HBMA

HEALTHCARE BUSINESS MANAGEMENT ASSOCIATION

July 17, 2024

Hon. Ron Wyden
Chair
Senate Finance Committee
219 Dirksen Senate Office building
Washington, DC 20510

Hon. Mike Crapo
Ranking Member
Senate Finance Committee
219 Dirksen Senate Office building
Washington, DC 20510

HBMA Response to Senate Finance Committee's Inquiry into Clearinghouses Following the Change Healthcare Cyberattack

Dear Chairman Wyden and Ranking Member Crapo:

We appreciate the Senate Finance Committee's interest in the Healthcare Business Management Association's (HBMA) suggestions as part of your inquiry into healthcare clearinghouses following the devastating cyberattack on the largest clearinghouse in the United States, Change Healthcare (Change) which is owned by UnitedHealth Group (UHG).

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.

The cyber incident on Change Healthcare earlier this year impacted 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. This creates avoidable confusion for patients about their medical bills.

We are pleased to submit these suggestions to the Committee on how Congress can help address these ongoing challenges and to help prevent similar attacks in the future.

Section I: Cybersecurity
Section II: Operational Challenges
Section III: Supporting Data
Section IV: Conclusion

Section I: Cybersecurity

- Enforce Existing Privacy and Cybersecurity Guidance, Statutes and Regulations

Victims of most large cybersecurity breaches are entities that had inadequate or no required risk assessment at the time of the attack. While sophisticated cyberattacks will always be possible, HBMA believes vigorously enforcing basic, longstanding cybersecurity standards are the most important first steps in prevention.

It is clear that Congress is interested in improving cybersecurity throughout our healthcare system to prevent similar attacks from occurring in the future. We believe Congress' approach to cybersecurity must begin with a focus on ensuring existing cybersecurity best practices are followed.

The federal government frequently updates public cybersecurity resources from the first Health Insurance Portability and Accountability Act (HIPAA) regulations through the subsequent Health Information Technology for Economic Clinical Health Act (HITECH) regulations.[1]

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.[2] These resources are simply necessary, addressable or mandatory, compliance requirements for every entity that accesses, uses or in any way touches protected health information (PHI).

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.

Stating it was overlooked or inadvertently missed is simply unacceptable. The Centers for Medicare and Medicaid Services (CMS), OCR, NIST, and private industry experts have provided hundreds of tools, risk assessment checklists, required policies and procedures, best practices, business associate requirements, system security, etc. to aid every practice, business, and entity of all sizes in ensuring everything possible has been done to prevent cyberattacks.

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.

HBMA Recommendation: 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. Rather than trusting

[1] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[2] https://csrc.nist.gov/pubs/sp/800/66/r2/final

entities to do the required risk assessments, risk mitigation, and corrective actions, independent analysis should be considered.

When necessary, modifications, updates, corrective actions, and required compliance audits with HIPAA privacy and security rules could be addressed by programs similar to a Corporate Integrity Agreement (CIA) or Deferred Prosecution Agreement (DPA). Holding the executives and managers personally accountable for such egregious errors and omissions as UHG and Change committed is recommended.

Section II: Operational Challenges

❖ Continued Lack of Functionality from Change Healthcare

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, added work for which we and our provider clients are not reimbursed by UHG.

These issues translate into confusion for patients about how much they owe because health plans are not able to communicate essential information about how a patient's health insurance benefit applies to each service. RCM companies are reliant on information they receive from payers to understand if a claim is paid, denied, etc., and what the patient's cost-sharing responsibility is under their plan's benefit. 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 and payers can fully restore functionality for all of its payers.

The lack of functionality includes:

Enrollment: Change Healthcare's online enrollment process to use this clearinghouse and EDI services is not fully functional. Typically, this process allows us to submit one application for multiple payers. Instead, we must submit separate enrollment forms for each individual CPID (payer) with different forms, websites, for each. It is much more time consuming and difficult to track status of enrollments as a result of these additional requirements.

Manual Workarounds: Another issue RCM companies are experiencing is inability to obtain Explanation of Benefits (EOB) on claims from the outage period to get posted to patient accounts. Payment posting is an essential part of the RCM process that allows RCM companies to accurately track information about a claim's payment status and patients to know their correct cost-sharing in a timely manner.

Four months after the cyberattack occurred, this typically automated process must now be done manually for many payers. This creates a huge time and administrative burden.

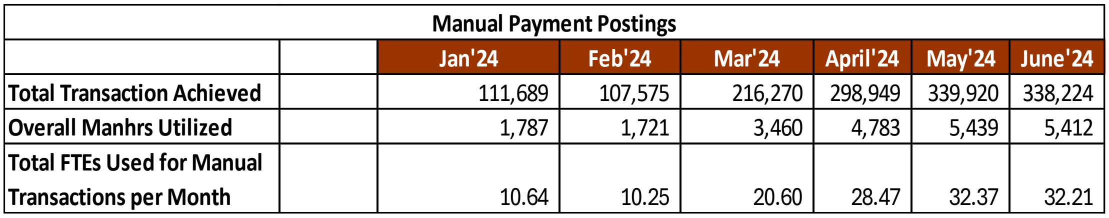
One large RCM company reported having to manually post $19 million worth of payments between March and June. Most of these claims are for relatively low dollar amounts, which suggests a high volume of manual entries. All of these manual postings were automated electronic 835 file transactions before the cyberattack on Change Healthcare.

