪ <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.³⁴ 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"> – <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. – <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 (https://zone.cms.gov/document/api-information).

³³ 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."

³⁴ 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
Consumer Identity Proofing Implementation (continued)	<ul style="list-style-type: none"> – 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. – 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. ▪ Review Standard: <ul style="list-style-type: none"> – If an EDE Entity uses the Exchange RIDP service, the Auditor must verify that the EDE Entity has successfully passed testing with the Hub.³⁵ – 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"> The ID proofing service is FICAM TFS-approved, and The EDE Entity has implemented the service correctly. – 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. – EDE Entity’s inclusion of the appropriate Consumer User ID fields in the EDE and Fetch Eligibility API calls.

³⁵ 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
Agent and Broker Identity Proofing Verification	<ul style="list-style-type: none"> ▪ <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"> – EDE Entity must integrate with IDM-Okta³⁶ 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. – 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"> Use the Exchange-provided RIDP/FARS APIs to remotely ID proof Agents and Brokers; OR Manually ID proof Agents and Brokers following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE EDE webpage (https://zone.cms.gov/document/api-information). 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. – 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 its EDE environment. – 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. – 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).

³⁶ 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
Agent and Broker Identity Proofing Verification (continued)	<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"> – 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. – 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. – EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3. ▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> – 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. – EDE Entity’s process for ID proofing an Agent or Broker prior to allowing an Agent or Broker to use its EDE environment. – 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. – 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. – 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.
Phase-dependent Screener Questions (EDE Phase 1 and 2 EDE Entities Only)	<ul style="list-style-type: none"> ▪ <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]. ▪ <i>Review Standard:</i> The Auditor must verify the following: <ul style="list-style-type: none"> – 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. – The EDE Entity’s EDE environment facilitates moving Consumers to one of the alternative enrollment pathways described immediately above.

Review Category	Requirement and Audit Standard
Accurate and Streamlined Eligibility Application User Interface (UI)	<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 (https://zone.cms.gov/document/eligibility-information). Auditors will need to access the FFE Application UI Principles document to conduct the audit.</p> <ul style="list-style-type: none"> – 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"> 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. – 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. <ul style="list-style-type: none"> ▪ <i>Review Standard:</i> The Auditor must review and certify the following: <ul style="list-style-type: none"> – The FFE Application UI has been implemented in EDE Entity's environment in accordance with the Exchange Application UI Principles document. – The FFE Application UI displays all appropriate eligibility questions and answers from the Application UI Toolkit, including any questions designated as optional. – 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"> 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. – 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.

Review Category	Requirement and Audit Standard
Post-eligibility Application Communications	<ul style="list-style-type: none"> ▪ <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"> – EDE Entity must provide Consumers with required UI messaging tied to API functionality and responses as provided in the EDE API Companion Guide³⁷. – 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.

³⁷ 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
Post-eligibility Application Communications (continued)	<ul style="list-style-type: none"> – 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. – 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. – 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. – 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). – 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. – 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. ▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> – The EDE Entity’s EDE environment is compliant with the requirements contained in the Communications Toolkit and API Companion Guide. – 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. – 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. – 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. – The EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI. – The EDE Entity must have a means for providing critical communications to the Consumer consistent with the standards above. – The EDE Entity must support all DMLs and SVIs in its post-eligibility application and post-enrollment functionality.

Review Category	Requirement and Audit Standard
Accurate Information about the Exchange and Consumer Communications	<ul style="list-style-type: none"> ▪ <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. ▪ <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.
Documentation of Interactions with Consumer Applications or the Exchange	<ul style="list-style-type: none"> ▪ <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,³⁸ as well as the Upstream EDE Entity users, of a Primary EDE Entity's EDE environment. ▪ <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"> – 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. – 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. – 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. – 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. – The EDE Entity's environment stores this information for 10 years.

³⁸ 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
Eligibility Results Testing and SES Testing	<ul style="list-style-type: none"> ▪ <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"> – 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 https://zone.cms.gov/document/business-audit. ▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> – 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. – 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).
API Functional Integration Requirements	<ul style="list-style-type: none"> ▪ <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 (https://zone.cms.gov/document/api-information). ▪ <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"> – 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. – 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.
Application UI Validation	<ul style="list-style-type: none"> ▪ <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. ▪ <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.

Review Category	Requirement and Audit Standard
Section 508-compliant UI	<ul style="list-style-type: none"> ▪ <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)). ▪ <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"> – 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. – 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.
Non-English-language Version of the Application UI and Communication Materials	<ul style="list-style-type: none"> ▪ <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.³⁹ 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.⁴⁰ ▪ <i>Review Standard:</i> The Auditor must verify and certify the following: <ul style="list-style-type: none"> – 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. – The Auditor must verify that the application UI has the same meaning as its English-language version. – The Auditor must also verify that EDE Entity has met all EDE communications translation requirements released by CMS in the Communications Toolkit. – 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.

³⁹ 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.

⁴⁰ 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
EDE Change Management Process	<ul style="list-style-type: none"> ▪ <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"> – A process that incorporates all elements of the Change Notification SOP as referenced in Section XI.A.i, EDE Entity-initiated Change Request Process; – 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; – A process for defining regression testing scope and developing or identifying applicable testing scenarios; – A process for conducting regression testing; – A process for identifying and correcting errors discovered through regression testing and re-testing the correction; – A process for maintaining separate testing environments and defining the purposes and releases for each environment; – 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 – 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. ▪ <i>Review Standard:</i> The Auditor must evaluate the EDE Entity's change management plan for compliance with the elements and criteria defined above.
Health Reimbursement Arrangement (HRA) Offer Required UI Messaging	<ul style="list-style-type: none"> ▪ <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.⁴¹ ▪ <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.

⁴¹ 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.⁴² 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)⁴³ 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.

⁴² “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.”

⁴³ 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>Notice of Intent to Participate and Auditor Confirmation</p>	<ul style="list-style-type: none"> ▪ 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"> – Prospective EDE Entity Name – Auditor Name(s) and Contact Information (Business Requirements and Privacy and Security, if different) – A copy of the executed contract with the Auditor(s) (pricing and proprietary information may be redacted) – EDE Phase (1, 2, or 3) – 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 – Prospective EDE Entity Technical POC name, email, and phone number. The Technical POC should be a person 	<ul style="list-style-type: none"> ▪ The Prospective Primary and Prospective Phase Change EDE Entity must email directenrollment@cms.hhs.gov ▪ Subject line should state: “Enhanced DE: Intent.” 	<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"> – who manages technical development – 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.⁴⁴ – CMS-issued Hub Partner ID 			
DE Entity Documentation Package—Privacy Questionnaire (or attestation, if applicable, see Submission Requirements column)	<ul style="list-style-type: none"> ▪ CMS has provided the privacy questionnaire as part of the DE Entity Documentation Package available on CMS zONE. ▪ EDE Entity must populate the privacy questionnaire and return it to CMS for review. 	<ul style="list-style-type: none"> ▪ Submit via the DE/EDE Entity PME Site ▪ 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. – The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents. 	Prospective Primary EDE Entities	Submit with audit submission

⁴⁴ 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.

Document	Description	Submission Requirements	Entity Responsible	Deadline
<p>DE Entity Documentation Package—Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements column)</p>	<ul style="list-style-type: none"> ▪ 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. ▪ 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. 	<ul style="list-style-type: none"> ▪ Submit via the DE/EDE PME Site ▪ 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"> – The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents 	<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
EDE Business Agreement	<ul style="list-style-type: none"> ▪ 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). ▪ 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. 	<ul style="list-style-type: none"> ▪ Submit via the DE/EDE Entity PME Site 	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>
DE Entity Documentation Package—Operational and Oversight Information	<ul style="list-style-type: none"> ▪ EDE Entities must submit the operational and oversight information to CMS to use the EDE pathway. This form must be filled out completely. ▪ The form is an Excel file that the EDE Entity will complete and submit to CMS. 	<ul style="list-style-type: none"> ▪ Submit via the DE/EDE Entity PME Site ▪ Prospective Primary EDE Entities will receive an encrypted, pre-populated version of the form from CMS ▪ Prospective Upstream EDE Entities will complete a blank version of the form that is available on CMS zONE 	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
Business Audit Report and Toolkits	<ul style="list-style-type: none"> EDE Entities must submit the Business Requirements Audit Report Template and all applicable toolkits completed by its Auditor(s). See Section VI.B.ii, Business Requirements Audit Resources, Exhibit 5, for more information. 	<ul style="list-style-type: none"> The EDE Entity and its Auditor(s) must submit the different parts of the Auditor resources package via the DE/EDE Entity PME Site 	Prospective Primary EDE Entities, Prospective Phase Change EDE Entities, and their Auditors	April 1 -July 1 (3:00 AM ET)
Training	<ul style="list-style-type: none"> EDE Entities (and their Auditors) must complete the trainings as outlined in Section VIII, Required Auditor and EDE Entity Training. The trainings are located on REGTAP (located at the following link: https://www.regtap.info/). 	<ul style="list-style-type: none"> The person taking the training must complete the course conclusion pages at the end of each module 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 	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>
HUB Onboarding Form	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Follow instructions on the Hub Onboarding Form (located at the following link: https://zone.cms.gov/document/hub-onboarding-form) Send to HubSupport@sparksoftcorp.com 	Prospective Primary and Prospective Upstream EDE Entities	Prior to accessing the EDE APIs

Document	Description	Submission Requirements	Entity Responsible	Deadline
Application Technical Assistance and Mini Audit Testing Credentials	<ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ Follow instructions on the EDE UI Eligibility Technical Assistance Credentials Form Template on CMS zONE: https://zone.cms.gov/document/eligibility-information 	Prospective Primary EDE Entities and Prospective Phase Change EDE Entities	Submit with audit submission date

Document	Description	Submission Requirements	Entity Responsible	Deadline
Interconnection Security Agreement (ISA)	<ul style="list-style-type: none"> ▪ A Prospective Primary EDE Entity must submit the ISA to use the EDE pathway. ▪ CMS will countersign the ISA after CMS has reviewed and approved the EDE Entity's business requirements audit and privacy and security audit. 	<ul style="list-style-type: none"> ▪ A Prospective Primary EDE Entity must submit the ISA via the DE/EDE Entity PME Site. ▪ The ISA contains Appendices that must be completed in full for an EDE Entity to be considered for approval. ▪ Appendix B of the ISA must detail: <ol style="list-style-type: none"> (1) all arrangements with Upstream EDE Entities and any related data connections or exchanges, (2) any arrangements involving Web-brokers, and (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. ▪ 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. 	<ul style="list-style-type: none"> ▪ Prospective Primary EDE Entities 	<ul style="list-style-type: none"> ▪ Submit with the audit submission

Document	Description	Submission Requirements	Entity Responsible	Deadline
Security Privacy Controls Assessment Test Plan (SAP)	<ul style="list-style-type: none"> ▪ This report is to be completed by the Auditor and submitted to CMS prior to initiating the audit. ▪ The SAP describes the Auditor's scope and methodology of the assessment. The SAP includes an attestation of the Auditor's independence. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the SAP completed by its Auditor via the DE/EDE Entity PME Site. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ At least thirty (30) Days before commencing the privacy and security audit; during the planning phase
Security Privacy Assessment Report (SAR)	<ul style="list-style-type: none"> ▪ This report details the Auditor's assessment findings of the Prospective EDE Entity's security and privacy controls implementation. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the SAR completed by its Auditor via the DE/EDE Entity PME Site. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ April 1 – July 1 (3:00 AM ET)

Document	Description	Submission Requirements	Entity Responsible	Deadline
Plan of Action & Milestones (POA&M)	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity must submit a POA&M if its Auditor identifies any privacy and security compliance issues in the SAR. ▪ The POA&M details a corrective action plan and the estimated completion date for identified milestones. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the POA&M in conjunction with the SAR via the DE/EDE Entity PME Site. ▪ POA&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&M, but must submit an update monthly to CMS until all significant or major findings are resolved. Thereafter, quarterly POA&M submissions are required as part of the ISCM activities. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Initial: April 1 – July 1 (3:00 AM ET) ▪ Monthly submissions, as necessary, if outstanding findings. ▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit quarterly POA&Ms by the last business Day of March, July, September, and December.

