HEALTHCARE BUSINESS MANAGEMENT ASSOCIATION

# Summary of HBMA's Recommendations to Senate Finance Committee Following the Change Healthcare Cyberattack

July 17, 2024

**About HBMA**: The Healthcare Business Management Association (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.

**Background:** The cyber attack on Change Healthcare earlier this year unfortunately impacted patients as well as the entire healthcare industry. Despite what is being said by UHG, this disruption and the fallout of this attack continues to impact the workflow and finances of healthcare providers and revenue cycle companies across the nation. Often, the interim processes put in place may be as much work to unwind as they were to put in place.

Contrary to what UHG is claiming, RCM companies continue to struggle with a lack of functionality from the Change Healthcare platform and with many of the payers that connect to Change Healthcare. This lack of functionality forces providers to engage in administratively burdensome and time consuming processes, for which we and our provider clients are not reimbursed by UHG. The lack of functionality includes:

- Millions (likely more) of dollars' worth of unpaid claims
- Many payers cannot provide accurate claim status information for millions of claims that were submitted during or since the cyberattack
    - Many payers do not allow resubmission of these claims citing timely filing requirements
- Inability to automatically post payments to patient accounts
- Many payers have not reconnected to Change Healthcare yet

**Recommendation 1: Enforce Existing Privacy and Cybersecurity Guidance, Statutes and Regulations**

The Change Healthcare cyberattack could have been prevented if United Healthcare had performed the most basic risk assessment due diligence. The lack of multi-factor authentication (MFA) by Change would have been immediately known and could have been addressed.

On February 14, 2024, the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) and National Institute of Standards of Technology (NIST) published a new, final version of their guidance for regulated healthcare entities to follow to improve cybersecurity compliance with the HIPAA Security Rule.[1] These resources are simply necessary, addressable

[1] https://csrc.nist.gov/pubs/sp/800/66/r2/final

or mandatory, compliance requirements for every entity that accesses, uses or in any way touches protected health information (PHI).

Congress should focus its cybersecurity response on existing guidance and best practices. HBMA supports OCR's resumption of HIPAA privacy and security audits. Similar to CMS and the Office of the Inspector General (OIG) high risk practice identification programs and targeted audits, the same types of random audits for high-risk entities that use, create, process, or handle PHI should be implemented.

There is no excuse for UHG not having operational redundancies in place to mitigate disruptions of this scale from any cause. HBMA members have faced operational disruptions from natural disasters such as earthquakes, hurricanes and tornadoes. However, these companies restored their operations within days, or even hours, because of the planning and contingencies we have in place. UHG must be held accountable for failing to incorporate such contingencies into such a vital part of the healthcare system.

**Recommendation 2: Require more transparency on exclusive clearinghouse agreements and require payers to allow multiple clearinghouse connections for all electronic transactions.**
Many clearinghouses have agreements to serve as the exclusive clearinghouse with payers. These requirements mean in many cases a claim is routed through multiple clearinghouses to reach the intended payer. Given Change Healthcare's size, many claims were routed through this clearinghouse. The cyberattack on Change Healthcare therefore had broader impacts across the entire RCM process.

**Recommendation 3: Standardize Plan ID Numbers**.
As it stands today, each clearinghouse can require the use of a different payer identification number to route electronic claims to the correct insurance company. These numbers are captured in practice management and hospital billing software and Electronic Health Records (EHR) systems across the healthcare industry. They are then transmitted in electronic files (837, 835, 276, 277) between RCM companies and clearinghouses to identify which insurance company the data should be sent to using a unique identification number for each payer and to help providers and their RCM companies understand the information they receive back from the payer.

While most clearinghouses utilize a five-digit payer identification number, what is unique to Change Healthcare is they utilize a four-digit payer identification number. It has been an administrative burden to the healthcare industry to update the payer identification number for every insurance in order to transmit or receive electronic files from any clearinghouse or payer other than Change Healthcare.

Unfortunately, there is not a standard for payer identification number even if it is five digits.

**Recommendation 4: Standardize the enrollment, testing, and approval process across all clearinghouses and payers.**
Enrolling with a clearinghouse to use its services to submit electronic claim files to and receive electronic remittance files from clearinghouses or direct to payers is an administrative burden with many insurance companies and clearinghouses. It is often a three-step process. The first, to be able to submit electronic files, such as a claim file (837). The second, to have an electronic file returned, such as an electronic remittance advice (ERA/835). And the third would be to receive payments direct to the provider account.