In June, another HBMA member was posting 48% more EOBs manually vs. electronically than before the Change attack. All RCM companies are experiencing similar issues.

Many RCM companies are still forced to submit claims on paper due to inability of various payers to accept automated electronic claim submissions. Since the cyberattack occurred, one HBMA member has submitted 5,749 paper claims, totaling $1,290,689 worth of outstanding revenue.

Change Healthcare established an EDI as an electronic workaround but there are still challenges with this method. The enrollment process is not simple and they can be slow to approve new enrollment applications. This same HBMA member submitted 9,275 claims through EDI worth $3,252,068 in outstanding revenue.

As shown in the table below, another HBMA member continues to experience triple the number of manual transactions compared to before the cyberattack occurred.



Manual Payment Postings							
		Jan'24	Feb'24	Mar'24	April'24	May'24	June'24
Total Transaction Achieved		111,689	107,575	216,270	298,949	339,920	338,224
Overall Manhrs Utilized		1,787	1,721	3,460	4,783	5,439	5,412
Total FTEs Used for Manual Transactions per Month		10.64	10.25	20.60	28.47	32.37	32.21

Payers not Reconnecting: Change Healthcare has connection issues with payers even though Change shows them as “available.” This causes immense confusion for our industry. RCM companies may receive an acknowledgement from Change Healthcare that a claim we submitted was received. However, the connecting payer will not show that it has received the claim. Our members therefore have no way of knowing a claim’s status.

Disproportionate Impact on Government Payers: These issues are especially present with government payers. Electronic claim status is also still not available for Medicare contractors. With two different Medicare contractors, one RCM company had to call the MAC’s (Medicare Administrative Contractor) electronic data interchange (EDI) department and work with them to figure out what they needed to fix in their system to bring in the claims from Change. RCM companies have received no assistance from Change in getting these fixes in place.

- ❖ Timely Filing

Exacerbating this concern is that each health plan has timely filing requirements that dictate how long we have to submit a claim. Many health plans are claiming that the timely filing deadline has passed for many of these lost claims and will not allow us to resubmit them.

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.

HBMA Recommendation: Payers must provide a one-year timely filing extension for all claims with dates of service since the cyberattack occurred.

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

Due to the ongoing disruptions to the RCM process, Congress should work with 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.

❖ <u>Difficulties Changing from Change to Another Clearinghouse</u>

In response to the cyberattack, Optum took Change Healthcare offline. Change Healthcare was the center hub of a large wheel with many spokes. Disconnecting Change Healthcare meant providers had no immediate alternative way to submit claims and receive payment and ERAs. This existential cashflow disruption meant many providers had to switch clearinghouses. But this process was slow and administratively difficult.

Further, we continue to deal with issues related to switching clearinghouses including:

- Providers were required to submit new enrollment forms or applications with each new clearinghouse. It could take weeks for the enrollment process to conclude.
- Some payers had exclusive agreements with Change Healthcare, meaning it was the only clearinghouse from which they would accept claims. This means that switching clearinghouses did not provide a viable pathway to submit claims to those payers.
- Many payers do not allow multiple claim submission methods or Electronic Remittance Advice (ERA) options. To establish connections with a new clearinghouse or for direct submission, providers had to sever their connections with Change. Often, separate connections were needed for claims and ERAs, requiring a complete switch for both or limited options for ERA switching.
- As Change began to come back online, payers frequently terminated their connections with other clearinghouses without notice. This led to a lack of acceptance acknowledgments or rejections, prompting providers to scramble to re-enroll with Change.

HBMA Recommendation:

- Payers should be required to provide and allow multiple avenues/clearinghouse connections for ALL electronic transactions: claims, acknowledgment, ERA, claims status, etc.
- Improve enforcement of HIPAA standard transactions.
- Limit payer & clearinghouse requirements for unique information or segments.

❖ Standardize Plan Identification Number

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) to notify the clearinghouses 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.

HBMA Recommendation: HBMA supports a standardized payer identification number across all payers. Utilizing a similar standard to the National Provider Identification (NPI) number would significantly reduce the administrative burden across the entire healthcare industry. These numbers should always be included on the patient’s insurance card which would allow for a significant increase in accurate submission of claims to the correct payer and specific plan on the first pass.

❖ Enrollment for Electronic Claims and Remittances

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. Often, there are different applications for claim enrollment, electronic remittance advice and electronic transfer for direct deposit. The enrollment process is time-consuming and different for each payer.

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.

HBMA Recommendation: HBMA supports standardization of the enrollment, testing, and approval process across all clearinghouses and payers. 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. This standardization would reduce the unnecessary delay in claims adjudication and payments to providers for services rendered.