Document	Description	Submission Requirements	Entity Responsible	Deadline
Risk Acceptance Form	<ul style="list-style-type: none"> ▪ The Risk Acceptance Form records the weaknesses that require an official risk acceptance from the organization's Authorizing Official. ▪ Before deciding to accept the risks, the relevant NEE's authorities should rigorously explore ways to mitigate the risks. 	<ul style="list-style-type: none"> ▪ 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&M. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ The Risk Acceptance Form should be submitted with the POA&M during the regular POA&M submission schedule.
Privacy Impact Assessment (PIA)	<ul style="list-style-type: none"> ▪ The PIA will detail the Prospective EDE Entity's evaluation of its controls for protecting PII. 	<ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Before commencing the privacy and security audit as part of the NEE SSP
Non-Exchange Entity System Security and Privacy Plan (NEE SSP)	<ul style="list-style-type: none"> ▪ The NEE SSP will include detailed information about the Prospective EDE Entity's implementation of required security and privacy controls. 	<ul style="list-style-type: none"> ▪ 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. ▪ The implementation of security and privacy controls must be completely documented in the NEE SSP before the audit is initiated. 	<ul style="list-style-type: none"> ▪ Prospective Primary and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Before commencing the privacy and security audit

Document	Description	Submission Requirements	Entity Responsible	Deadline
Incident Response Plan and Incident/Breach Notification Plan	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity is required to implement Breach and Incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures. ▪ A Prospective EDE Entity must incorporate these procedures into its own written policies and procedures.⁴⁵ 	<ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Before commencing the privacy and security audit as part of the NEE SSP

⁴⁵ <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf>.

<p>Annual Penetration Testing</p>	<ul style="list-style-type: none"> ▪ The penetration test must include the EDE environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10. ▪ 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 and must provide the following information to CMS, a minimum of five (5) business Days using the CMS-provided form⁴⁶, prior to initiation of the penetration testing: <ul style="list-style-type: none"> – Period of testing performance (specific times for all penetration 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. ▪ 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 mirrors the production environment. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the Penetration Test results with the SAR via the DE/EDE Entity PME Site. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities 	<ul style="list-style-type: none"> ▪ Initial: April 1 – July 1 (3:00 AM ET) ▪ 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.
------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Document	Description	Submission Requirements	Entity Responsible	Deadline
<p>Vulnerability Scan</p>	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity is required to conduct monthly Vulnerability Scans. 	<ul style="list-style-type: none"> ▪ A Prospective EDE Entity and its Auditor must submit the last three months of their Vulnerability Scan Reports, in conjunction with POA&M and SAR via the DE/EDE Entity PME Site. ▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&M. ▪ Similar findings can be consolidated. 	<ul style="list-style-type: none"> ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities. 	<ul style="list-style-type: none"> ▪ Initial: April 1 – July 1 (3:00 AM ET) ▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit Vulnerability Scans annually.

⁴⁶ 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	sgupta@absurance.com
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.⁴⁷ 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
Phase 1: Host Simplified Application + EDE API Suite	<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"> ▪ Application filer (and others on application, if applicable) resides in the application state and all dependents have the same permanent address, if applicable ▪ 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 ▪ 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 ▪ No household members are full-time students aged 18-22 ▪ No household member is pregnant ▪ All Applicants are U.S. citizens ▪ All Applicants can enter Social Security Numbers (SSNs) ▪ No Applicants are applying under a name different than the one on his/her Social Security cards ▪ No Applicants were born outside of the U.S. and became naturalized or derived U.S. citizens ▪ No Applicants are currently incarcerated (detained or jailed) ▪ No household members are American Indian or Alaska Native ▪ No Applicants are offered health coverage through a job or COBRA ▪ No Applicants are offered an individual coverage health reimbursement arrangement (HRA) or qualified small employer health reimbursement arrangement (QSEHRA) ▪ No Applicants were in foster care at age 18 and are currently 25 or younger ▪ All dependents are claimed on the Application filer's federal income tax return for the coverage year ▪ All dependents are the Application filer's children who are single (not married) and 25 or younger ▪ No dependents are stepchildren or grandchildren ▪ No dependents live with a parent who is not on the Application filer's federal income tax return 	<p>Lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.</p>

⁴⁷ 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
Phase 2: Host Expanded Simplified Application + EDE API Suite	<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"> ▪ All scenarios covered by Phase 1 ▪ Full-time student ▪ Pregnant application members ▪ Non-U.S. citizens ▪ Naturalized U.S. citizens ▪ Application members who do not provide an SSN ▪ Application members with a different name than the one on their SSN cards ▪ Incarcerated application members ▪ Application members who previously were in foster care ▪ Stepchildren 	<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>
Phase 3: Host Complete Application + EDE API Suite	<p>EDE Entity hosts an application that supports all application scenarios (equivalent to existing HealthCare.gov):</p> <ul style="list-style-type: none"> ▪ All scenarios covered in Phase 2 ▪ American Indian and Alaskan Native household members ▪ Application members with differing home addresses or residing in a State separate from where they are applying for coverage ▪ Application members with no home address ▪ Application members not planning to file a tax return ▪ Married application members not filing jointly ▪ 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) ▪ Application members offered coverage through their job, someone else's job, or COBRA ▪ Application members with dependent children who are over age 25 or who are married ▪ Application members with dependent children living with a parent not on their federal income tax return ▪ Dependents who are not sons/daughters ▪ Applicants who are offered an individual coverage HRA or QSEHRA 	<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 6

Thursday, September 5, 2024 at 13:02:50 Eastern Daylight Time

Subject: Re: CMS/Speridian
Date: Friday, August 30, 2024 at 7:52:24 PM Eastern Daylight Time
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
Attachments: image001.png

Hello David:

Please find our response to the questions you'd send on Aug 28. Files referenced are available in the Dropbox folder shared for previous queries. Link [Benefitalign Documents To CMS](#) .

Specifically, please find the following documents/folder:

[Benefitalign Response Aug 30 2024.pdf](#)

[VPC-Flow-log](#)

[Benefitalign Remote Access Acceptable Use Policy.pdf](#)

We would like to request a call with your team as soon as possible so we can provide any additional clarifications you may need and/or discuss any additional questions. Would appreciate your providing availability to meet on Tuesday.

Thanks
Manal.

From: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>
Sent: Wednesday, August 28, 2024 12:12 PM
To: Manal Mehta <manal.mehta@benefitalign.com>
Cc: Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Ashwini Deshpande. <ashwini.deshpande@Truecoverage.com>; Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>; Sonu S. Rajamma <sonu.sr@speridian.com>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Tamara White <tamara.white@benefitalign.com>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; Grant, Jeff (CMS/CCIIO)

<jeffrey.grant1@cms.hhs.gov>; CMS CCIIO Office of the Director
<CCIIOOfficeoftheDirector@cms.hhs.gov>; Shynihan Muhammed
<shynihan.muhammed@benefitalign.com>; Paradis, David (CMS/OIT)
<David.Paradis1@cms.hhs.gov>

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@benefitalign.com immediately if you suspect it's a suspicious email.

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 # (443)764-4514

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 <manal.mehta@benefitalign.com>

Sent: Thursday, August 22, 2024 10:25 AM

To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>

Cc: Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Ashwini Deshpande. <ashwini.deshpande@Truecoverage.com>; Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Busby, Keith (CMS/OIT)

<Keith.Busby@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>; Sonu S. Rajamma <sonu.sr@speridian.com>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Tamara White <tamara.white@benefitalign.com>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Shynihan Muhammed <shynihan.muhammed@benefitalign.com>
Subject: Re: CMS/Speridian

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) <David.Paradis1@cms.hhs.gov>
Date: Tuesday, August 20, 2024 at 3:29 PM
To: Kalpit Dantara <kalpit.dantara@Truecoverage.com>, Busby Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>, CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>, Montz Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>, Grant Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>, Girish Panicker <girish.panicker@speridian.com>, Manal Mehta <manal.mehta@benefitalign.com>, Ashwini Deshpande <ashwini.deshpande@Truecoverage.com>, Sonu S. Rajamma <sonu.sr@speridian.com>, Shynihan Muhammed <shynihan.muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Hunt Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>, Paradis David (CMS/OIT) <David.Paradis1@cms.hhs.gov>
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 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;

1. 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.
2. Irrespective of Role, EDE is only enabled if the user is ID Proofed.
3. 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.
4. 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.
5. Inactivity timeouts are set to 5 mins by default. Users can configure it to different times but cannot exceed 30 mins.
6. 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 # (443)764-4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>
Sent: Monday, August 19, 2024 12:04 AM
To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>; Ashwini Deshpande <ashwini.deshpande@Truecoverage.com>; Sonu S. Rajamma <sonu.sr@speridian.com>; Shynihan Muhammed <shynihan.muhammed@benefitalign.com>; tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>
Subject: RE: CMS/Speridian

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>, Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>, CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>, Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>, Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>, Girish Panicker <girish.panicker@speridian.com>, Manal Mehta <manal.mehta@benefitalign.com>, Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>, Sonu S. Rajamma <sonu.sr@speridian.com>, Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
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 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:

Agent gets a call [Lead] and this creates a Lead record in CustomerEngage [CRM].

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.

The customer record is synced into BrokerEngage [EDE].

The agent can navigate to BrokerEngage and see the newly created Customer Record.

The agent then can create Quotes/Proposals in BrokerEngage.

If the customer wants to enroll, the EDE Flow is initiated in BrokerEngage by the agent.

When the application is completed and submitted, the BrokerEngage Customer Record Status is updated to reflect the enrolled status.

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.

Regards,

-Dave

David V. Paradis

Primary contact # (443)764-4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>

Sent: Thursday, August 15, 2024 6:22 PM

To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Busby, Keith (CMS/OIT)

<Keith.Busby@cms.hhs.gov>; CMS CCIIO Office of the Director

<CCIIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO)

<Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Girish

Panicker <girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>;

Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>; Sonu S. Rajamma

<sonu.sr@speridian.com>; Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>;

tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>;

Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO)

<Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>

Cc: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Hunt, Patrick (CMS/OIT)

<Patrick.Hunt@cms.hhs.gov>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>

Subject: Re: CMS/Speridian

Hi David,

We have added the requested data in the dropbox shared yesterday.

