June 26, 2024

Dear Sec. Xavier Becerra,

We represent provider organizations nationwide focused on balancing the use of secure technology systems and trusted data to provide the best care possible to patients. Our organizations represent hospitals and providers both large and small that have been materially impacted by the Change Healthcare cybersecurity incident. Today we ask you to use the regulatory authorities available across the U.S. Department of Health and Human Services (HHS) and its federal partners to mitigate the impact of these types of attacks in the future through increased resiliency, transparency, and after-incident support.

The scope and impact of the Change Healthcare attack on the ability of providers to deliver and cover practice costs has been well documented both by HHS and UnitedHealth Group (UHG), parent company of Change Healthcare. An informal survey conducted by the American Medical Association in late April demonstrated the overwhelming nature and impact on medical practices. Even several months after the attack, 85 percent of physicians continued to experience disruption and 62 percent were using personal funds to cover practice expenses. While Change Healthcare reports to be back online and functional, the impact of the extended downtime is still being felt by providers nationwide. Provider organizations are waiting for the full functionality of Change Healthcare services to become available again and many are facing a future of additional administrative burden in the form of extensive documentation and claims and denials processing in support of cleanup activities.

Changes must be made within our nation's healthcare system to ensure that one piece of technology, intermediary, or vendor cannot disrupt the delivery of care nor the stability of the revenue cycle and clinical data exchange. We recommend the Biden Administration take the following steps to reduce the likelihood of a similar attack against our healthcare system in the future and HHS should partner with relevant agencies including, but not limited to, the Federal Trade Commission (FTC) and Department of Labor (DOL) when appropriate. If, for any reason, HHS does not have the authority to accomplish any of these recommendations we urge HHS to seek those authorities from Congress where necessary.

1. Increase resiliency in the healthcare system.

Increasing resiliency includes the Biden Administration **conducting an HHS led nationwide technology audit to understand the scope of technologies used in healthcare and to identify areas reliant on one technology platform or tool.** With healthcare services and systems stretching far beyond the provider, it is important to have an accurate understanding of the true scope of technology services in the business of healthcare. This audit should identify critical services and key points of failure in systems owned and operated by health plans, insurers, and intermediaries such as clearinghouses. HHS will be positioned to use the findings of the audit to encourage greater technology diversity throughout healthcare, particularly in areas that are reliant on sole-source technology platforms and/or tools, and to work with other federal partners to accomplish similar goals within their programs.

We also recommend **increasing interoperability in healthcare technology systems to enable agile organizational shifts when one technology is unavailable.** Provider organizations were damaged beyond measure by the Change Healthcare attack, not only because of the ubiquitous nature of the platform, but also due to providers' limited ability to pivot to another technology platform or solution. Additionally, many providers were constrained by existing contractual obligations that prevented them from transitioning to an alternative tool or platform. These limitations and contractual agreements only

become more limiting as the number of different technology players in the market decreases and providers are unable to adopt the few, if any, alternatives available to them. We believe HHS has the authority necessary to strengthen the nation's cybersecurity posture by increasing interoperability and ensuring healthcare is not reliant on only a few technology solutions to support the revenue cycle. In situations where a technology or platform is the victim of a cyberattack and unable to function, the entities that developed the technology should be required to have redundancy plans in place that allow provider organization clients to be able to switch to other vendors with as few roadblocks as possible and at no additional cost to providers from that current vendor. HHS should consider its regulatory authority to include health plans, insurers, and intermediaries in these requirements. Absent this authority, HHS should work with Congress to make sure all health plans, insurers, and intermediaries are subject to these requirements.

Ensuring multiple technology solutions are available in the market for critical healthcare infrastructure processes is also key to improving technology resiliency throughout the healthcare system. Change Healthcare is one of the few service providers for multiple critical administrative and clinical processes in healthcare today – including claims processing, remittances, eligibility and claim status checks, and other crucial services. For example, provider organizations have limited choice in terms of technology platforms to support such activities as ePrescribing, which is a federal mandate. Although in the short term having just a few technology platforms may facilitate interoperability advancement, this limited choice of platforms may create additional, unanticipated liability risk for providers in the event of any disruption, much like in the case of the cyber event with Change Healthcare. For that reason, we ask the Biden Administration to utilize its regulatory levers to ensure multiple solutions are available for federally required healthcare technology infrastructure. In addition, we recommend HHS continue to collaborate with its other federal partners to determine other opportunities to increase the number of high-quality technology solutions available to providers.

2. Increase transparency throughout a nationwide healthcare infrastructure cyberattack and beyond.

Increasing transparency throughout the nation's healthcare infrastructure includes **providing clear and accurate accountings of the timelines and expectations throughout the cyber incident and beyond.** With notification and reporting requirements placed on providers during cybersecurity incidents, it is crucial for providers to have a clear timeline of events and expectations. Trust between the patient and provider becomes paramount during cyber incidents, and HHS can increase that trust by working to require greater transparency.

Continuing system-wide communication on the status of technology recovery after an incident is completed is also critical to improving transparency. We appreciate UHG's efforts throughout the incident to hold regular teleconference calls on the status of the cyber incident. However, the communications ceased when Change Healthcare stated the incident was resolved and Change Healthcare was deemed safe to use again – when in reality many provider organizations were still experiencing impacts of the attack. Confusion within the healthcare system continued as announcements related to functionality restorations often did not equate to services being fully available for all providers. This led many providers to be faced with tedious and time-consuming processes of reviewing and determining the availability of each of their connections one-by-one. We encourage HHS to use its authority to ensure providers receive trusted communications on recovery including after the

primary attack is mitigated, as we know recovery work continues after an intruder is removed from a system.

3. Support provider organizations through post-incident cleanup activities.

Provider organizations require continued support as part of post-incident cleanup activities. This includes **providing guidance and organizational support throughout the breach notification process**. Large scale infrastructure attacks lead to confusion including who must report and when under federal requirements. We recommend HHS provide robust guidance in the wake of these types of attacks to ensure providers understand the department's expectations.

Requiring attacked technology organizations to support post-incident processes, such as post-claims processing, is also a critical component of post-incident cleanup activities. While some of Change Healthcare's systems may be back online, the recovery work for provider organizations is only beginning. Transactions and claims that were processed outside of the system or on paper must now be input into Change Healthcare's system and claims processed prior to the attack must be updated. Practices already report a significant uptick in claim denials due to issues with timely filing deadlines, eligibility verification, or missing prior authorization approvals. We ask HHS to pursue and advocate for regulatory authorities that require entities that are attacked – including health plans, insurers, and intermediaries – work with impacted provider organizations throughout post-incident recovery to equitably share the burden of recovery.

Our organizations understand cybersecurity incident recovery requires a nationwide effort. We stand ready to work with HHS and our technology partners to create a safer healthcare system. These recommendations are the first step in putting our nation on a path towards a stronger healthcare infrastructure. If you would like to discuss our recommendations further, please contact AHIMA's Senior Director of Regulatory and International Affairs at andrew.tomlinson@ahima.org.

Sincerely,

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