UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA *ex rel.* ANDREW SHEA, Plaintiff, v. eHEALTH, INC., *et al.*, Defendants.	No. 21-cv-11777-DJC

THE UNITED STATES' OPPOSITION TO DEFENDANTS' CROSS-MOTION FOR PROTECTIVE AND CONFIDENTIALITY ORDER

The United States opposes Defendants' Cross-Motion for the same reasons articulated in the Government's own Motion on this topic. Dkt. No. 196 ("Gov't Motion"). First, cases generally cannot be litigated in secret, and blanket confidentiality provisions run counter to that principle. Second, parties cannot wait years to claim privilege and then claw back previously produced documents. Third and finally, this case does not warrant imposition of a novel and untested data breach provision that offers no additional information security. Rather than address the United States' Motion, Defendants instead filed within two hours a cross-motion and memorandum. Dkt. Nos. 197 and 198 (together, "Cross-Motion"). Leaving aside its other deficiencies, the Cross-Motion misrepresents the Government's position on key provisions. Specifically, during the meet-and-confer process, the Government proposed compromises on certain provisions only in tandem with *specific other provisions* that guaranteed appropriate public access. *E.g.*, Gov't Motion at 7 n.3. Defendants now wrongly assert that the Government agreed to individual parts of those balanced compromises as stand-alone positions.

ARGUMENT

The Government provides this Opposition to correct Defendants' mischaracterizations of the Government's positions and to clarify the points in dispute. The Government's Proposed Order includes provisions for "Confidential" and "Highly Confidential" material, but with appropriate weight given to public access. *See* Dkt. No. 196-1 ("Gov't Prop. Order") at 1–3, 10–11. The Government remains concerned with the interplay of Defendants' confidentiality definitions and their blanket sealing proposal. *See* Gov't Motion at 3–6. Next, the Government's Proposed Order would allow for re-designation and, as appropriate, "Confidential" or "Highly Confidential" treatment for material produced during the Government's investigation, including under all confidentiality-related provisions throughout the protective order. Gov't Prop. Order at 1–3; *see* Gov't Motion at 6–7. The Government does not agree, however, that: (a) Defendants' seemingly indiscriminate confidentiality designations during the Government's investigation should carry over without further review; or that (b) any party or third party should have a retroactive clawback provision, supplanting Federal Rule of Evidence 502, for material produced years ago during the Government's investigation. Gov't Motion at 7–8. Finally, the Government opposes Defendants' data breach provision for reasons beyond novelty, including lack of any demonstrated benefit to information security and the possible harm to the Government's investigation and remediation of a cyber incident.

I. The Government Has Proposed Tailored Confidentiality Provisions That Balance Privacy and Commercial Interests with Public Access to Judicial Filings

Contrary to Defendants' assertion in the Cross-Motion, the Government's Proposed Order includes various confidentiality provisions. These cover, among other things, personal health information, employee personnel files, trade secrets, and certain other confidential business or operational information discussed below. Gov't Prop. Order at 1–3.

Government's Proposed Order	**Defendants' Proposed Order**
2.b. "Confidential Business or Operational Information." For purposes of this Order, "Confidential Business or Operational Information" shall mean a Party's confidential commercial or operational information that is less than five years old and that bears upon a Party's or third party's competitive position or sensitive operations, and that does not fall within the definition of "Commercially Sensitive Information" as defined in Paragraph 3 *infra*	2.b. commercial or operational information that bears upon a Party's or a third party's competitive position or sensitive operations; . . . . 2.f. Trade secret or other confidential research, development, or commercial information.
3. "Highly Confidential" information, which shall be designated "Highly Confidential – Attorneys' Eyes Only" means: (a) information related to the Medicare Advantage bid process; or (b) "Commercially Sensitive Information," meaning any document or information that the producing party in good faith believes: to contain current or future bidding or contracting strategy; to be a trade secret as defined by federal law; to disclose current or future confidential research or development information; or to disclose current or future confidential pricing terms or negotiation. Moreover, to qualify as Commercially Sensitive Information, it must bear upon a producing party's current or future competitive position.	3. "Highly Confidential" information, which shall be designated "Highly Confidential – Attorneys' Eyes Only," means trade secrets or other commercial or operational information, including information related to the Medicare Advantage bid process, that any producing party, including any third party, in good faith believes to be extremely confidential and/or extremely sensitive in nature.