[Benefitalign Documents To CMS](#)

The file name is FSFADOM3-FGT_elog_TC-VPN.csv. Please note that the VPN logs are only retained for 3 weeks.

This log contains the employees from your list who have accessed AWS through the Forticlient VPN (54.157.134.187).

The other two VPNs have not been used by any of these employees.

The employees that are not in this log file have accessed AWS through our Albuquerque, NM office network.

Also - not all employees on your list have access to BenefitAlign BrokerEngage/Inshura EDE platforms as they work on other applications.

If you have questions, we are available to meet at your convenience.

-Kalpit

From: Kalpit Dantara <kalpit.dantara@Truecoverage.com>
Date: Thursday, August 15, 2024 at 1:20 PM
To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>, Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>, CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>, Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>, Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>, Girish Panicker <girish.panicker@speridian.com>, Manal Mehta <manal.mehta@benefitalign.com>, Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>, Sonu S. Rajamma <sonu.sr@speridian.com>, Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>, Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>
Subject: Re: CMS/Speridian
Hi David,

Let me have my team work on getting this data to you.

-Kalpit

From: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>
Date: Thursday, August 15, 2024 at 11:58 AM
To: Kalpit Dantara <kalpit.dantara@Truecoverage.com>, Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>, CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>, Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>, Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>, Girish Panicker <girish.panicker@speridian.com>, Manal Mehta <manal.mehta@benefitalign.com>, Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>, Sonu S. Rajamma

<sonu.sr@speridian.com>, Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>

Cc: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>, Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>

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 immediately if you suspect it's a suspicious email.

Kalpit,

Thank you for the additional information!

Could we request a copy of the last three months of logs from each of these VPN solutions that show the datestamped true source IP's connecting, translation to specific VPN IP's and what they connected to – Narrowed by the following list of users?

amit.kumar1@speridian.com
boravancha.manogna@speridian.com
girish.sasidharan@speridian.com
jerin.george@speridian.com
manish.awasthi@speridian.com
muhammad.ahmed@speridian.com
prakash.moni@speridian.com
raghavendra.kumar@speridian.com
rakesh.rathi@speridian.com
rakesh.reddy@speridian.com
rana.pratap@speridian.com
sabari.chandran@speridian.com
siva.radhakrishnan@benefitalign.com
sonu.rajamma
sreekanth.g@speridian.com
sreekumar.venukumar1@speridian.com
sumankumar.patra@speridian.com
syed.nijamuddin@speridian.com
umar.farooque@speridian.com
venu.telagathoti@speridian.com

Regards,

-Dave

David V. Paradis

Primary contact # (443)764-4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>
Sent: Thursday, August 15, 2024 10:45 AM
To: Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; CMS CCIO Office of the Director <CCIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIO) <Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIO) <jeffrey.grant1@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>; Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>; Sonu S. Rajamma <sonu.sr@speridian.com>; Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>; tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Dorsey, Kevin Allen (CMS/CCIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIO) <Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Subject: Re: CMS/Speridian

Hi Keith,

We have confirmed that there are 3 VPN solutions being used by the organization – 2 FortiClient solutions hosted inhouse and a Palo Alto solution used as a SaaS product.

-Kalpit

From: Keith.Busby@cms.hhs.gov
When: 9:00 AM - 10:00 AM August 15, 2024
Subject: CMS/Speridian
Location: <https://cms.zoomgov.com/j/1602119654?pwd=RbZ0g15kA0lJG8mBATuh8EDbeXInj.1>

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 immediately if you suspect it's a suspicious email.

Amended Declaration of Girish Panicker

1. My name is Girish Panicker. I am over the age of 18 and am competent to testify to the matters set forth in this Declaration.

2. I am the Founder and Chairman of Speridian Group of Companies which include TrueCoverage, LLC (“TrueCoverage”), Benefitalign LLC (“Benefitalign”) and Speridian Technologies (“Speridian”). I am authorized to make this Declaration on behalf of TrueCoverage and Benefitalign LLC.

3. Benefitalign is a Software-as-a-Service (“SaaS”) Platform company that specializes in software platforms for health insurance stakeholders including insurance carriers, agents and brokers and Third Party Administrators (“TPA”) of insurance companies. One of the software platforms that Benefitalign owns and operates is BrokerEngage™ which is typically licensed to Brokers and Agents. The BrokerEngage™ Platform also has a special certification provided by Center of Medicare & Medicaid Services (“CMS”) known as Enhanced Direct Enrollment (“EDE”) that allows consumers, agents, and brokers to shop and enroll customers in Qualified Health Plans (“QHP”) under the Affordable Care Act (“ACA”).

4. Plaintiff Benefitalign has been an approved Direct Enrollment (“DE”) and its successor Enhanced Direct Enrollment (“EDE”) entity since 2017 and licenses this capability under its BrokerEngage™ Platform to agents/brokers and insurance carriers. Besides BrokerEngage™, Benefitalign also delivers other end-to-end technology solutions for Benefits Administration, namely EmployerEngage™, and Customer Relationship Management (CustomerEngage™), across all lines of business for carriers, agencies, brokers, and employers. Additionally, Benefitalign also offers its “BrokerEngage™” EDE platform as a white-labelled solution to carriers, agencies, and agents/brokers. One such white-labelled solution of BrokerEngage™ is

licensed by its affiliate company TrueCoverage under the brand name “*Inshura*.”

5. Plaintiff TrueCoverage is a private health insurance marketplace for individuals, families, and employers. It is a “One-Stop-Insurance Shop” where consumers and agents—including TrueCoverage agents—(on behalf of consumers) can shop, compare, and enroll in qualified health insurance plans under the Affordable Care Act. TrueCoverage offers insurance plans from more than 600 top carriers across the country. TrueCoverage is an approved web-broker pursuant to 45 C.F.R. § 155.220. In addition, d/b/a its “Inshura” brand, TrueCoverage has Centers for Medicare and Medicaid Services (“CMS”) approval to offer a free white-labelled health plan quoting and enrollment platform, using the Benefitalign BrokerEngage™ platform, to agencies and agents/brokers. Marketed as Inshura, TrueCoverage does not charge agents a user subscription fee and instead makes money from referrals submitted by agents.

6. The BrokerEngage™ platform and its white-labelled version Inshura, which Benefitalign and TrueCoverage use respectively is key to serving their carrier, broker, and agent customers. As an approved EDE Platform, the platform enables access to CMS APIs for conducting eligibility and enrollment. Customers need access to databases operated by the CMS in order to function. Benefitalign and TrueCoverage designed their businesses to interact seamlessly with CMS databases.

7. The majority of TrueCoverage and Benefitalign’s revenues come from operating an EDE Platform that accesses the ACA exchanges.

8. TrueCoverage and Benefitalign rely on revenues from supporting entities that participate in the ACA marketplace. Without the ability to access the healthcare exchanges, the companies’ EDE Platform cannot function. If the EDE Platform cannot function, the companies cannot generate any revenue.

TrueCoverage and Benefitalign's Prior Interactions with CMS

9. Prior disputes between TrueCoverage or Benefitalign, on the one hand, and CMS on the other, have been relatively minor and quickly resolved.

10. On April 19, 2018, CMS preliminarily suspended TrueCoverage's 2018 Marketplace Agreements and proposed to terminate those agreements and deny TrueCoverage its right to enter Exchange agreements through the end of open enrollment for the 2021 Plan Year. TrueCoverage duly requested reconsideration of the preliminary decision. The reconsideration was denied in part and granted in part, with CMS upholding its termination of TrueCoverage's 2018 Marketplace Agreements, but rescinding its proposed denial of TrueCoverage's right to enter future agreements and allowing TrueCoverage to participate in open enrollment for Plan Year 2019. The suspension arose from the unnecessary mandatory inclusion of a field for social security numbers in the then-current, early version of the DE platform used by TrueCoverage agents. In situations where customers were unable to provide their social security numbers, agents were unable to complete an application even where the consumer consented to the enrollment, as filling the social security number field was necessary to complete the application flow. To overcome the problem, agents typed in a placeholder number.

11. In its request for reconsideration, TrueCoverage maintained that all of the affected enrollments were legitimate, authorized enrollments, and that it and its agents did not nor did they intend to commit fraud by entering those placeholder numbers. CMS, "after due consideration of the rebuttal evidence submitted" as part of TrueCoverage's reconsideration request, determined the submission of the placeholder information was non-compliant, even if not fraudulent. TrueCoverage accepted this result. CMS has noted that it was satisfied with the good-faith evidence provided by TrueCoverage during the response and reconsideration process. Further,

there was no finding of fraudulent or abusive conduct against TrueCoverage, and neither this nor any similar non-compliance issue has recurred.

12. CMS suspended TrueCoverage dba Inshura on October 3, 2022, for failing to submit satisfactory independent audit documentation assessing its additional functionality to implement consumer and agent/broker identity proofing as required by the CMS EDE guidelines. TrueCoverage quickly responded that it had not understood the requirement to submit those documents. There was no gap in TrueCoverage's procedures to implement the "identity-proofing" functionality, and the required documentation was provided on October 11, 2022. CMS then immediately confirmed TrueCoverage/Inshura's compliance and lifted the suspension on October 12, 2022.

13. CMS issued a Notice of Non-compliance to Benefitalign on April 6, 2023, based on CMS's identification of an attempt to access a CMS test server from India on March 8, 2023. This was an isolated incident on one test server that did not house any production data or consumer personally identifiable information. CMS did not suspend or terminate Benefitalign's access, but instead asked Benefitalign to submit a signed acknowledgement and plan to remediate the issue. Benefitalign duly and timely submitted the required materials. CMS has not required any further action and no suspension was imposed. Benefitalign implemented additional geo-fencing controls on lower environments similar to those in production, and since then there have been no further reports of non-compliant access. CMS has not required any further action and no suspension was imposed.

14. Plaintiffs and CMS have had a longstanding, cooperative working relationship, which these details do not negate. In every instance when CMS has raised concerns about compliance with CMS regulations and agreements, Plaintiffs have promptly responded and fully addressed

CMS' concerns. Regarding CMS's assertion that since the April 6, 2023 Notice of Noncompliance was served and Benefitalign's response, CMS has "corresponded with Speridian Companies on a near monthly basis regarding a variety of noncompliance issues," Plaintiffs – like all primary EDE partners – have participated in group monthly calls with CMS where issues generally applicable to all partners are discussed. Plaintiffs do not recall that CMS ever raised any Plaintiff-specific non-compliance issue on those calls, or otherwise since Benefitalign complied with CMS's April 6, 2023 Notice of Noncompliance. The purpose of the group calls has been open communication to prophylactically address any common issues, not address specific noncompliance concerns particular to Plaintiffs.

