June 26, 2024

Melanie Fontes Rainer, Director
Office for Civil Rights
200 Independence Avenue, SW
Washington, DC 20201

Dear Director Rainer:

Thank you for the prompt response to the letter we sent to Secretary Becerra on May 20th concerning the Change Healthcare cyber incident and breach reporting responsibilities associated with this unprecedented attack likely involving millions of breach patient records.

The undersigned organizations, representing a broad range of clinicians and providers nationwide, continue to navigate the aftermath of this incident dating back to February 21st. We appreciate that your agency has updated the Frequently Asked Questions (FAQs) on your website. Upon reviewing your letter and the updated material, we have received a host of questions that our members simply cannot answer without further assistance and guidance from the Office for Civil Rights (OCR).

We understand that Change Healthcare and United Health Group (UHG) (Change Healthcare/UHG) have not yet reported the breach, and that OCR is conducting an investigation. Yet, clinicians and providers are committed to staying in compliance with the Health Insurance Portability and Accountability Act (HIPAA) and want to be fully prepared to support their patients. We appreciate that OCR's attention is directed primarily at Change Healthcare/UHG. However, given the complicated nature of this situation, our members have several outstanding questions and seek immediate guidance and resolution from your office. **It is essential that OCR promptly outlines and communicates the "when, what, why, and how" in this situation, ensuring that the accountable party can act without delay.**

Attached, you will find a set of questions where we seek clear, straightforward guidance to ensure that every clinician and provider has confidence that the responsibility for breach reporting continues to lie squarely with Change Healthcare/UHG. Additionally, any responsibilities borne by clinicians and providers are minimized, and there is no impact to patients.

The priority is for OCR to provide this needed clarity and guidance as soon as possible. We do, however, respectfully request a meeting to further discuss these concerns so that we can be assured we have a clear pathway forward surrounding these matters. Please do not hesitate to reach out to us by contacting Mari Savickis at mari.savickis@chimecentral.org.

Sincerely,

College of Healthcare Information Management Executives (CHIME)
American Academy of Family Physicians (AAFP)
American College of Physicians (ACP)
American Medical Association (AMA)
Medical Group Management Association (MGMA)

cc: The Honorable Xavier Becerra

Outstanding Questions Related to Change Healthcare/UHG

Breach Reporting Responsibility

Delegating Breach Reporting

- Specifically, clarification is needed regarding three OCR communications released on the same date:
    a. OCR Press Release, May 31: Covered Entities (CEs) "**may delegate**" and "would not have additional HIPAA breach notification obligations" if they "**work with**" Change Healthcare/UHG.
    b. OCR Updated FAQs, May 31: CEs must "**ensure that**" Change Healthcare/UHG fulfills the obligations and describes how Change Healthcare/UHG can give providers details on a piecemeal basis until enough detail is known to support a compliant breach notification to the individual, which then starts the 60-day notification window.
    c. OCR Response to our Letter, May 31: "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."
- Particularly on the last point above, clarification is needed on what it means for a CE to delegate a responsibility, when the CE "remains responsible." **We request confirmation that upon completing the delegation, the notification obligations will rest with Change Healthcare/UHG, with CEs responding to reasonable requests to provide Change Healthcare/UHG with any needed information to the extent feasible. Anything less will fall short of the mark in providing clarity and reducing the overwhelming burden already experienced by affected clinicians and providers.**
- Will there be a formal process created by Change Healthcare/UHG or HHS that CEs can complete to delegate the breach reporting responsibility to Change Healthcare/UHG to make this as seamless as possible – for example, an online submission form?
- If delegation may not be accomplished via an online portal hosted by Change Healthcare/UHG, what are the expected and specific actions that need to be taken by CEs who are in a Business Associate (BA) relationship with Change Healthcare/UHG and who wish to delegate breach notifications to Change Healthcare/UHG?
- We request that OCR provide a clear statement that CEs who are not in a BA relationship with Change Healthcare/UHG are under no breach notification obligation regarding the Change Healthcare/UHG data breach.
- What if Change Healthcare/UHG is not a CE's direct BA, but rather is a downstream (third-party or 4th party) subcontractor of a CE's BA? Does the CE then delegate required notifications to their BA, who in turn delegates to the Change Healthcare/UHG subcontractor?

Process for Sharing Names of Those Breached

- The Change Healthcare/UHG breach has impacted an untold number of patients – likely numbering in the millions. What is the process OCR expects for CEs to be made aware that their patient's data has been breached? For example, will Change Healthcare/UHG supply CEs with a file listing impacted patients? When does OCR expect this to occur?
- What assurance will Change Healthcare/UHG give to clinicians and providers that the breach has been reported to OCR for their impacted patients?

Impact from State Laws

- Given OCR's Frequently Asked Questions guidance appears to only apply to federal breach reporting, are OCR and Change Healthcare/UHG coordinating with state officials?
- In instances where reporting, notification, and remedy requirements are more stringent at the state level, how does OCR anticipate working with state officials to ensure Change Healthcare/UHG compliance?
- How does OCR anticipate working with clinicians and providers to ensure communications reach providers, including those in rural communities that do not have access to broadband and may best receive information via mailings or FAQ?

Clinicians and Providers with No Direct Relationship to Change Healthcare/UHG

- Some clinicians and providers are aware that some of their patients' protected health information is or has been found on the dark web, but have not had a contractual relationship with Change Healthcare/UHG for years. How will OCR handle these situations?

Patient Notification

- Given that patients see multiple clinicians and providers and may have more than one payer, it is likely most patients will receive multiple breach notification letters – unless this process is carefully managed and handled by Change Healthcare/UHG The overwhelming quantity of notifications could create undue stress, anxiety and confusion for patients. What is OCR's process to minimize the impact on patients so that they are only contacted once?