The Government does not seek a one-sided order favoring its material over any Defendant's material. In fact, the Government's definition of "Commercially Sensitive Information" would likely apply more frequently to for-profit entities like Defendants than to the Government. The Government's proposal is also consistent with Rule 26(c)(1)(G). None of the cases cited by defendants, *see* Dkt. No. 198 at 4 n.3, support their contention that communications such as those quoted in the Government's Complaint or the Court's order constitute confidential commercial information. For example, emails directing a broker not to market to disabled beneficiaries or confirming how many beneficiaries have been referred hardly constitute trade secrets or forward-looking "market analyses and strategies" allegedly requiring confidentiality. *Id.* at 5.

The Government's proposal also addresses Defendants' concern that, notwithstanding their joint defense in this litigation, "a producing Defendant faces the risk that confidential information would be . . . shared with its competitor and thereafter used to secure a competitive advantage." *Id.* The Government's Proposed Order provides *greater* protection than Defendants' Proposed Order for (a) bona fide trade secrets and (b) "current or future confidential research or development information" that bears upon a "current or future competitive position." Gov't Prop. Order at 3 (including each as "Highly Confidential"). It simply defines these categories at an appropriate level of specificity, including considering the age of material. *See* Gov't Motion at 7–8.

Defendants' description of "other confidential . . . commercial information" and wholesale confidentiality designation of all internal company communications demonstrate the overbreadth of Defendants' proposals. As explained in the Government's Motion, when reviewing Defendants' productions during the Government's investigation,

> the Government has seen numerous public documents stamped for production as "Confidential," "Confidential Business Information," or similar within Defendants' productions to the Government during the investigation. These include dozens of copies of the Government's own agency regulations which, despite markings by Defendants' counsel, are emphatically not the "Confidential Business Information" of any Defendant.

Id. Such overbroad designations risk significant inefficiencies in litigation. For example, they risk repeated court intervention, on a document-by-document level, across numerous parties and rolling productions throughout fact discovery. And as explained further below, the potential harm of overbroad confidentiality provisions stretches beyond taxing judicial resources to ultimately affecting the public's right to access judicial records.

II. Defendants' Sealing Proposal Would Require Multi-Week or Longer Delays in Public Access to Judicial Records

Defendants seek a blanket sealing order allowing any producing party to force any other party to file judicial records under seal for at least fourteen days and likely much longer. That approach violates both Local Rule 7.2 and the presumption of public access to judicial records. The Government has explained its concern with Defendants' sealing proposal in detail, Gov't Motion at 3–6, including explaining how the Government's notification proposal is consistent with numerous intervened FCA cases in this District, *id.* at 6 (citing Wyeth Protective Order at 6; Regeneron ASP Protective Order at 11; Regeneron Co-Pay Protective Order at 8; and SATP Protective Order at 8). Defendants never discuss the presumption of openness that governs court filings and how this would be affected by their proposed confidentiality and sealing provisions. *E.g.*, *United States v. Kravetz*, 706 F.3d 47, 59 (1st Cir. 2013). Far from "conflat[ing] two distinct issues," Dkt. No. 198 at 16, the scope of "Confidential" material and the required filing and sealing procedure for that same "Confidential" material necessarily intersect.

Government Proposed Order	**Defendants' Proposed Order**
11. A Party seeking to file another party's Confidential or Highly Confidential information shall provide the producing party notice of the Confidential or Highly Confidential information it intends to use at least three (3) business days prior to filing. The producing party shall then have three (3) business days in which either to consent to the request to file said information in the public record or to file a motion pursuant to Local Rule 7.2 to keep such papers under seal. If the producing party moves to keep papers under seal, the papers with the designated Confidential or Highly Confidential information under seal, or with any references to the Confidential or Highly Confidential information, will be filed under seal or redacted, as appropriate, until the Court rules on the motion to seal.	11. A Party seeking to file another party's Confidential or Highly Confidential information may provide the producing party notice of the Confidential or Highly Confidential information that it intends to use no later than the day of filing. Unless the producing party consents to a request to file said information in the public record, the filing party shall file the information provisionally under seal in compliance with Local Rule 7.2. The producing party shall have fourteen (14) days from the day of filing in which to file a motion pursuant to Local Rule 7.2 to keep such papers under seal. If the producing party does not file such a motion within this period, the papers shall be unsealed. If the producing party moves to keep papers under seal, the papers with the designated Confidential or Highly Confidential information, or with any references to the Confidential or Highly Confidential information, will remain under seal until the Court rules on the motion to seal. Notwithstanding the foregoing, nothing in this paragraph prevents a Party from obtaining the written consent of the producing party in advance of filing to file its Confidential or Highly Confidential information in the public record.