The enrollment process, whether paper or electronic, must be completed before moving into a testing phase. Depending on the revenue cycle billing or EHR system used, the testing phase may or may not be quick. Again, this will need to be completed for both claims submissions as well as files returned electronically. If the standard format is based on ANSI ASC X12 version 5010A2 for institutional claims and version 5010A1 for professional claims, then the enrollment, testing and approval process should be simple and not the burden it is today.

Requiring the healthcare industry to adhere to the ANSI ASC X12 v5010A2 or v5010A1 would be a significant advancement in interoperability and decrease the administrative burden across the healthcare industry, not only for healthcare providers but also for clearinghouses and insurance companies.

**Recommendation 5: Compensate providers and RCM companies for burdens incurred from the cyberattack and improve federal response coordination**.
The cyberattack led to high amounts of additional labor costs for providers and RCM companies. UHG should have to compensate healthcare providers, RCM companies and other impacted entities for the added costs caused by the continued disruptions from the Cyberattack.

We believe Congress must look at this cyberattack as akin to an environmental disaster. Federal agencies play an important role in helping impacted industries recover from these disasters. For example, FEMA coordinates a federal emergency response. It would be helpful to have a similar federal agency coordinating the government's response to large cyberattacks such as what happened to Change Healthcare.

CMS faced delays providing advanced/accelerated payments to Part B providers and suppliers because of concerns about having the authority to do so without a national emergency declaration. Additionally, the industry lacked transparency about law enforcement's role in the response and what other resources would be made available to impacted industries.

The Change Healthcare cyberattack was unique in that it impacted essentially the entire healthcare system's business transactions. A more coordinated federal response would have helped direct federal resources to impacted agencies and provided needed transparency during a major cybersecurity crisis.

When corporations cause large environmental contaminations, they might be required to fund a "superfund" for cleaning up the harm they caused to the environment. This cyberattack is a digital version of an environmental disaster. In 1980, Congress gave the Environmental Protection Agency (EPA) the authority to require responsible parties to fund clean up of environmental contamination. Congress should pass similar legislation to allow HHS to require entities fund "superfund" sites for cyberattacks that cause major disruptions to the healthcare system.

**Recommendation 6: Provide a one-year timely filing extension for all claims with dates of service since the cyberattack occurred.**
Providers and their RCM companies need more flexibility from commercial payers on timely filing requirements due to the ongoing challenges with Change Healthcare. Most commercial payers require claims to be filed within specified timelines. Typical timely filing is 60 or 90 days. Notably, Medicare offers a one-year timely filing period.

Under normal circumstances, the RCM process is highly automated and the HIPAA standard transactions help RCM companies submit claims, know the general status of all claims pending adjudication and receive all necessary information back from the payer. Due to the cyberattack on Change Healthcare, there are still many disruptions to the RCM process such as many claims are being submitted by paper or being held up by lengthy EDI enrollment processes.

While the situation is improving, many payers cannot provide information about a claim's status or return electronic remittance advice to RCM companies. This has resulted in many payers not allowing RCM companies to resubmit claims citing timely filing deadlines.

Due to timely filing and issues with health plans processing claims submitted through their own workarounds, patients might first be told they owe no cost-sharing only to later learn that they actually do owe cost-sharing after the claim is re-adjudicated by the payer. Patients will continue to experience confusion until Change Healthcare can fully restore functionality for all of its payers.

Congress should require payers to provide a one-year timely filing extension for all claims with dates of service on or after the cyberattack took place until Change Healthcare's functionality is fully restored for all payers that use this clearinghouse.

**Conclusion:** Despite UHG's claims that Change Healthcare functionality is restored, many impacts of the cyberattack remain unresolved. Claims are not processing normally, and many medical practices and RCM companies must still rely on administratively burdensome manual processes and workarounds.

Congress can and should help create a process by which UHG can be held financially accountable to help compensate impacted entities for incurred expenses. Change Healthcare was unprepared for the attack, which could have been prevented by the most basic set of cybersecurity protocols. The Committee must hold Change accountable for their negligence and urge OCR to enforce existing cybersecurity regulations and encourage companies to adapt industry best practices more effectively to prevent future attacks.

Thank you for your consideration of our concerns and recommendations. We greatly appreciate the opportunity to serve as a resource to the Committee on this important topic.

HBMA has also developed a more detailed version of our recommendations that includes supporting metrics which will also be made available to the Committee and any interested Congressional office.

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).