

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

**IN RE: CHANGE HEALTHCARE, INC.
CUSTOMER DATA SECURITY BREACH
LITIGATION**

This Document Relates to All Actions

MDL No. 24-3108 (DWF/DJF)

**PRETRIAL ORDER NO. 37
PROTECTIVE ORDER RE: IMPACTED
DATA FILES**

For good cause shown, and for the reasons set forth below, the Court APPROVES the Parties' *Stipulation for Protective Order Re: Impacted Data Files* (ECF No. 702).

WHEREAS, the Court previously entered a Protective Order and Qualified HIPAA Protective Order (ECF No. 271) in this action;

WHEREAS, the Court ordered MDL Defendants to produce information stolen during the cyberattack that began on or about February 12, 2024 (the "Impacted Data Files").

WHEREAS, the Parties agree that the production by MDL Defendants of the Impacted Data Files, which include certain Personally Identifying Information and/or Protected Health Information ("Personal Information"), requires heightened security precautions.

WHEREAS, MDL Defendants¹ and Plaintiffs (together, the "Parties") request that the Court enter this Stipulated Protective Order re: Impacted Data Files (the "Order"); and

WHEREAS, Plaintiffs have retained a cyber security and forensics expert, who has opined that the processes and controls specified in this proposed Order are sufficient to keep the Impacted

¹ For the purposes of this Order, the term "MDL Defendants" means UnitedHealth Group Incorporated; United HealthCare Services, Inc.; Optum, Inc., OptumInsight, Inc.; Optum Financial, Inc.; Optum Bank, Inc.; Change Healthcare Inc.; Change Healthcare Operations, LLC; Change Healthcare Solutions, LLC; Change Healthcare Holdings, Inc.; Change Healthcare Technologies, LLC; and Change Healthcare Pharmacy Solutions, Inc.

Data Files safe and protected. Plaintiffs' expert also confirmed that he can host and analyze these the Impacted Data Files pursuant to the terms of this proposed Order.

THEREFORE, pursuant to the Parties' joint stipulation and for good cause shown,

IT IS HEREBY ORDERED that:

1. The Impacted Data Files shall be treated as Designated Discovery Material pursuant to the terms of the Protective Order and Qualified HIPAA Protective Order (ECF No. 271) ("PTO 10") entered into in this litigation, except that the security provisions below will govern in case of a conflict.

2. MDL Defendants shall produce not more than a single copy of the Impacted Data Files either to Plaintiffs, or an expert designated in writing by Plaintiffs, either on an encrypted Federal Information Processing Standards ("FIPS") 140-2 or 140-3 compliant external hard drive.

3. The Impacted Data Files will be referred to as CHCMDL_DATA_0001 Bates Number in all future briefings in this action.

4. Plaintiffs or Plaintiffs' expert will encrypt the Impacted Data Files using the Advanced Encryption Standard ("AES") 256 algorithm or an equivalent industry-standard encryption method.

5. After MDL Defendants transfer the Impacted Data Files to Plaintiffs, Plaintiffs' or Plaintiffs' expert's hard drive(s) containing the Impacted Data Files will not be connected to the Internet, and the hard drive(s) will be connected only to computers that are "air-gapped" while connected to the hard drive(s). While air-gapped, the computers will be physically isolated from any connection to the Internet, any and all networks and/or systems, and other computers. To the extent computers are connected to the Internet when not connected to the hard drives, connection to the Internet will only be made to the extent necessary to complete analysis related to the

Impacted Data Files or to install, update, license, or maintain software that is reasonably necessary to complete analysis related to the Impacted Data Files, and the Impacted Data Files, including any portion(s) or excerpt(s) of the Impacted Data Files, shall not be accessible during any such connection. Any computing environment that connects to the Impacted Data Files may contain only the software that comes loaded on the computer at the time of purchase or that is reasonably necessary for working with the Impacted Data Files. Such computing devices must be newly provisioned systems relating to the operating system. The computing environment must be hardened and fully patched before any hard drive containing the Impacted Data Files is connected to the computing environment for the first time and on an ongoing basis in a timely manner against all vulnerabilities according to hardware and software manufacturer guidelines, including, but not limited to, the operating system and any installed software, hardware, or firmware updates. Any and all wireless cards/capability will be disabled on computers to which the hard drives may be connected. Any and all Bluetooth capability will be disabled on computers to which the hard drives may be connected. No mobile phones or similar mobile devices will be connected to the computers to which the hard drives may be connected. No network cables will be attached to the computers while air-gapped. No other USB thumb drives, hard drives, or other external storage devices will be attached to the air-gapped computers while a hard drive containing the Impacted Data Files is connected.

6. MDL Defendants may seek additional or modified restrictions on the Impacted Data Files at any time upon a showing of good cause, including but not limited to changes in applicable law, regulatory guidance, or threat landscape. Plaintiffs agree not to oppose any motion seeking such additional restrictions solely on the basis that the restrictions were not included in this Order at the time of its entry.