The Government's approach strikes a balance between respect for a party's truly confidential information and the right of public access. It requires a party disputing public filing to substantiate the need for secrecy before that filing and does not allow presumptive sealing. Under Defendants' approach, so long as a producing party objects, any of its purportedly "Confidential" material must remain under seal for at least fourteen days, plus additional time for briefing and the Court's decision. *But see Globe Newspaper Co. v. Pokaski*, 868 F.2d 497, 507 (1st Cir. 1989) (explaining that "even a one to two day delay" to otherwise appropriate public access "impermissibly burdens the First Amendment"). That, eventually, a "producing party must justify the seal under Local Rule 7.2," Dkt. No. 198 at 16, does not provide a sufficient safeguard because Defendants' approach would still allow even the most baseless "Confidentiality" assertions to seal judicial records for at least two weeks and likely much longer in practice.

Further, Defendants seek a "blanket order[]" that would violate Local Rule 7.2(d). Their response appears to be that their presumptive sealing request would not constitute a blanket order because it would not allow such sealing "in perpetuity." Dkt. No. 198 at 15. That concept is absent from sub-part (d) of the Local Rule, which instead provides that "[a] motion for impoundment must be presented each time a document or group of documents is to be filed" for sealing. L.R. 7.2(d). Moreover, under the blanket sealing order sought by Defendants, large swaths of the Government's Complaint and the Court's own order on motion to dismiss would have remained under seal for weeks, absent prior consent of every producing party. *See* Gov't Motion at 4. Unsupported, weeks-long sealing of evidence underlying the Government's claims and of material relied upon in the Court's substantive decisions cannot be squared with the presumption of public access to judicial records. *See Siedle v. Putnam Invs., Inc.*, 147 F.3d 7, 9–10 (1st Cir. 1998); Gov't Motion at 3–5. Defendants may well prefer to avoid public scrutiny for their conduct, such as profit-seeking discrimination against Americans with disabilities (e.g., setting up meetings "so they can work with us on the issue of minimizing enrolling disabled folks," Dkt. No. 41 ¶ 551). But whether this preference stems from "commercial embarrassment" or fear of market-based repercussions, it is no basis to seal the record. *Poliquin v. Garden Way, Inc.*, 989 F.2d 527, 533 (1st Cir. 1993).

III. Material Produced During the Government's Investigation Should Be Evaluated on a Document-Specific Basis

A. Confidentiality Designations for Previously Produced Material

Defendants misstate the Government's position for previously produced material as expressed in the Government's Motion, instead borrowing snippets from conferral discussions that were premised on separate draft sections. To be clear, the Government has not agreed to "preserve previously applied confidentiality labels on Previously Produced Documents while excluding those materials from the remaining provisions of the Protective Order." Dkt. No. 198 at 9–10. Instead, the Government's Proposed Order would provide Defendants an extended period to review material previously produced during the Government's investigation and designate for confidentiality (or high confidentiality) as the terms are defined in a protective order. Gov't Prop. Order at 4. During that review period, the Government expressly would agree to "continue to handle such documents under the terms of the form of process under which they were obtained." *Id.*; *see, e.g.*, 31 U.S.C. § 3733(i)(2) (handling for material produced under a Civil Investigative Demand). And if a Defendant designates a previously produced document as "Confidential" or "Highly Confidential," the Proposed Order's other processes for "Confidential" and "Highly Confidential" material would apply to that material. *See* Gov't Prop. Order at 3–11.

