DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Director
Office for Civil Rights
Washington, D.C. 20201

May 31, 2024

Anders Gilberg, Sr. Vice President, Government Affairs
Medical Group Management Association
1717 Pennsylvania Ave NW #600
Washington, DC 20006

Dear Anders Gilberg:

Thank you for your letter regarding the cyberattack on UnitedHealth Group's (UHG) subsidiary Change Healthcare. The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) takes this issue very seriously. We recognize the impact the Change Healthcare cyberattack has had on healthcare providers, health plans, and individuals and are working expeditiously to do our part to ease the impact of the cyberattack. We are prioritizing our investigations of Change Healthcare and United Health Group (UHG) and continue to provide guidance and assistance across the health care industry. I appreciate hearing from you on this important issue.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009[1] and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Breach Notification Rule[2] require HIPAA covered entities[3] (health plans, health care clearinghouses, and most health care providers) to provide breach notification to affected individuals (patients, beneficiaries, and others) following a breach of unsecured protected health information (PHI). Breach notification is essential for patient privacy because it provides transparency about what caused the breach, when the breach occurred, what PHI was disclosed, what steps affected individuals should take to protect themselves, and information about what the HIPAA covered entity is doing to investigate the breach, mitigate harm to affected individuals, and protect against further breaches.

Covered entities are responsible for ensuring that HHS, affected individuals, and, where applicable, the media, are timely notified of the breach of unsecured PHI.[4] This means that they must file a breach report with HHS through HHS's Breach Portal in addition to notifying affected individuals and, where applicable, the media.

Business associates are responsible for ensuring that HIPAA covered entities that are affected by

[1] Public Law 111–5, 123 Stat. 226 (Feb. 17, 2009) (codified at 42 U.S.C. 1390w–4(O)(2)).
[2] 45 CFR part 160 and subpart D of part 164.
[3] Covered entities are health plans, health care clearinghouses, and health care providers that conduct transactions for which HHS has adopted a standard.
[4] 42 USC 17932; 45 CFR 164.400 *et. seq.*

a breach at the business associate are timely notified of the breach of unsecured PHI.[5]

Under the HITECH Act and the HIPAA Breach Notification Rule, when covered entities discover a breach of unsecured PHI (for example, when they receive notification by their business associate of a breach at the business associate), covered entities are responsible for ensuring that HHS, affected individuals, and, where applicable, the media, are timely notified of the breach of unsecured PHI. Affected covered entities may delegate the task of providing these breach notifications to their business associate. Only one entity—which could be the covered entity itself or its business associate—needs to complete notifications to affected individuals, the HHS Secretary, and where applicable the media. In this case, affected covered entities could delegate to Change Healthcare or UHG the task of fulfilling all of the HIPAA breach notification requirements on the covered entities' behalf. Note, however, that even if breach notification tasks are delegated to another entity, the covered entities remain responsible for ensuring that the breach notification requirements are fulfilled such that the covered entities are in compliance with those requirements.

Decisions about who will perform breach notification to HHS, affected individuals, and where applicable the media, are up to the covered entities affected by this breach. Affected covered entities should contact Change Healthcare or UHG if they wish to delegate to Change Healthcare or UHG these breach notification tasks. If covered entities affected by this breach ensure that Change Healthcare performs the required breach notifications in a manner consistent with the HITECH Act and HIPAA Breach Notification Rule, those covered entities would not have additional HIPAA breach notification obligations.

As stated in our March 13, 2024, Dear Colleague letter,[6] OCR's investigation is focused on whether a breach of PHI occurred and Change Healthcare's and UHG's compliance with the HIPAA Privacy, Security, and Breach Notification Rules. OCR's investigation and enforcement interests in other entities that have partnered with Change Healthcare and UHG is secondary.

OCR also created a webpage[7] with information about the cyberattack on Change Healthcare that answers some of the frequently asked questions OCR has received, including questions concerning HIPAA breach notification requirements. This webpage is being updated in real time as questions arise.

---

[5] When a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

[6] https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html

[7] https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html

We hope this information is helpful to you. Thank you again for your letter.

Sincerely,

Melanie Fontes Rainer
Director
Office for Civil Rights