CMS Suspension of TrueCoverage and Benefitalign EDE Platform

15. On Thursday, August 8 at 6:37 PM I received an email from Jeffrey D. Grant, Deputy Director for Operations for CMS. The email stated that "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." See Exhibit A. I responded to Mr. Grant that evening requesting a call to discuss the potential anomalies referenced in his email. See Exhibit A.

16. Eventually CMS agreed to a series of meetings and email exchanges. For the remainder of the month of August, our technical team responded to CMS's questions and provided representatives from CMS with the information we understood they were requesting. See Exhibits A-I. Early in that process, I reiterated to Mr. Grant that "the suspension is having catastrophic consequences for our business, our clients who rely on our platform and most importantly customers. The impact is multiplying by the hour." See Exhibit G. At no point, during this process, however, did CMS tell us what specific concerns they had or what we could do to alleviate them.

17. Facing ruin, and with no answers from CMS, we were forced to file suit on August 28, 2024.

18. Thereafter, on September 2, 2024, CMS sent us a letter stating that we would be immediately suspended, describing the reasons for its suspension decision, announcing that it would initiate an audit of Benefitalign and TrueCoverage and that it would leave the suspension in place for the duration of the audit. However, audits take months, and Benefitalign and TrueCoverage will be driven out of business within weeks if the suspension remains in place. If CMS proceeds with this course of action, there will be nothing left standing to audit, and the irreparable harm will be complete.

19. To date, the EDE Platform and brokerage remain cut off from EDE Access.

Impact of CMS Suspension on TrueCoverage and Benefitalign

20. CMS's ongoing suspension of Benefitalign and TrueCoverage's EDE access administered by CMS has already ground Plaintiffs' ability to do business to a halt, and each day of ongoing suspension jeopardizes their ability to stay in business.

21. The CMS suspension threatens practically all of the revenue generated by TrueCoverage and Benefitalign. The EDE Platform forms the foundation for brokers and agencies to sell healthcare plans to new customers and serve existing customers. Benefitalign and TrueCoverage work with over 5,000 such brokers and agencies, each of whom simply cannot perform these functions if they do not have access to the EDE Platform where all the relevant information resides.

22. Indeed, in the month since the CMS initial suspension, many brokers and agencies that previously used the Benefitalign and/or Inshura EDE Platform have turned to other, functioning, EDE platforms to enroll customers, resulting in a substantial, overwhelming loss of revenue to

Benefitalign and TrueCoverage. With the open enrollment period quickly approaching, this trend will accelerate if Plaintiffs' EDE Platform is not reinstated. Unless the EDE Platform is quickly reinstated, well in advance of open enrollment, Benefitalign and TrueCoverage are almost certain to lose their remaining customers permanently.

23. The ACA open enrollment period begins November 1, 2024. The only hope for TrueCoverage and Benefitalign to salvage their business is to regain EDE access in advance of the ACA open enrollment period's start on November 1, in order to restart their businesses, secure new customers, and secure the relationships with agencies and brokers needed to participate in the open enrollment season. If TrueCoverage and Benefitalign can retain, regain, or secure new agencies and brokers who either do not have current access to a platform or are looking to switch away from another platform in advance of open enrollment, then the businesses have a chance to survive. Otherwise, all existing brokers and agencies will migrate to functioning platforms. Without immediate EDE access, TrueCoverage and Benefitalign will not have time to secure the relationships they need to participate meaningfully in the open enrollment season. If TrueCoverage and Benefitalign are unable to participate in the upcoming enrollment period, the business's demise will be imminent.

24. TrueCoverage itself is a purveyor of healthcare plans and uses the Benefitalign platform to enroll new customers and service existing customers. TrueCoverage works with, and provides support to, over 150,000 customers. It receives at least 300 customer calls each day. Its ability to support customers without access to its EDE Platform is in jeopardy. As long as CMS renders its EDE Platform non-functional, TrueCoverage cannot perform these functions, resulting in ongoing loss of revenue.

25. The same is true for the health insurance carriers, such as AvMed Health Plans, that use

our EDE Platform and whose operations are severely affected by the suspension of the EDE Platform. Without access to platform-based records showing which customers have health insurance plans with the carrier and what their plans cover, the carriers are hamstrung in their ability to serve existing customers.

26. Ongoing suspension of our EDE Platform also risks initiating a torrent of license termination proceedings against TrueCoverage from state insurance departments.

27. TrueCoverage has a \$20 million loan from its banking partners and is required to demonstrate a revenue stream each month to sustain that loan. But because CMS's suspension virtually destroys all revenues that TrueCoverage and Benefitalign receive, the suspension will render TrueCoverage unable to satisfy the requirements of its loan.

28. TrueCoverage works with over 100 employees whose ongoing employment is jeopardized by the CMS suspension. As revenues plummet while brokers and carriers turn to EDE platform alternatives, TrueCoverage's ability to retain its employee base will rapidly diminish.

29. As revenue evaporates, TrueCoverage and Benefitalign risk being unable both to sustain its loan and to compensate its employees, either of which will force them to cease operations.

Impact of CMS Suspension on Consumers and Other Third Parties

30. The suspension also threatens to deny consumers access to affordable healthcare plans, prevent brokers and agents from accessing customer records, and deny insurance carriers and doctors the ability to confirm the existence and scope of customers' health coverage.

31. The EDE Platform is an important tools for consumers, often low-income individuals, who seek timely access to affordable healthcare. The EDE Platform aggregates information about different carriers' health plan offerings and serves as a search engine to identify health plans available to that individual. Health insurance brokers use it to input information about potential

customers who need access to healthcare, determine what health insurance plan offerings the customer is eligible for, determine if the customer is eligible for any subsidy, and enroll the customer in their chosen health plan.

32. Since CMS's suspension, brokers have been unable to access the EDE Platform and have thus been unable to sell health insurance to new customers who need it to fund their healthcare. With each day that passes, more potential customers will be rebuffed in their efforts to enroll in health insurance.

33. The suspension will also have drastic impact on customers who are already enrolled in a health plan and who require service on that plan. The EDE Platform serves as a virtual "filing cabinet" of customer records. These records help determine, for example, what medical care is and is not covered by the enrolled customer's health insurance plan. Brokers cannot service current customers without access to those customer records.

34. For example, customers call brokers with questions about the scope of their existing coverage under their current health plan. Without access to the customer's records, brokers will be unable to confirm for a customer whether or not particular medical care is covered by their plan. Customers may also seek to alter their health plans-for example, they may wish to add a dependent to their plan. An open enrollment health insurance period is coming up imminently-a time when many customers make adjustments to their health coverage. Without access to customer records, brokers will be unable to honor customers' requests for change. Similarly, health plan enrollees are often required to submit documentation proving their health plan coverage-but without access to the EDE Platform containing those records, they will be unable to do so.

35. CMS's suspension of the EDE Platform means that new consumers face considerable obstacles in accessing affordable health coverage, while existing consumers face obstacles in

exercising their benefits under their existing health plans. With the Benefitalign and Inshura EDE Platform shut down, brokers and agencies have lost access to a key tool that, for years, has allowed them to help consumers shop for and enroll in affordable healthcare plans.

36. If Benefitalign and TrueCoverage go out of business, they will be unable to participate in the upcoming open enrollment period, leaving consumers with fewer choices for their health coverage needs.

37. Moreover, consumers who already purchased plans through Plaintiffs' EDE Platform have lost access to their customer records, which will prevent brokers from answering important questions about the scope of consumers' coverage under their existing plans. Consumers will also lose the ability to make changes to their existing plans or to obtain documentation proving that they have health coverage.

38. Likewise, insurance carriers will be unable to verify that a particular consumer is actively enrolled in one of the carrier's health plans, nor will the carrier be able to answer questions about services that are covered by their plan. Several health insurance carriers use the EDE Platform to do business, and their ability to serve current customers is severely impacted by its abrupt unavailability.

39. To provide one common example, patients are required to submit insurance documentation prior to a medical appointment. The medical office commonly contacts the health insurance carrier's Provider Services line to verify coverage so that the patient can be treated. But without access to customer records stored on the EDE Platform, carriers will be unable to verify whether a particular individual is actively enrolled in one of that carrier's health plan offerings, which impacts the patient's ability to receive medical treatment from the contacting medical office.

40. Similarly, an individual may contact the carrier's Member Services line to inquire about

their health insurance coverage-and without access to the customer's records, the carrier will be unable to provide that information.

41. Enrolled customers may also contact TrueCoverage directly to request this information. TrueCoverage receives approximately 300 such calls each day. Without access to the customer's records, TrueCoverage will be unable to respond to the customers' inquiries.

42. TrueCoverage also works with multiple downline agencies that license the Benefitalign and Inshura EDE Platform. In these instances, TrueCoverage acts as an interface between the health insurance carrier and the broker agency: TrueCoverage facilitates the carrier appointments, and the revenue from the downline agencies' sales of that carrier's health plans passes to TrueCoverage, which passes it along to the downline agency that made the sale.

43. The downline agencies with which TrueCoverage works have approximately 200,000 customers they support, and their ability to support these customers without access to the EDE Platform will be in jeopardy.

44. CMS's abrupt suspension will thus lead to carriers in turn suspending payments, and any suspension of payments by carriers to TrueCoverage will impact TrueCoverage's ability to transmit payment to downline agencies. Most such agencies are small to mid-size organizations that could not survive for more than a month if their payments are not timely released. These agencies employ hundreds of individuals whose ongoing employment will be jeopardized by the suspension.

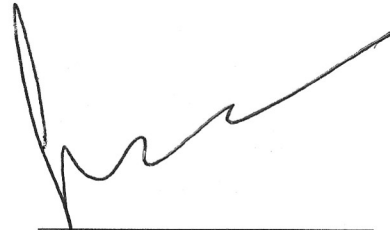
TrueCoverage and Benefitalign's EDE Platform

45. Benefitalign's EDE Platform is called BrokerEngage™, which TrueCoverage d/b/a Inshura also offers as the Inshura EDE Platform. This EDE Platform is connected to the Marketplaces but is not interconnected with overseas computers at all. Benefitalign and

TrueCoverage have repeatedly made this fact clear to CMS over the past month.

I declare under penalty of perjury that the foregoing is true and correct.

Date: September 6, 2024

A handwritten signature in black ink, consisting of a series of loops and a long horizontal stroke extending to the right.

Girish Panicker

Exhibit A

RE: EDE/DE/EBP Suspension

Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Tue 8/13/2024 9:37 AM

To: Girish Panicker <girish.panicker@speridian.com>; Pringle (she/her), Megan (CMS/CCIIO) <Megan.Pringle@cms.hhs.gov>; Seaman, Patrick (CMS/CCIIO) <patrick.seaman@cms.hhs.gov>
Cc: Lowery, Bradley (CMS/CCIIO) <Bradley.Lowery@cms.hhs.gov>

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 immediately if you suspect it's a suspicious email.

We will schedule a call with you this PM. We will not have our lawyers on as this is going to be a specific discussion of what we have found. If you bring legal counsel we will have to get our legal team together and that will take more time to set up. Look for an appointment for early afternoon.