Government's Proposed Order	**Defendants' Proposed Order**
4.c. . . . Defendants will have 120 days from the date of this Order, and third parties will have 30 days from the receipt of a subpoena or notice by the United States that it intends to produce the third party's documents, to affirmatively designate any such document as Confidential or Highly Confidential by providing a crosswalk for such documents, and a Party may, at any time, challenge the confidentiality designation of any such documents by identifying the specific document(s). The producing party shall respond to the challenge within a reasonable amount of time by (1) affirmatively designating challenged documents as Confidential or Highly Confidential or (2) agreeing that the documents should not be considered Confidential or Highly Confidential under the terms of this Order. If documents are required to be produced before the deadline for designation set forth above, (1) Defendants agree to treat documents that are marked as confidential as Confidential until such status is resolved with the producing party; and (2) the United States agrees to continue to handle such documents under the terms of the form of process under which they were obtained. Any party may subsequently challenge the producing party's designation in accordance with Paragraph 5 of this Order.	4.c . . . Information to be treated as Confidential under this Order includes all Previously Produced Documents labeled as "protected," "confidential," "proprietary," or a similar designation. Any Party may challenge the confidentiality designation of any such documents in accordance with Paragraph 5 of this Order.

The Government's Proposed Order also does not require separate tracks "for purposes of the Proposed Protective Order's confidentiality protections" or otherwise create administrability issues for the Court. Dkt. No. 198 at 9. It lays out a single process, following this extended opportunity for any producing party to assess confidentiality of its material. The Government does not, of course, take the strawman positions that a document necessarily "become[s] less confidential because it was produced in response to a CID or subpoena rather than a Rule 34 request" or that Defendants are "entitled to less protection" after the United States files suit. Dkt. No. 198 at 9–10.

Next, Defendants gesture at a concern with the termination provision and HIPAA compliance for material produced during the Government's investigation. *Id.* at 10. That concern is misplaced. HIPAA regulations include exceptions permitting disclosure of protected health information to Government officials acting, among other things, in a "health oversight" capacity. 45 C.F.R. § 164.512(d). During the FCA investigation underlying this action, the Department of Justice was acting in its "health oversight" capacity. Thus, a termination provision that does not apply to materials produced during a Government "health oversight"-related investigation does not create any issue under HIPAA. In addition, the False Claims Act has its own distinct return provisions for material produced pursuant to civil investigative demands under 31 U.S.C. § 3733(i)(4).

B. Clawback or Inadvertent Production Provisions

The Government's Proposed Order allows for no-fault clawback for material produced in litigation where a party has "a good faith claim of any privilege or protection (including the attorney-client privilege, work product protection, and governmental privileges such as deliberative process, investigatory files, and official privileges)." Gov't Prop. Order at 11–12. This simple proposal applies evenly to every party's productions in litigation, and so is hardly "fundamentally unfair," Dkt. No. 198 at 12. The Government included this clawback provision to make litigation productions more efficient and to require less Court intervention.

Defendants' argument in their Cross-Motion is at odds with the actual language of their proposal. Defendants complain that the Government has conflated "the *procedural right* to *retrieve* a produced document" and "whether *the privilege itself has been forfeited*," Dkt. No. 198 at 12 (emphasis in original). Defendants' Proposed Order, however, would exempt documents produced during the Government's investigation from Federal Rule of Evidence 502, which requires that a disclosure be inadvertent, that the holder took reasonable steps to prevent disclosure, and the holder *promptly* took reasonable steps to rectify the error. Fed R. Evid. 502(b).[1] Thus, Defendants' proposal addresses both the procedural and substantive issues by allowing that production more than four years ago "shall in no way . . . constitute a waiver" of privilege under Rule 502. *Id.*

Defendants' one-sided approach would invite inefficiencies, delays, and gamesmanship. A defendant in this litigation could, for example, repeatedly and belatedly claim privilege for material produced to the Government in 2022, forcing the Government to expend resources in evaluating how and whether it used any of the material produced four or more years ago. And several Defendants did not even provide a privilege log during the Government's investigation, leaving the Government only to guess at potential clawbacks years later. Finally, Defendants' retrospective approach is out of step with case law in the circuit and would not favor justice. *See, e.g.*, *United States ex rel. Omni Healthcare, Inc. v. MD Spine Sols. LLC*, 736 F. Supp. 3d 75, 86 (D. Mass. 2024) (finding that "the overriding interests of fairness and justice weigh in favor of waiver even though such a finding may disadvantage the defendants").

