March 26, 2024

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

Dear Secretary Becerra:

The College of Healthcare Information Management Executives (CHIME) is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders in hospitals, health systems and other healthcare settings across the country. Launched by CHIME in 2014, the Association for Executives in Healthcare Information Security (AEHIS) represents healthcare security leaders and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT and experts, including on the topics of cybersecurity, privacy and security.

I write to you today on behalf of thousands of C-suite executives working in healthcare delivery organizations (HDOs) across the country to express concerns and request your assistance. As you are aware, Change Healthcare – a unit of UnitedHealth Group (UHG) – was impacted by an unprecedented cybersecurity incident on February 21, 2024. However, the fallout and financial impact stemming from this cyberattack continues to impact not only our members – but the entire healthcare ecosystem. While we appreciate the administration's ongoing efforts to assist healthcare providers, there continues to be much confusion and a dearth of information needed by those impacted, which continues to hinder recovery efforts and exacerbates the burden on providers.

The scale of the Change Healthcare cyberattack is unprecedented, and its tentacles have reached into nearly every corner of our sector. The implications of this attack, now more than a month ago, are still being felt. We recognize that Change Healthcare is working tirelessly to resolve the myriad of issues following this attack, and that the complexity associated with the recovery is enormous. We appreciate the steps you have taken thus far to coordinate federal response efforts and maintain communication and contact with UHG. We appreciate that UHG has and continues to host stakeholder calls, is sharing some information with our members, and announced more updates on March 22nd. However, the level of detail they are sharing remains insufficient and more outreach is needed to providers as many feel they are operating in the dark.

Our members are committed to cybersecurity best practices and take their responsibility to protect not only the privacy and security of patients via the data, devices, and third-party services networked to their system – but critically – their patient's overall safety and well-being. However, our members are frustrated and burdened by the lack of forthcoming, reliable, detailed information and the resulting uncertainty. It is hampering recovery efforts and time is of the essence. To put it simply, what they need three things from UHG and Change Healthcare: 1) is more information related to assurances from third-party assessors

that it is safe to reconnect to their systems as there is ongoing confusion surrounding this issue; 2) timely, reliable and more complete communication in general; and 3) the controls that are being put in place to avoid future attacks. I write to seek your additional intervention and assistance in resolving these outstanding concerns.

There is still widespread confusion among providers concerning when it is safe to reconnect to the Change Healthcare systems and many still do not feel they have a clear path forward. We recognize that Change Healthcare continues to update their website, however information is not reaching all HCOs and there are still several outstanding questions and concerns. Not all HCOs are being invited to the UHG weekly calls, some questions are being asked regularly on the calls, but answers have not yet been provided, or the level of detailed shared is insufficient. For instance, Change Healthcare has not shared details about controls they are adding to help guard against future cyber incidents. Like nearly all organizations in the United States, hospitals and HDOs must care – to some degree – about their ability to generate positive net revenue in order to keep their doors open. However, they are unlike other organizations in that their first and most important mission is to care for their patients.

Thus far, the information being shared and conveyed to our members has been focused on directing connections to Optum systems – also owned by UHG – as a workaround. Further, the level of ambiguity related to timing is exacerbating our members' concerns, and more information from Change Healthcare is needed immediately. While UHG has repeatedly said that if one of their systems is up that they are confident that it is safe to reconnect to it, many providers remain deeply concerned about reconnecting without third-party attestations. We appreciate that UHG recently announced that there is now third-party documentation and an Assurance Security Environment Statement now available for request. Many providers remain unaware of this.

The longer this situation remains unresolved, the more precarious the financial situation becomes for HDOs. Providers have engaged in workaround solutions to the best of their ability, but cash flow remains extremely concerning for many. Presently, since the payors are sitting on billions of dollars of claims, this essentially amounts to HDOs giving zero percent loans to insurance companies who use Change Healthcare. Providers are already shouldering an enormous financial and administrative burden and many cannot afford to go a day longer without being made whole. The workaround that providers have had to undertake to try and get paid by updating transactions to route through Optum and reverting back to Change Healthcare will take time. Additionally, as this situation drags out, it becomes more and more challenging for providers to meet federal compliance deadlines.

Our members need to know:

Patient Privacy

- Was there a breach of protected health information (PHI) and if so how many patients' data were exposed?
- When will HDOs and individual patients be notified?
- What are UHG's plans for reporting the breach? Will they be acting as a HIPAA covered entity and thus handling the reporting or will they act as a business associate and shift the burden of notification reporting to the providers?

Reconnecting & Cybersecurity

- Are there plans to communicate and make the information related to third-party attestation widely available to HDOs?

- What assurances will be given to providers, and when, that there are no additional cyber vulnerabilities? And, how can they be certain should further cyber vulnerabilities come to light following reconnection – that they will not be held responsible or liable in any way?
- What are Change Healthcare's detailed plans on how they will bring providers back on to their systems, and how will access be throttled – if at all? How will they decide this, how will this be communicated, and critically – when will it be communicated?

Payers & Payment

- When will Change Healthcare make available a list of payers directly connected to their systems?
- What will be the process for handing payers who already migrated to the Optum Intelligent EDI platform? How will they be reverted back to CHC?
- What are Change Healthcare's detailed plans to handle cash flow should these issues continue to persist past a fifth week?

As the named Sector Risk Management Agency (SRMA) for the Health Care and Public Health (HPH) Sector pursuant to Section 9002 of the National Defense Authorization Act of 2021, the U.S. Department of Health & Human Services (HHS) plays a critical role in overseeing the response stemming from this attack. **We implore you as the SMRA to:**

1. **Take swift action by compelling Change Healthcare to release the answers to these vitally important questions, institute a widespread communication plan and put providers and the patients they care for on the path to a full and safe recovery, as quickly as possible;**
2. **Ensure that HDOs are fully reimbursed along with interest owed by those payers with connections to Change Healthcare who are sitting on billions of dollars of their payment;**
3. **Conduct a sector-wide risk assessment to ensure this type of attack does not happen again;**
4. **Establish a cyberattack communication and action plan providing immediate response and action steps minimizing ongoing industry wide disruptions in the future;**
5. **Establish criteria for when the U.S. government constitutes a cyber-attack against our sector as rising to the level a national disaster; and**
6. **Consider extending federal compliance deadlines as HDOs continue to wrestle with the most extensive cyber-attack our sector has ever experienced.**

CHIME and AEHIS stand ready to assist in any manner. Should you have questions please contact Mari Savickis, CHIME's vice president of public policy at mari.savickis@chimecentral.org.

Sincerely,

Russ P. Branzell, CHCIO, LCHIME
President and CEO, CHIME