7. MDL Defendants will secure the Impacted Data Files when they are transferred using a strong password, which will be provided to Plaintiffs or Plaintiffs' expert separately from the Impacted Data Files.

8. All documents containing information derived from the Impacted Data Files and that contain Designated Discovery Material will be treated by Plaintiffs and Plaintiffs' expert in accordance with PTO 10 and will be saved only on authorized encrypted hard drives subject to this Order. Documents containing information derived from the Impacted Data Files that do not contain any Designated Discovery Material may be saved on the air-gapped computers and transferred elsewhere as reasonably necessary solely for purposes of this litigation.

9. All hard drives used by Plaintiffs or Plaintiffs' expert to store the Impacted Data Files and related documents will be disconnected and stored in locked, secure locations whenever not in active use or transport with physical access controls in place to manage and track access to such secure locations. Plaintiffs and Plaintiffs' expert shall not make a copy of the complete set of Impacted Data Files but may make excerpts of the Impacted Data Files pursuant to Paragraph 10 that encompass the PII and/or PHI of twenty-five or fewer individuals..

10. Any excerpts of the Impacted Data Files created by Plaintiffs or Plaintiffs' expert(s) that contain PII and/or PHI must be transmitted only on FIPS 140-2 or 140-3 compliant hard drives, encrypted using AES 256 or equivalent, and accessed by strong, unique passwords provided separately from the excerpts or Impacted Data Files. The passwords shall contain, at a minimum, sixteen characters, an uppercase character, a lowercase character, a number, and a special character.

11. Any excerpts of the Impacted Data Files created by Plaintiffs or Plaintiffs' expert(s) that contain PII and/or PHI must be maintained only on FIPS 140-2 or 140-3 compliant hard drives, encrypted using AES 256 or equivalent, and accessed by strong, unique passwords provided

separately from the excerpts or Impacted Data Files. Or, excerpts of the Impacted Data Files created by Plaintiffs or Plaintiffs' expert(s) for purposes of expert discovery, expert reports, and briefing in this Action—and if password protected (using strong, unique passwords)—may be stored consistent with Plaintiffs' counsel's practice for storing Designated Discovery Material (as defined by PTO 10).

12. Plaintiffs and Plaintiffs' expert will permit access to the Impacted Data Files only as permitted by PTO 10 and this Order. Plaintiffs may permit access to aggregate or de-identified data derived from the Impacted Data Files or to samples of the data, in good faith and as reasonably necessary, to individuals or entities pursuant to Paragraphs 13, 14, 15, and 16 of PTO 10 and this Order. Plaintiffs shall maintain comprehensive, accurate, and up-to-date records sufficient to document the custody and transfer of the Impacted Data Files, including identification of the individual(s) with access to the Impacted Data Files, the location or device on which Impacted Data Files are stored, and the dates of any transfers of the Impacted Data Files.

13. Paragraph 9 through 12 govern the Impacted Data Files themselves and do not govern (1) de-identified excerpts, or (2) descriptions, analyses, reports, or summaries that do not contain PII and/or PHI concerning the contents of the Impacted Data Files that may be created by Plaintiffs' counsel or Plaintiffs' expert(s). Plaintiffs' counsel and Plaintiffs' expert(s) may create, transmit, and maintain de-identified excerpts or descriptions, analyses, reports, or summaries of the Impacted Data Files created by Plaintiffs' counsel or Plaintiffs' expert(s) that do not contain PII and/or PHI, consistent with PTO No. 10.

14. The Impacted Data Files, and any information derived therefrom, shall be used solely for purposes permitted under PTO 10 and this Order. Neither Plaintiffs, Plaintiffs' counsel, nor any expert, consultant, vendor, or other person granted access by Plaintiffs to the Impacted Data Files

may use the Impacted Data Files, directly or indirectly, to identify, contact, solicit, recruit, or encourage any individual to serve as a named plaintiff, class representative, claimant, or participant in this or any other litigation, arbitration, administrative proceeding, or legal action. Nothing in this paragraph shall prohibit communications otherwise authorized by the Federal Rules of Civil Procedure, a court order, or written agreement of the Parties, provided that such communications are not based upon or facilitated by information obtained from the Impacted Data Files.

15. Any and all transfers of custody of the hard drive(s) that store the Impacted Data Files will be documented on a log that will travel with each hard drive. Custody changes should be limited. Chain of custody documentation shall be provided to MDL Defendants each time custody changes and upon reasonable request. The information to be recorded on the log is the person transferring custody, the person taking custody, the date and time, the location of the hard drive, and the serial number of the hard drive.