Jeff

Jeffrey D. Grant

Deputy Director for Operations

Center for Consumer Information and Insurance Oversight

Centers for Medicare & Medicaid Services

From: Girish Panicker <girish.panicker@speridian.com>**Sent:** Tuesday, August 13, 2024 11:08 AM**To:** Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Pringle (she/her), Megan (CMS/CCIIO) <Megan.Pringle@cms.hhs.gov>; Seaman, Patrick (CMS/CCIIO) <patrick.seaman@cms.hhs.gov>**Cc:** Lowery, Bradley (CMS/CCIIO) <Bradley.Lowery@cms.hhs.gov>; Fried, Bruce Mer in <bruce.fried@dentons.com>**Subject:** RE: EDE/DE/EBP Suspension

Jeff,

Yes, Bruce/Dentons represents us. We're very eager to discuss the matter with you through any channel that CMS is willing to use, including Bruce, who is copied here.

Sincerely,

Girish

From: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>**Sent:** Tuesday, August 13, 2024 10:41 AM**To:** Girish Panicker <girish.panicker@speridian.com>; Pringle (she/her), Megan (CMS/CCIIO) <Megan.Pringle@cms.hhs.gov>; Seaman, Patrick (CMS/CCIIO) <patrick.seaman@cms.hhs.gov>**Cc:** Lowery, Bradley (CMS/CCIIO) <Bradley.Lowery@cms.hhs.gov>**Subject:** RE: EDE/DE/EBP Suspension

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 immediately if you suspect it's a suspicious email.

Good morning,

We were contacted last Friday afternoon by Bruce Fried, saying that he and his firm, Denton, were representing your company. He also said that he was aware that you had asked for a meeting and then requested that we speak with him before we talk with you. That has temporarily delayed our ability to speak with you as we needed to verify what our response to his request should be. We now need to confirm with you that Bruce Fried is indeed representing your company and would like to know how you would like to proceed here.

Jeff

Jeffrey D. Grant
Deputy Director for Operations
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services

From: Girish Panicker <girish.panicker@speridian.com>
Sent: Tuesday, August 13, 2024 10:02 AM
To: Pringle (she/her), Megan (CMS/CCIIO) <Megan.Pringle@cms.hhs.gov>; Seaman, Patrick (CMS/CCIIO) <patrick.seaman@cms.hhs.gov>
Cc: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Lowery, Bradley (CMS/CCIIO) <Bradley.Lowery@cms.hhs.gov>
Subject: FW: EDE/DE/EBP Suspension

Megan/Patrick,

Please see my urgent message to Jeff Grant below. I am forwarding this to you as per Mr. Lowery out-of-office message. Would you please respond as soon as possible?

Sincerely,

Girish Panicker

From: Girish Panicker
Sent: Tuesday, August 13, 2024 9:58 AM
To: bradley.lowery@cms.hhs.gov
Cc: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Subject: FW: EDE/DE/EBP Suspension

Dear Mr. Lowery,

Please see my urgent message to Jeff Grant below. I am forwarding this to you as per his out-of-office message. Would you please respond as soon as possible?

Sincerely,

Girish Panicker

From: Girish Panicker
Sent: Tuesday, August 13, 2024 9:40 AM
To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Subject: RE: EDE/DE/EBP Suspension

Dear Jeff,

Five days have now passed since your August 8, 2024 email informing me that "Inshura/TrueCoverage and Benefitalign EDE access has been suspended due to "potential anomalous activity" You said in that email, "CMS will follow up with additional communication to provide next steps." In your last communication on Friday, August 09th 2024, you mentioned that you will be scheduling a call to discuss the matter, but we have heard nothing.

As you know, your unexplained decision to cut off our companies from EDE, DE, and EBP is devastating to our business, our employees, our downline agencies, and customers. In fact, it threatens to imminently put us out of business. This is an emergency for us.

What does “*potential anomalous activity*” mean?

When will you restore our access?

Do you have any concerns about our companies’ participation in EDE, DE, and EBP? If so, what are they?

Sincerely,

Girish Panicker

From: Girish Panicker

Sent: Friday, August 9, 2024 10:06 AM

To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Subject: RE: EDE/DE/EBP Suspension

Thanks Jeff. Really appreciate your quick response. Will wait for your call.

Meanwhile, I have asked the team to hold off their communication with the clients till we get some clarity and direction from CMS.

Girish

From: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Sent: Friday, August 9, 2024 9:57 AM

To: Girish Panicker <girish.panicker@speridian.com>

Subject: RE: EDE/DE/EBP Suspension

You don't often get email from jeffrey.grant1@cms.hhs.gov. [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 immediately if you suspect it's a suspicious email.

We will be setting up a call. I have to coordinate with the CMS information systems security team in a different office from CCIIO and a few others. We will reach out to you when we have found a time that we can get this on the books today.

Jeff

From: Girish Panicker <girish.panicker@speridian.com>

Sent: Thursday, August 8, 2024 8:50 PM

To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Subject: RE: EDE/DE/EBP Suspension

Jeff,

I just saw this email which is very concerning. Can you please let us know what these potential anomalies are so that we can review them? This has serious business consequences for us as well as the partners who use the platform.

If you are available, I would like to get on a quick call with you first thing in the morning OR as per your convenience to understand this better

Girish Panicker

From: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Sent: Thursday, August 8, 2024 6:37 PM

To: girish.panicker <girish.panicker@benefitalign.com>

Cc: Tamara White <tamara.white@speridian.com>; Sonu Rajamma <sonu.sr@benefitalign.com>

Subject: EDE/DE/EBP Suspension

You don't often get email from jeffrey.grant1@cms.hhs.gov. [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 immediately if you suspect it's a suspicious email.

This message has originated from an **External Source**. Please use proper judgment and caution before attending it. Please report it to phishing.report@benefitalign.com immediately if you suspect it's a suspicious email.

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 B

From: [Fried, Bruce Merlin](#)
To: [Grant, Jeff \(CMS/CCIIO\)](#)
Subject: Re: Please call me
Date: Friday, August 9, 2024 5:43:15 PM

Jeff,

Thanks very much for getting back to me.

By way of background, my colleagues at Dentons and I have been assisting TrueCoverage following it's been named as a defendant in the Florida lawsuit.

We have exercised significant due diligence and have found nothing to suggest that TrueCoverage or its associated companies have been involved in any way in improper or even questionable activities regarding churning or switching ACA enrollees or misleading those interested in possible enrollment. In fact, based on our due diligence, we feel quite comfortable that TrueCoverage has taken proactive steps to prevent improper activities by brokers, and, when improper activities have been found, they have terminated those brokers from their EDE system.

I was very surprised and more than a bit disappointed when I was informed of TrueCoverage being suspended from EDE activities as result of "potential anomalous activities." While I understand a more detailed notice is forthcoming, in my time at HCFA and during the many years of my representing organizations facing enforcement actions by CMS, I have never heard of CMS imposing sanctions for "potential" improper activities. On that basis, alone, I would ask CMS to rescend the suspension of TrueCoverage.

As you can imagine, with TrueCoverage being suspended from the EDE system, brokers seeking to use TrueCoverage are finding it inaccessible and are already turning to other means of enrolling people. The longer the suspension applies, the greater the number of brokers who will turn elsewhere. The irreparable harm resulting from this loss of business jeopardizes the existence of TrueCoverage and its associated companies.

Similarly, it is our understanding that CMS is to notify the state insurance commissioners regarding suspensions of this sort. We ask that you delay any notification to state insurance commissioners until such time as TrueCoverage is informed of the "potential anomalous activities" and is provided with an opportunity to address CMS's concerns.

Indeed, we request that CMS end TrueCoverage's suspension immediately given the lack of information that has been provided, that the suspension is based, at least in part, on "potential" activities, and that TrueCoverage is already confronting irreparable harm as a result.

Finally, on behalf of TrueCoverage, we request a direct meeting with you too fully review these issues and address CMS' concerns.

Thanks again for your consideration. I look forward to hearing from you. Please call me if I can provide any additional information.

Best regards,

Bruce
Office: 202-408-9159
Mobile: 202-744-2393

Bruce Merlin Fried
Partner

 +1 202 408 9159

Assistant: Patricia L. Parris +1 202 408 6943
Washington, DC

From: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Sent: Friday, August 9, 2024 5:03:51 PM
To: Fried, Bruce Merlin <bruce.fried@dentons.com>
Subject: Re: Please call me

[WARNING: EXTERNAL SENDER]

Hi Bruce,
Could you please let me know the nature of what you want to discuss? We will not be setting up any discussion until Monday at this point.
Jeff

Get [Outlook for iOS](#)

From: Fried, Bruce Merlin <bruce.fried@dentons.com>
Sent: Friday, August 9, 2024 3:11:54 PM
To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Subject: Please call me

Jeff,

I would appreciate it if you would give me a call. My colleagues and I at Dentons are counseling TrueCoverage regarding the EDE issues. I understand that TrueCoverage's CEO has asked to meet with you. I think it would be helpful if we touched base prior to that.

Thanks, Jeff

Bruce

202-744-2393

Bruce Merlin Fried
Partner

 +1 202 408 9159

bruce.fried@dentons.com | [Bio](#) | [Website](#)

Assistant: Patricia L. Parris +1 202 408 6943

Dentons US LLP | 1900 K Street, NW, Washington, DC 20006-1102

[Logo](#)

[Our Legacy Firms](#) | [Client Experience \(CX\)](#)

Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This email may be confidential and protected by legal privilege. If you are not the intended recipient, disclosure, copying, distribution and use are prohibited; please notify us immediately and delete this copy from your system. Please see [dentons.com](https://www.dentons.com) for Legal Notices.

Exhibit C

Automatic reply: EDE/DE/EBP Suspension

Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Tue 8/13/2024 9:40 AM

To: Girish Panicker <girish.panicker@speridian.com>

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 immediately if you suspect it's a suspicious email.

I am away from the office from Monday August 12 through Friday, August 16 on official travel to a couple of conferences. I return to the office August 19. I will have intermittent access to email or internet this week.

If you need immediate assistance, please contact bradley.lowery@cms.hhs.gov.

Thank you,

Jeff Grant

Deputy Director for Operations

Center for Consumer Information and Insurance Oversight

Centers for Medicare & Medicaid Services

Exhibit D

Automatic reply: EDE/DE/EBP Suspension

Lowery, Bradley (CMS/CCIIO) <Bradley.Lowery@cms.hhs.gov>

Tue 8/13/2024 9:58 AM

To: Girish Panicker <girish.panicker@speridian.com>

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 immediately if you suspect it's a suspicious email.

I'm currently out of the office, will return on Wednesday, 08/14/24.

For our CCIIO/FO Senior Leadership's availability or urgent requests please contact Megan Pringle at Megan.Pringle@cms.hhs.gov and Patrick Seaman at Patrick.Seaman@cms.hhs.gov.

For scheduling please contact Everett Smith at Everett.Smith@cms.hhs.gov or Lourdes Antezana at Lourdes.Antezana1@cms.hhs.gov.

Any urgent Timecard Issues please contact Christina Johnson at Christina.Johnson@cms.hhs.gov and Paola Roos at Paola.Roos@cms.hhs.gov.

