HEALTHCARE BUSINESS MANAGEMENT ASSOCIATION

May 29, 2024

Hon. Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Melanie Fontes Rainer
Director, Office of Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Secretary Becerra and Director Rainer,

I am writing to you on behalf of the Healthcare Business Management Association (HBMA) to urge you to clarify its April 19th FAQ document regarding entities that may be impacted by the HIPAA breach notification requirements related to the Change Healthcare cyberattack.[1] More specifically, we are asking the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) to clarify that UnitedHealth Group (UHG), which owns Change Healthcare, should be the only entity required to provide notifications to patients.

HBMA is a non-profit professional trade association for the healthcare revenue cycle management (RCM) industry in the United States. HBMA members play an essential role in the operational and financial aspects of the healthcare system. Our work on behalf of medical practices allows physicians to focus their attention and resources on patient care - where it should be directed - instead of on the many administrative burdens they currently face. The RCM process involves everything from the lifecycle of a claim to credentialing, compliance, coding and managing participation in value-based payment programs.

We are concerned that the FAQ, as currently written, would allow UHG to shift the notification burden to healthcare providers or revenue cycle management companies. Question 8 on the FAQ says,

> *Additionally, with respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified,* ***the covered entity may delegate the responsibility of providing individual notices to the business associate****. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may vary, depending on the circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.*

Many RCM companies have business associate (BA) agreements with Change Healthcare as part of our contracts. Further, Change Healthcare could be a covered entity (CE) and/or a BA depending on its arrangement with each provider, health plan and RCM company.

Right now, our members are trying to understand what their responsibilities are under the HIPAA breach notification regulation (45 CFR 164.410). This FAQ only adds to the confusion by suggesting that all

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

RCM companies with a BA agreement could be required to notify patients of this breach if UHG chooses to delegate that responsibility to its business associates.

It would be both incredibly burdensome and unfair for UHG to abdicate its responsibilities for notifying patients by delegating this responsibility to its business associates. We appreciate UHG CEO Andrew Witty's assertion at a May 1st Congressional hearing[2] that UHG will handle patient notifications.

> *So first and foremost, we are offering to take full responsibility of all notification obligations for everybody involved in this. And we're working with the regulatory offices to manage that process. So ideally, we would like to take that over, so that the physicians don't have to worry about those situations. We do have to make sure that the various regulatory oversight organizations support that approach. But, that's very much the way we would -- we want to step in and take that responsibility.*

It is clear that UHG has a desire to do the right thing and facilitate all of the patient notifications so that other parties do not have to but is looking for approval from regulators.

We understand that the FAQ is describing the HIPAA notification regulation (45 CFR 164.410) as written. A strict interpretation of how the regulation applies to this situation places a notification requirement on multiple entities, including Change Healthcare, providers and RCM companies**. HHS and OCR should use its enforcement discretion to provide a waiver to all parties other than UHG for the patient notification requirements and therefore only require UHG to facilitate the notifications.** This is the appropriate course of action because it is the fairest approach and the least burdensome. UHG should be the party responsible for patient notifications due to its ownership of Change Healthcare. Further, requiring multiple other parties such as providers and RCM companies to notify patients would create redundancies and confuse patients.

We understand that OCR might need additional statutory authority to implement this recommendation. We also intend to ask Congress to work collaboratively with OCR to ensure that it has the necessary authority for this enforcement discretion.

Thank you for your consideration of our concerns and recommendations. Please do not hesitate to contact HBMA if we can be of any assistance to you or if you have any questions for us about our recommendations by emailing HBMA Director of Government Affairs, Matt Reiter (reiterm@capitolassociates.com) or HBMA Executive Director Brad Lund (brad@hbma.org).

Sincerely,

Kyle Tucker
President, HBMA

[2] https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-examining-the-change-healthcare-cyberattack