16. In addition to the obligations set forth in Paragraph 21 of PTO 10, Plaintiffs will report to MDL Defendants any: (i) access to, use, or disclosure of the Impacted Data Files not permitted by this Order or by written agreement with the MDL Defendants; (ii) any “security incident” as defined in the HIPAA Security Rule involving the Impacted Data Files or data derived from it. Plaintiffs will, without unreasonable delay, but no later than within two (2) days after Plaintiffs’ Discovery (as defined in the HIPAA Breach Notification Rule) of a Breach, notify MDL Defendants in writing, to the extent such information is available, of the nature of the Breach, the date(s) of the Breach, the date of Discovery of the Breach, the Impacted Data in the Breach (including the number of individuals who are the subject of the Impacted Data Files involved in or affected by the Breach), the identity of the individual or entity that caused the Breach, the identity of the individual or entity that accessed or received the Impacted Data Files as a result of

the Breach, what corrective action Plaintiffs took or will take to prevent further Breaches, what Plaintiffs did or will do to mitigate any harmful effect of the Breach, and provide any other information as MDL Defendants may reasonably request. Inability to timely provide any of the preceding information does not extend the two (2) day requirement for notification.

17. If Plaintiffs learn of, or if MDL Defendants independently learn of, potential: (i) access to, use, or disclosure of the Impacted Data Files, or excerpts of the same, not permitted by this Order or by written agreement with the MDL Defendants; or (ii) any “security incident” as defined in the HIPAA Security Rule involving the Impacted Data Files or excerpts or data derived from it, Plaintiffs shall cooperate in investigating the potential Breach and in meeting MDL Defendants’ or any Covered Entities’ obligations under the HIPAA Breach Notification Rule, and any applicable federal or state security breach notification laws or regulatory obligations. Such cooperation shall entail the retention by Plaintiffs of an independent third-party forensic firm to investigate the potential Breach, jointly selected by the Plaintiffs and MDL Defendants. If Plaintiffs’ counsel or Plaintiffs’ expert(s) are responsible for such a breach, Plaintiffs’ counsel shall presumptively bear the responsibility for costs associated with the breach of the Impacted Data Files, or excerpts of the same, in their or Plaintiffs’ expert’s possession. Such presumption may be rebutted with evidence that Plaintiffs’ Counsel or their expert(s) bore no responsibility for such breach.

18. Given the volume and sensitivity of certain Personal Information in the Impacted Data Files, and given Plaintiffs’ request for these materials as purportedly relevant to the MDL litigation, the Impacted Data Files are excepted from Pretrial Order No. 7 (ECF No. 236), including but not limited to PTO 7 Paragraph 39 (which otherwise states that all parties to the MDL Proceeding and the Coordinated Actions shall have access to documents produced in either the MDL Proceeding

or in any Coordinated Action) and PTO 7 Paragraph 40 (which otherwise provides that documents produced in the MDL will be added by MDL Lead Counsel to a “document depository” for MDL plaintiffs and plaintiffs in Coordinated Actions). This Order shall be considered a “MDL Discovery Order” as that term is defined in PTO 7 Paragraph 13.

19. Data Destruction Procedures and Timelines. Upon the earlier of: (i) final resolution of this litigation (including exhaustion of all appeals or the expiration of time for any appeal), (ii) dismissal of Plaintiffs’ claims with prejudice, or (iii) mutual written agreement of the Parties, Plaintiffs and Plaintiffs’ expert shall destroy all copies of the Impacted Data Files, including any portions, excerpts, or derivatives thereof, within thirty (30) days (the “Destruction Deadline”).

20. Destruction Methodology. The destruction of the Impacted Data Files shall be accomplished using one or more of the following methods, as appropriate: (i) for electronic files stored on hard drives, secure data wiping using a minimum of three-pass overwrite compliant with NIST SP 800-88 guidelines, or physical destruction of the storage media by shredding, degaussing, or incineration; and (ii) for any paper documents containing information derived from the Impacted Data Files that constitute Designated Discovery Material, cross-cut shredding resulting in particles no larger than 5mm x 25mm. Destruction shall be conducted by Plaintiffs’ expert or a certified data destruction vendor.

21. Certification of Destruction. Within ten (10) business days after the Destruction Deadline, Plaintiffs’ lead counsel shall provide MDL Defendants’ counsel with a written Certification of Destruction (the “Certification”), signed under penalty of perjury, which shall include: (i) confirmation that all copies of the Impacted Data Files, including any portions, excerpts, or derivatives, have been destroyed in accordance with Paragraph 19; (ii) the date(s) on which the destruction occurred; (iii) a description of the destruction method(s) used; (iv) identification of the

individual(s) or entity(ies) who performed the destruction; (v) the serial number(s) of any hard drives or storage media that were destroyed or wiped; (vi) if a third-party destruction vendor was used, a certificate of destruction from such vendor; and (vii) confirmation that the signatory has made reasonable inquiry and believes the statements in the Certification to be true and accurate.

IT IS SO ORDERED.

Dated: August 7, 2026

s/ Dulce J. Foster

Dulce J. Foster

United States Magistrate Judge