Thank you so much,
Brad Lowery

Exhibit E

Automatic reply: EDE/DE/EBP Suspension

Pringle (she/her), Megan (CMS/CCIIO) <Megan.Pringle@cms.hhs.gov>

Tue 8/13/2024 10:02 AM

To: Girish Panicker <girish.panicker@speridian.com>

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 immediately if you suspect it's a suspicious email.

Thank you for your email. I am out of the office without access until Monday August 12th, and then at a conference with limited access to email through Friday August 16th. If your message is in regards to scheduling time with CCIIO's senior leadership team, please contact Brad Lowery (Bradley.Lowery@cms.hhs.gov). If it pertains to an urgent matter that cannot await my return, please reach out to Patrick Seaman (Patrick.Seaman@cms.hhs.gov). Otherwise, I will respond to your message as soon as possible.

Thanks,

Megan

Megan Pringle

Special Assistant to the Deputy Director for Operations

CCIIO/CMS

Megan.Pringle@cms.hhs.gov | 443.862.5595

Pronouns: she/her

Exhibit F

Re: EDE/DE/EBP Suspension

Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Wed 8/14/2024 5:26 PM

To: Girish Panicker <girish.panicker@speridian.com>

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 immediately if you suspect it's a suspicious email.

Girish,

Keith and his team have some questions and will be looking to set up a follow up with your team. We are not in a position to talk about a reconnection timetable without having made the determinations that we need to make. Keith is going to reach out to the group email where the information was exchanged.

I have been in meetings with insurance commissioners all day and so not been able to reply as promptly as usual.

Jeff

Get [Outlook for iOS](#)

From: Girish Panicker <girish.panicker@speridian.com>

Sent: Wednesday, August 14, 2024 10:58:01 AM

To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Subject: Re: EDE/DE/EBP Suspension

Jeff,

Sorry to bother you again. Is there any update from Keith and team? It would be helpful if we understand the timeline for getting things back up. I would like to provide all the clients some more clarity on timeline.

Girish

Get [Outlook for iOS](#)

From: Girish Panicker <girish.panicker@speridian.com>

Sent: Wednesday, August 14, 2024 10:07:46 AM

To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Subject: Re: EDE/DE/EBP Suspension

Jeff

I understand Keith and team have received all documents they requested from my tech team. Let me know once you had a chance to talk with Keith and if he has any additional questions .

Girish

Get [Outlook for iOS](#)

From: Girish Panicker <girish.panicker@speridian.com>
Sent: Tuesday, August 13, 2024 2:55 PM
To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Subject: RE: EDE/DE/EBP Suspension

Jeff,

Thanks for arranging the call. My phone # is 609 351 0034. Please call me when you get a chance. I am available anytime today.

Girish

From: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Sent: Tuesday, August 13, 2024 11:58 AM
To: Girish Panicker <girish.panicker@speridian.com>; Pringle (she/her), Megan (CMS/CCIIO) <Megan.Pringle@cms.hhs.gov>; Seaman, Patrick (CMS/CCIIO) <patrick.seaman@cms.hhs.gov>
Cc: Lowery, Bradley (CMS/CCIIO) <Bradley.Lowery@cms.hhs.gov>
Subject: RE: EDE/DE/EBP Suspension

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 immediately if you suspect it's a suspicious email.

We are scheduling for 2:30. Please have any relevant, knowledgeable operations, security and/or systems staff attend as we will be discussing technical findings.
Jeff

From: Girish Panicker <girish.panicker@speridian.com>
Sent: Tuesday, August 13, 2024 10:02 AM
To: Pringle (she/her), Megan (CMS/CCIIO) <Megan.Pringle@cms.hhs.gov>; Seaman, Patrick (CMS/CCIIO) <patrick.seaman@cms.hhs.gov>
Cc: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Lowery, Bradley (CMS/CCIIO) <Bradley.Lowery@cms.hhs.gov>
Subject: FW: EDE/DE/EBP Suspension

Megan/Patrick,

Please see my urgent message to Jeff Grant below. I am forwarding this to you as per Mr. Lowery out-of-office message. Would you please respond as soon as possible?

Sincerely,

Girish Panicker

From: Girish Panicker
Sent: Tuesday, August 13, 2024 9:58 AM
To: bradley.lowery@cms.hhs.gov
Cc: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Subject: FW: EDE/DE/EBP Suspension

Dear Mr. Lowery,

Please see my urgent message to Jeff Grant below. I am forwarding this to you as per his out-of-office message. Would you please respond as soon as possible?

Sincerely,

Girish Panicker

From: Girish Panicker
Sent: Tuesday, August 13, 2024 9:40 AM
To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Subject: RE: EDE/DE/EBP Suspension

Dear Jeff,

Five days have now passed since your August 8, 2024 email informing me that “Inshura/TrueCoverage and Benefitalign EDE access has been suspended due to “*potential anomalous activity*” You said in that email, “CMS will follow up with additional communication to provide next steps.” In your last communication on Friday, August 09th 2024, you mentioned that you will be scheduling a call to discuss the matter, but we have heard nothing.

As you know, your unexplained decision to cut off our companies from EDE, DE, and EBP is devastating to our business, our employees, our downline agencies, and customers. In fact, it threatens to imminently put us out of business. This is an emergency for us.

What does “*potential anomalous activity*” mean?

When will you restore our access?

Do you have any concerns about our companies’ participation in EDE, DE, and EBP? If so, what are they?

Sincerely,

Girish Panicker

From: Girish Panicker
Sent: Friday, August 9, 2024 10:06 AM
To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Subject: RE: EDE/DE/EBP Suspension

Thanks Jeff. Really appreciate your quick response. Will wait for your call.

Meanwhile, I have asked the team to hold off their communication with the clients till we get some clarity and direction from CMS.

Girish

From: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Sent: Friday, August 9, 2024 9:57 AM
To: Girish Panicker <girish.panicker@speridian.com>
Subject: RE: EDE/DE/EBP Suspension

You don't often get email from jeffrey.grant1@cms.hhs.gov. [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 immediately if you suspect it's a suspicious email.

We will be setting up a call. I have to coordinate with the CMS information systems security team in a different office from CCIIO and a few others. We will reach out to you when we have found a time that we can get this on the books today.

Jeff

From: Girish Panicker <girish.panicker@speridian.com>
Sent: Thursday, August 8, 2024 8:50 PM
To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Subject: RE: EDE/DE/EBP Suspension

Jeff,

I just saw this email which is very concerning. Can you please let us know what these potential anomalies are so that we can review them? This has serious business consequences for us as well as the partners who use the platform.

If you are available, I would like to get on a quick call with you first thing in the morning OR as per your convenience to understand this better

Girish Panicker

From: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>
Sent: Thursday, August 8, 2024 6:37 PM
To: girish.panicker <girish.panicker@benefitalign.com>
Cc: Tamara White <tamara.white@speridian.com>; Sonu Rajamma <sonu.sr@benefitalign.com>
Subject: EDE/DE/EBP Suspension

You don't often get email from jeffrey.grant1@cms.hhs.gov. [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 immediately if you suspect it's a suspicious email.

This message has originated from an **External Source**. Please use proper judgment and caution before attending it. Please report it to phishing.report@benefitalign.com immediately if you suspect it's a suspicious email.

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 G

Re: CMS EDE Suspension

Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Thu 8/15/2024 10:09 AM

To: Girish Panicker <girish.panicker@speridian.com>

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 immediately if you suspect it's a suspicious email.

Girish,

A reporter reached out to CMS and asked about the disconnections. We gave a very short reply saying that we had noted anomalous activity and were currently researching. We don't normally share our press statements with other parties, and the contents are known if the reporter decides to publish anything.

As for a timetable, that would depend on the results of our current work. To provide a timetable would presume to know the results of research that is not yet complete. If we got to a point where the research said we should reconnect, we would do so in fairly short order.

Jeff

Get [Outlook for iOS](#)

From: Girish Panicker <girish.panicker@speridian.com>

Sent: Wednesday, August 14, 2024 8:36:26 PM

To: Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>

Subject: CMS EDE Suspension

Jeff,

We just received information from a reporter that, while we have been working in good faith to address your questions about our systems, CMS's press office is telling the press that there is some "anomalous activity" by two Enhanced Direct Enrollment (EDE) entities associated with Speridian Global Holdings (Speridian). The press office is also telling the media that CMS has suspended the connections between the FFM/SBM-FPs and Inshura/TrueCoverage and Benefitalign. It also stated that the suspensions will continue while the "anomalous activity" is researched. As we have previously explained, the suspension is having catastrophic consequences for our business, our clients who rely on our platform and most importantly customers. The impact is multiplying by the hour. The statement by CMS's press office obviously amplifies this impact and the harm to everyone involved. Can you please explain why CMS decided to make these disclosures to the media? Please provide me with a copy of any media disclosures, including this press office statement, about our companies.

Given this escalation, we need to have some timetable for reinstatement in place by tomorrow.

Girish

Exhibit H

RE: CMS/Speridian

Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>

Wed 8/28/2024 12:13 PM

To: Manal Mehta <manal.mehta@benefitalign.com>

Cc: Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Ashwini Deshpande <ashwini.deshpande@Truecoverage.com>; Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>; Sonu S. Rajamma <sonu.sr@speridian.com>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Tamara White <tamara.white@benefitalign.com>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Shynihan Muhammed <shynihan.muhammed@benefitalign.com>; Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>

You don't often get email from david.paradis1@cms.hhs.gov. [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 immediately if you suspect it's a suspicious email.