- Transparency for Payer Connections & Exclusivity Agreements

It is not uncommon for many insurance companies to enter into an exclusive agreement with a specific clearinghouse. Unfortunately, both the clearinghouse and the insurance company do not publicize these exclusive agreements leaving the provider of healthcare services unaware their claim for services is not being directly transmitted to the payer by the clearinghouse with which they are enrolled.

It is not uncommon to send a Blue Cross claim to clearinghouse A, at which time clearinghouse A will submit that claim to clearinghouse B, which will then submit the claim to Blue Cross. In this scenario, there was only one extra transmission before reaching the correct insurance company. However, transactions commonly process through multiple clearinghouses prior to reaching the payer.

Change Healthcare had several exclusive agreements requiring clearinghouse companies to send claims to Change Healthcare to then be transmitted to the insurance company through their exclusive agreement. In some cases, the claims may go through one clearinghouse, but the payment remittance would then come through Change Healthcare.

Lack of transparency contributed to the cyberattack’s disruptive effects because providers who submitted claims through a different clearinghouse had no way of knowing that their claims were also routing through Change Healthcare.

HBMA Recommendation: HBMA recommends each clearinghouse have the ability to submit directly to an insurance company. If this does not occur, then the insurance company and the clearinghouse must disclose to the public what companies are being utilized in exchanging electronic information to and from healthcare providers. By having exclusive relationships, this makes it very difficult to quickly pivot to another company in the event of a future clearinghouse malfunction or cyberattack.

- Compensating Providers and RCM Companies for Burdens Incurred from Cyberattack

As indicated throughout this letter, the cyberattack led to high amounts of additional labor costs for providers and RCM companies. Change Healthcare and payers that accept claims through Change Healthcare are not able to provide accurate claim status information for millions of claims that were submitted. Millions of dollars’ worth of unpaid claims remain tied up.

While UHG made some financial assistance available, that assistance was intended to provide temporary cash flow restoration until normal operations resumed. UHG has not shown any willingness to reimburse medical practices, RCM companies, and other impacted entities for expenses incurred due to the past and continued lack of functionality.

HBMA Recommendation: 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.

While there is ongoing litigation from several parties seeking damages against UHG, most impacted entities do not have the resources to participate in litigation against the largest healthcare conglomerate in the country nor do they have the time to wait for that process to play out for financial relief.

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 are often 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.

Section III: Supporting Data

Since the Change Healthcare cyberattack occurred, HBMA has been gathering as much information from our members as we can about the impacts the disruptions are having on the RCM industry. HBMA has conducted surveys of our members to assess the damage inflicted by the attack and has received more detailed information from certain members.

Below is an overview of data we received from our members through surveys and direct information. HBMA is in the process of collecting additional data from our members on the cyberattack's continued impacts. We will share updated metrics as we receive more data from our members.

- According to one HBMA member, as of July, 260 payers they work with still have not reconnected to Change Healthcare
- According to another member from a national RCM company with clients in every state, there are over 7.93 million claims submitted during the disruption that have not been paid. This is only for one specialty.
    - To contextualize this volume as a percentage of revenue, one large hospitalist group still has 5%-10% of its claims outstanding.
- One HBMA member lost existing and potential client contracts due to the outage worth a total cumulative value of $200,000 - $400,000, annually.
- In June one HBMA member was posting 48% more EOBs manually vs. electronically than before the Change attack. These manual payment postings are among the most administratively burdensome impacts of the cyberattack.
- One large RCM company reported having to manually post $19 million worth of payments between March and June. Most of these claims are for relatively low dollar amounts, which suggests a high volume of manual entries. All RCM companies are experiencing similar issues. All of these transactions were automated electronic transactions prior to the cyberattack.
- Since the cyberattack occurred, one HBMA member has submitted 5,749 paper claims, totaling $1,290,689 worth of outstanding revenue.
- Change Healthcare established an EDI as an electronic workaround but there are still challenges with this method. The enrollment process is not simple and they can be slow to approve new enrollment applications. This same HBMA member submitted 9,275 claims through EDI worth $3,252,068 in outstanding revenue.

While it is clear the situation has improved since the height of the cyberattack, the depth of that disruption means we have a long way to go before returning to normal functionality. Below is a summary of HBMA's survey results on the cyberattack's disruptions during the peak of the cyberattack's impacts in March and April.

- During the height of the cyberattack disruption in March, 26% of respondents had to post payments manually (a time/administrative burden) compared to the typical, more automated process. All respondents reported having to post at least some payments manually.
- Denial rates went up for over half of respondents during the height of the disruption. The most common answer was 10-20% increase, which was reported by 31% of respondents.
- During the height of the disruption, 76% of respondents had to provide more financial reports to clients than usual.
- Over half of respondents switched clearinghouses (and faced the substantial additional problems associated with doing so outlined earlier in this letter).

Section IV: 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.

Change Healthcare and payers that accept claims through Change Healthcare are not able to provide accurate claim status information for millions of claims that were submitted.

While UHG made some financial assistance available, that assistance was intended to provide temporary cash flow restoration until normal operations resumed. UHG has not shown any willingness to reimburse medical practices, RCM companies, and other impacted entities for expenses incurred due to the past and continued lack of functionality. 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.

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).