IV. Defendants' Novel Data Breach Provision Risks Harming Information Security and Would Infringe Upon the Executive Branch's Prosecutorial Function

The Government expects that all parties will fulfill their legal obligations as to protected health or personal information and minimize the risk of any data breaches or unauthorized

[1] Contrary to Defendants' assertion that the Government "points to no law or authority to support its position" about length of time for waiver, Dkt. No. 198 at 12, the Government's Motion provided four cases in the District. Gov't Motion at 8 (citing *United States ex rel. Omni Healthcare, Inc. v. MD Spine Sols. LLC*, 736 F. Supp. 3d 75, 84 (D. Mass. 2024); *Kaiser v. Kirchick*, No. 21- cv-10590-MBB, 2022 WL 182375, at *8 (D. Mass. Jan. 20, 2022); *Santullo v. Woburn*, No. 07-11478-RWZ, 2008 WL 2778819, at *1 (D. Mass. July 14, 2008); and *In re: New England Compounding Pharm., Inc.*, No. 13-2419-RWZ, 2016 WL 6883215, at *4 (D. Mass. July 28, 2016). By contrast, Defendants do not cite or refer to a single case, statute, or regulation in this section of their Cross-Motion.

disclosures.[2] Defendants' proposal, however, would not enhance information security and, in fact, would risk the opposite. As the Government's Motion explained, "requiring disclosure under vague circumstances, and regardless of how such a disclosure might harm remedial efforts and law enforcement investigations, would not improve information security." Gov't Motion at 2 n.2. Cybersecurity investigations by the Department of Justice and its Government partners may necessitate secrecy and careful consideration of investigative steps, not Court-ordered notification within three days of any "potential" access to a wide swath of commercial information. It is hardly "entirely hypothetical," Dkt. No. 198 at 8, that near-immediate notification outside the Government of "potential" unauthorized access could, for example, ultimately tip off wrongdoers or otherwise damage the Government's investigative or prosecutorial efforts. Defendants offer nothing to rebut the commonsense conclusion that there often is a need for secrecy during law enforcement investigations.

Finally, Defendants cannot point to a single example of an analogous data breach provision in any case in this District where the Government is a party. Their only cited example, in the Southern District of New York, is not a sweeping provision requiring notification about any "potential" unauthorized use or access to all business information labeled as "Confidential" or "Highly Confidential" by any party. It is instead a narrow provision focusing exclusively on the actual data breach of personally identifiable information: "In the event the person who received

[2] For example, Anthem (now known as Elevance Health) has experienced massive breaches of Americans' protected health information. These include "the largest U.S. health data breach in history [that] exposed the electronic protected health information of almost 79 million people" after Anthem had "failed to conduct an enterprise-wide risk analysis, . . . failed to identify and respond to suspected or known security incidents, and failed to implement adequate minimum access controls." HHS OCR, Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History (Oct. 15, 2018), *available at* https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html.

PII experiences a data breach, it shall immediately notify the producing party of same and cooperate with the producing party to address and remedy the breach." *United States v. Anthem, Inc.*, No. 1:20-cv-2593 (S.D.N.Y. Mar. 26, 2020) (Dkt. No. 485 ¶ 18).

CONCLUSION

The Court should enter the Government's Proposed Order, Dkt. No. 196-1, which is consistent with protective orders repeatedly entered in intervened FCA litigation in the District and reflects an appropriate balance between confidentiality and public access, and deny Defendants' Cross-Motion.

Respectfully submitted,

BRETT A. SHUMATE
Assistant Attorney General
Civil Division

/s/ David G. Miller
Jamie Ann Yavelberg
Edward C. Crooke
David G. Miller
Anna H. Jugo
Diana E. Curtis
Laurie A. Oberembt
Paden Gallagher
Attorneys, Civil Division
U.S. Department of Justice
175 N Street N.E.
Washington, D.C. 20002
(202) 305-2335
David.G.Miller@usdoj.gov
Anna.H.Jugo@usdoj.gov
Diana.E.Curtis@usdoj.gov
Paden.Gallagher@usdoj.gov
Laurie.Oberembt@usdoj.gov

LEAH B. FOLEY
United States Attorney

/s/ Charles B. Weinograd
Abraham R. George
Charles B. Weinograd
Julien M. Mundele
Hillary H. Harnett
Assistant United States Attorneys
1 Courthouse Way, Suite 9200
Boston, MA 02210
(617) 748-3100
Abraham.George@usdoj.gov
Charles.Weinograd@usdoj.gov
Julien.Mundele@usdoj.gov
Hillary.Harnett@usdoj.gov

Dated: August 12, 2026

Attorneys for the United States