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 # (443)764-4514

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 <manal.mehta@benefitalign.com>

Sent: Thursday, August 22, 2024 10:25 AM

To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>

Cc: Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Ashwini Deshpande. <ashwini.deshpande@Truecoverage.com>; Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>; Sonu S. Rajamma <sonu.sr@speridian.com>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Tamara White <tamara.white@benefitalign.com>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Shynihan Muhammed <shynihan.muhammed@benefitalign.com>
Subject: Re: CMS/Speridian

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) <David.Paradis1@cms.hhs.gov>

Date: Tuesday, August 20, 2024 at 3:29 PM

To: Kalpit Dantara kalpit.dantara@Truecoverage.com , Busby Keith (CMS/OIT) Keith.Busby@cms.hhs.gov , CMS CCIIO Office of the Director CCIIOOfficeoftheDirector@cms.hhs.gov , Montz Ellen (CMS/CCIIO) Ellen.Montz@cms.hhs.gov , Grant Jeff (CMS/CCIIO) jeffrey.grant1@cms.hhs.gov , Girish Panicker girish.panicker@speridian.com , Manal Mehta manal.mehta@benefitalign.com , Ashwini Deshpande ashwini.deshpande@Truecoverage.com , Sonu S. Rajamma sonu.sr@speridian.com , Shynihan Muhammed shynihan.muhammed@benefitalign.com , tamara.white@benefitalign.com tamara.white@benefitalign.com , Nettles Leslie (CMS/OIT) Leslie.Nettles1@cms.hhs.gov , Dorsey Kevin Allen (CMS/CCIIO) Kevin.Dorsey@cms.hhs.gov , Lyles Darrin (CMS/CCIIO) Darrin.Lyles@cms.hhs.gov , Kania Michael (CMS/OIT) michael.kania@cms.hhs.gov
Cc: Hunt Patrick (CMS/OIT) Patrick.Hunt@cms.hhs.gov , Berry Dawn (CMS/OIT) Dawn.Berry@cms.hhs.gov , Paradis David (CMS/OIT) David.Paradis1@cms.hhs.gov

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 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;

1. 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.
2. Irrespective of Role, EDE is only enabled if the user is ID Proofed.
3. 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.
4. 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.
5. Inactivity timeouts are set to 5 mins by default. Users can configure it to different times but cannot exceed 30 mins.
6. 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 # (443)764 4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>

Sent: Monday, August 19, 2024 12:04 AM

To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>; Ashwini Deshpande <ashwini.deshpande@Truecoverage.com>; Sonu S. Rajamma <sonu.sr@speridian.com>; Shynihan Muhammed <shynihan.muhammed@benefitalign.com>; tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>

Cc: Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>

Subject: RE: CMS/Speridian

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 , Busby, Keith (CMS/OIT) Keith.Busby@cms.hhs.gov , CMS CCIO Office of the Director CCIOOfficeoftheDirector@cms.hhs.gov , Montz, Ellen (CMS/CCIO)

Ellen.Montz@cms.hhs.gov , Grant, Jeff (CMS/CCIO) jeffrey.grant1@cms.hhs.gov , Girish Panicker girish.panicker@speridian.com , Manal Mehta manal.mehta@benefitalign.com , Ashwini Deshpande Ashwini.deshpande@truecoverage.com , Sonu S. Rajamma sonu.sr@speridian.com , Shynihan Muhammed Shynihan.Muhammed@benefitalign.com , tamara.white@benefitalign.com tamara.white@benefitalign.com ,

Nettles, Leslie (CMS/OIT) Leslie.Nettles1@cms.hhs.gov , Dorsey, Kevin Allen (CMS/CCIO)

Kevin.Dorsey@cms.hhs.gov , Lyles, Darrin (CMS/CCIO) Darrin.Lyles@cms.hhs.gov , Kania, Michael (CMS/OIT) michael.kania@cms.hhs.gov

Cc: Hunt, Patrick (CMS/OIT) Patrick.Hunt@cms.hhs.gov , Berry, Dawn (CMS/OIT) Dawn.Berry@cms.hhs.gov ,

Kania, Michael (CMS/OIT) michael.kania@cms.hhs.gov

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 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:

Agent gets a call [Lead] and this creates a Lead record in CustomerEngage [CRM].

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.

The customer record is synced into BrokerEngage [EDE].

The agent can navigate to BrokerEngage and see the newly created Customer Record.

The agent then can create Quotes/Proposals in BrokerEngage.

If the customer wants to enroll, the EDE Flow is initiated in BrokerEngage by the agent.

When the application is completed and submitted, the BrokerEngage Customer Record Status is updated to reflect the enrolled status.

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.

Regards,

-Dave

David V. Paradis

Primary contact # (443)764 4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>

Sent: Thursday, August 15, 2024 6:22 PM

To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Girish Panicker

<girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>; Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>; Sonu S. Rajamma <sonu.sr@speridian.com>; Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>; tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>
Subject: Re: CMS/Speridian

Hi David,

We have added the requested data in the dropbox shared yesterday.

[Benefitalign Documents To CMS](#)

The file name is FSFADOM3-FGT_elog_TC-VPN.csv. Please note that the VPN logs are only retained for 3 weeks.

This log contains the employees from your list who have accessed AWS through the Forticlient VPN (54.157.134.187).

The other two VPNs have not been used by any of these employees.

The employees that are not in this log file have accessed AWS through our Albuquerque, NM office network.

Also - not all employees on your list have access to BenefitAlign BrokerEngage/Inshura EDE platforms as they work on other applications.

If you have questions, we are available to meet at your convenience.

-Kalpit

From: Kalpit Dantara kalpit.dantara@Truecoverage.com

Date: Thursday, August 15, 2024 at 1:20 PM

To: Paradis, David (CMS/OIT) David.Paradis1@cms.hhs.gov , Busby, Keith (CMS/OIT) Keith.Busby@cms.hhs.gov , CMS CCIIO Office of the Director CCIIOOfficeoftheDirector@cms.hhs.gov , Montz, Ellen (CMS/CCIIO) Ellen.Montz@cms.hhs.gov , Grant, Jeff (CMS/CCIIO) jeffrey.grant1@cms.hhs.gov , Girish Panicker girish.panicker@speridian.com , Manal Mehta manal.mehta@benefitalign.com , Ashwini Deshpande

<Ashwini.deshpande@truecoverage.com>, Sonu S. Rajamma <sonu.sr@speridian.com>, Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>, Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>
Subject: Re: CMS/Speridian

Hi David,

Let me have my team work on getting this data to you.

-Kalpit

From: Paradis, David (CMS/OIT) David.Paradis1@cms.hhs.gov
Date: Thursday, August 15, 2024 at 11:58 AM
To: Kalpit Dantara kalpit.dantara@Truecoverage.com , Busby, Keith (CMS/OIT) Keith.Busby@cms.hhs.gov , CMS CCIIO Office of the Director CCIIOOfficeoftheDirector@cms.hhs.gov , Montz, Ellen (CMS/CCIIO) Ellen.Montz@cms.hhs.gov , Grant, Jeff (CMS/CCIIO) jeffrey.grant1@cms.hhs.gov , Girish Panicker girish.panicker@speridian.com , Manal Mehta manal.mehta@benefitalign.com , Ashwini Deshpande Ashwini.deshpande@truecoverage.com , Sonu S. Rajamma sonu.sr@speridian.com , Shynihan Muhammed Shynihan.Muhammed@benefitalign.com , tamara.white@benefitalign.com tamara.white@benefitalign.com , Nettles, Leslie (CMS/OIT) Leslie.Nettles1@cms.hhs.gov , Dorsey, Kevin Allen (CMS/CCIIO) Kevin.Dorsey@cms.hhs.gov , Lyles, Darrin (CMS/CCIIO) Darrin.Lyles@cms.hhs.gov , Kania, Michael (CMS/OIT) michael.kania@cms.hhs.gov
Cc: Paradis, David (CMS/OIT) David.Paradis1@cms.hhs.gov , Hunt, Patrick (CMS/OIT) Patrick.Hunt@cms.hhs.gov , Berry, Dawn (CMS/OIT) Dawn.Berry@cms.hhs.gov
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 immediately if you suspect it's a suspicious email.

Kalpit,

Thank you for the additional information!

Could we request a copy of the last three months of logs from each of these VPN solutions that show the timestamped true source IP's connecting, translation to specific VPN IP's and what they connected to – Narrowed by the following list of users?

amit.kumar1@speridian.com

boravancha.manogna@speridian.com

girish.sasidharan@speridian.com

jerin.george@speridian.com

manish.awasthi@speridian.com

muhammad.ahmed@speridian.com

prakash.moni@speridian.com

raghavendra.kumar@speridian.com

rakesh.rathi@speridian.com

rakesh.reddy@speridian.com

rana.pratap@speridian.com

sabari.chandran@speridian.com

siva.radhakrishnan@benefitalign.com

sonu.rajamma

sreekanth.g@speridian.com

sreekumar.venukumar1@speridian.com

sumankumar.patra@speridian.com

syed.nijamuddin@speridian.com

umar.farooque@speridian.com

venu.telagathoti@speridian.com

Regards,

-Dave

David V. Paradis

Primary contact # (443)764-4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>

Sent: Thursday, August 15, 2024 10:45 AM

To: Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>; Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>; Sonu S. Rajamma <sonu.sr@speridian.com>; Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>; tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>

Subject: Re: CMS/Speridian

Hi Keith,

We have confirmed that there are 3 VPN solutions being used by the organization 2 FortiClient solutions hosted inhouse and a Palo Alto solution used as a SaaS product.

-Kalpit

From: Keith.Busby@cms.hhs.gov

When: 9:00 AM - 10:00 AM August 15, 2024

Subject: CMS/Speridian

Location: <https://cms.zoomgov.com/j/1602119654?pwd=RbZ0g15kA0lJg8mBATuh8EDbeXlnj.1>

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 immediately if you suspect it's a suspicious email.

Exhibit I

Thursday, September 5, 2024 at 13:02:50 Eastern Daylight Time

Subject: Re: CMS/Speridian
Date: Friday, August 30, 2024 at 7:52:24 PM Eastern Daylight Time
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
Attachments: image001.png

Hello David:

Please find our response to the questions you'd send on Aug 28. Files referenced are available in the Dropbox folder shared for previous queries. Link [Benefitalign Documents To CMS](#) .

Specifically, please find the following documents/folder:

[Benefitalign Response Aug 30 2024.pdf](#)

[VPC-Flow-log](#)

[Benefitalign Remote Access Acceptable Use Policy.pdf](#)

We would like to request a call with your team as soon as possible so we can provide any additional clarifications you may need and/or discuss any additional questions. Would appreciate your providing availability to meet on Tuesday.

Thanks
Manal.

From: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>
Sent: Wednesday, August 28, 2024 12:12 PM
To: Manal Mehta <manal.mehta@benefitalign.com>
Cc: Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Ashwini Deshpande. <ashwini.deshpande@Truecoverage.com>; Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>; Sonu S. Rajamma <sonu.sr@speridian.com>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Tamara White <tamara.white@benefitalign.com>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; Grant, Jeff (CMS/CCIIO)

<jeffrey.grant1@cms.hhs.gov>; CMS CCIIO Office of the Director
<CCIIOOfficeoftheDirector@cms.hhs.gov>; Shynihan Muhammed
<shynihan.muhammed@benefitalign.com>; Paradis, David (CMS/OIT)
<David.Paradis1@cms.hhs.gov>
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@benefitalign.com immediately if you suspect it's a suspicious email.

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 # (443)764-4514

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 <manal.mehta@benefitalign.com>
Sent: Thursday, August 22, 2024 10:25 AM
To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>
Cc: Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Ashwini Deshpande. <ashwini.deshpande@Truecoverage.com>; Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Busby, Keith (CMS/OIT)

<Keith.Busby@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>; Sonu S. Rajamma <sonu.sr@speridian.com>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Tamara White <tamara.white@benefitalign.com>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Shynihan Muhammed <shynihan.muhammed@benefitalign.com>
Subject: Re: CMS/Speridian

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) <David.Paradis1@cms.hhs.gov>
Date: Tuesday, August 20, 2024 at 3:29 PM
To: Kalpit Dantara <kalpit.dantara@Truecoverage.com>, Busby Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>, CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>, Montz Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>, Grant Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>, Girish Panicker <girish.panicker@speridian.com>, Manal Mehta <manal.mehta@benefitalign.com>, Ashwini Deshpande <ashwini.deshpande@Truecoverage.com>, Sonu S. Rajamma <sonu.sr@speridian.com>, Shynihan Muhammed <shynihan.muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Hunt Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>, Paradis David (CMS/OIT) <David.Paradis1@cms.hhs.gov>
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 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;

1. 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.
2. Irrespective of Role, EDE is only enabled if the user is ID Proofed.
3. 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.
4. 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.
5. Inactivity timeouts are set to 5 mins by default. Users can configure it to different times but cannot exceed 30 mins.
6. 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 # (443)764-4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>
Sent: Monday, August 19, 2024 12:04 AM
To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>; Ashwini Deshpande <ashwini.deshpande@Truecoverage.com>; Sonu S. Rajamma <sonu.sr@speridian.com>; Shynihan Muhammed <shynihan.muhammed@benefitalign.com>; tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>
Subject: RE: CMS/Speridian

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>, Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>, CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>, Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>, Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>, Girish Panicker <girish.panicker@speridian.com>, Manal Mehta <manal.mehta@benefitalign.com>, Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>, Sonu S. Rajamma <sonu.sr@speridian.com>, Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Cc: Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
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 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:

Agent gets a call [Lead] and this creates a Lead record in CustomerEngage [CRM].

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.

The customer record is synced into BrokerEngage [EDE].

The agent can navigate to BrokerEngage and see the newly created Customer Record.

The agent then can create Quotes/Proposals in BrokerEngage.

If the customer wants to enroll, the EDE Flow is initiated in BrokerEngage by the agent.

When the application is completed and submitted, the BrokerEngage Customer Record Status is updated to reflect the enrolled status.

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.

Regards,

-Dave

David V. Paradis

Primary contact # (443)764-4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>

Sent: Thursday, August 15, 2024 6:22 PM

To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Busby, Keith (CMS/OIT)

<Keith.Busby@cms.hhs.gov>; CMS CCIIO Office of the Director

<CCIIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIIO)

<Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>; Girish

Panicker <girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>;

Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>; Sonu S. Rajamma

<sonu.sr@speridian.com>; Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>;

tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>;

Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIIO)

<Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>

Cc: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Hunt, Patrick (CMS/OIT)

<Patrick.Hunt@cms.hhs.gov>; Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>

Subject: Re: CMS/Speridian

Hi David,

We have added the requested data in the dropbox shared yesterday.

[Benefitalign Documents To CMS](#)

The file name is FSFADOM3-FGT_elog_TC-VPN.csv. Please note that the VPN logs are only retained for 3 weeks.

This log contains the employees from your list who have accessed AWS through the Forticlient VPN (54.157.134.187).

The other two VPNs have not been used by any of these employees.

The employees that are not in this log file have accessed AWS through our Albuquerque, NM office network.

Also - not all employees on your list have access to BenefitAlign BrokerEngage/Inshura EDE platforms as they work on other applications.

If you have questions, we are available to meet at your convenience.

-Kalpit

From: Kalpit Dantara <kalpit.dantara@Truecoverage.com>

Date: Thursday, August 15, 2024 at 1:20 PM

To: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>, Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>, CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>, Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>, Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>, Girish Panicker <girish.panicker@speridian.com>, Manal Mehta <manal.mehta@benefitalign.com>, Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>, Sonu S. Rajamma <sonu.sr@speridian.com>, Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>

Cc: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>, Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>

Subject: Re: CMS/Speridian

Hi David,

Let me have my team work on getting this data to you.

-Kalpit

From: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>

Date: Thursday, August 15, 2024 at 11:58 AM

To: Kalpit Dantara <kalpit.dantara@Truecoverage.com>, Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>, CMS CCIIO Office of the Director <CCIIOOfficeoftheDirector@cms.hhs.gov>, Montz, Ellen (CMS/CCIIO) <Ellen.Montz@cms.hhs.gov>, Grant, Jeff (CMS/CCIIO) <jeffrey.grant1@cms.hhs.gov>, Girish Panicker <girish.panicker@speridian.com>, Manal Mehta <manal.mehta@benefitalign.com>, Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>, Sonu S. Rajamma

<sonu.sr@speridian.com>, Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>, tamara.white@benefitalign.com <tamara.white@benefitalign.com>, Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>, Dorsey, Kevin Allen (CMS/CCIIO) <Kevin.Dorsey@cms.hhs.gov>, Lyles, Darrin (CMS/CCIIO) <Darrin.Lyles@cms.hhs.gov>, Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>

Cc: Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>, Hunt, Patrick (CMS/OIT) <Patrick.Hunt@cms.hhs.gov>, Berry, Dawn (CMS/OIT) <Dawn.Berry@cms.hhs.gov>

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 immediately if you suspect it's a suspicious email.

Kalpit,

Thank you for the additional information!

Could we request a copy of the last three months of logs from each of these VPN solutions that show the datestamped true source IP's connecting, translation to specific VPN IP's and what they connected to – Narrowed by the following list of users?

amit.kumar1@speridian.com
boravancha.manogna@speridian.com
girish.sasidharan@speridian.com
jerin.george@speridian.com
manish.awasthi@speridian.com
muhammad.ahmed@speridian.com
prakash.moni@speridian.com
raghavendra.kumar@speridian.com
rakesh.rathi@speridian.com
rakesh.reddy@speridian.com
rana.pratap@speridian.com
sabari.chandran@speridian.com
siva.radhakrishnan@benefitalign.com
sonu.rajamma
sreekanth.g@speridian.com
sreekumar.venukumar1@speridian.com
sumankumar.patra@speridian.com
syed.nijamuddin@speridian.com
umar.farooque@speridian.com
venu.telagathoti@speridian.com

Regards,

-Dave

David V. Paradis

Primary contact # (443)764-4514

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: Kalpit Dantara <kalpit.dantara@Truecoverage.com>
Sent: Thursday, August 15, 2024 10:45 AM
To: Busby, Keith (CMS/OIT) <Keith.Busby@cms.hhs.gov>; Kalpit Dantara <kalpit.dantara@Truecoverage.com>; CMS CCIO Office of the Director <CCIOOfficeoftheDirector@cms.hhs.gov>; Montz, Ellen (CMS/CCIO) <Ellen.Montz@cms.hhs.gov>; Grant, Jeff (CMS/CCIO) <jeffrey.grant1@cms.hhs.gov>; Girish Panicker <girish.panicker@speridian.com>; Manal Mehta <manal.mehta@benefitalign.com>; Ashwini Deshpande <Ashwini.deshpande@truecoverage.com>; Sonu S. Rajamma <sonu.sr@speridian.com>; Shynihan Muhammed <Shynihan.Muhammed@benefitalign.com>; tamara.white@benefitalign.com; Nettles, Leslie (CMS/OIT) <Leslie.Nettles1@cms.hhs.gov>; Paradis, David (CMS/OIT) <David.Paradis1@cms.hhs.gov>; Dorsey, Kevin Allen (CMS/CCIO) <Kevin.Dorsey@cms.hhs.gov>; Lyles, Darrin (CMS/CCIO) <Darrin.Lyles@cms.hhs.gov>; Kania, Michael (CMS/OIT) <michael.kania@cms.hhs.gov>
Subject: Re: CMS/Speridian

Hi Keith,

We have confirmed that there are 3 VPN solutions being used by the organization – 2 FortiClient solutions hosted inhouse and a Palo Alto solution used as a SaaS product.

-Kalpit

From: Keith.Busby@cms.hhs.gov
When: 9:00 AM - 10:00 AM August 15, 2024
Subject: CMS/Speridian
Location: <https://cms.zoomgov.com/j/1602119654?pwd=RbZ0g15kA0lJG8mBATuh8EDbeXInj.1>

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 immediately if you suspect it's a suspicious email.

UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

BENEFITALIGN, LLC; AND
TRUECOVERAGE, LLC,

Plaintiffs,

v.

CENTERS FOR MEDICARE AND
MEDICAID SERVICES;

XAVIER BECERRA, in his official capacity
as Secretary of Health and Human Services;

THE U.S. DEPARTMENT OF HEALTH
AND HUMAN SERVICES;

CHIQUITA BROOKS-LASURE, in her
official capacity as Administrator of the
Centers for Medicare & Medicaid Services;

Defendants.

Case No.: 1:24-cv-02494-JEB

**CERTIFICATE OF COUNSEL IN SUPPORT OF AMENDED MOTION
FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY
INJUNCTION AND REQUEST FOR EXPEDITED HEARING**

Pursuant to LCvR 65.1(a) of the Rules of the United States District Court for the District of Columbia, I, Amy E. Richardson, hereby certify that I have provided actual notice of this Amended Motion for Temporary Restraining Order and Preliminary Injunction and Request for Expedited Hearing (“Motion”) to Defendants, and served the same on Defendants, via filing this document via the Court’s Case Management/Electronic Case Filing system. *See* LCvR 5.4(d). Defendants have, through CM/ECF, been provided copies of all pleadings and papers filed in the action to date.

Dated: September 6, 2024

Respectfully submitted,

/s/ Amy E. Richardson

Amy E. Richardson, Esq. (DC Bar # 472284)

Patrick P. O'Donnell (DC Bar # 459360)

Walter E. Anderson, Esq. (DC Bar # 975456)

HWG LLP

1919 M Street NW, 8th Floor

Washington, DC 20036

Tel.: 202-730-1329

Email: arichardson@hwglaw.com

*Counsel for Plaintiffs Benefitalign, LLC and
TrueCoverage, LLC*

UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

BENEFITALIGN, LLC; AND
TRUECOVERAGE, LLC,

Plaintiffs,

v.

Case No.: 1:24-cv-02494-JEB

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

Defendants.

**[PROPOSED] ORDER GRANTING PLAINTIFFS' MOTION FOR TEMPORARY
RESTRAINING ORDER AND PRELIMINARY INJUNCTION AND REQUEST FOR
EXPEDITED HEARING**

This matter is before the Court on the motion of Plaintiffs Benefitalign, LLC and TrueCoverage, LLC (d/b/a Inshura) to temporarily enjoin the Centers for Medicare and Medicaid Services ("CMS") from suspending Plaintiffs' access to CMS' Data Services Hub ("CMS Network").

Upon due consideration of the Complaint and Motion for Temporary Restraining Order and Preliminary Injunction and Request for Expedited Hearing, the Court finds that Plaintiffs are likely to succeed on the merits, that immediate and irreparable injury, loss, and damage will result to Plaintiffs if the motion is not granted, and that the balance of equities favors enjoining the CMS's suspension.

Therefore, for these reasons, and for good cause shown, it is hereby

ORDERED that Plaintiffs' Motion for Temporary Restraining Order and Preliminary Injunction and Request for Expedited Hearing is GRANTED; and it is further

ORDERED that Defendants are enjoined from enforcing their suspension of Plaintiffs from CMS' Data Services Hub, and must restore Plaintiffs' access to such systems immediately;

and it is further

ORDERED that Defendants are enjoined from preventing Plaintiffs from participation in ACA marketplaces; and it is further

ORDERED, in accordance with Fed. R. Civ. P. 65(b)(2), that this temporary restraining order shall expire fourteen days after its entry upon the docket, unless extended for good cause shown.

Dated: September __, 2024

JAMES E. BOASBERG
United States District Judge