June 11, 2024

CHIME's response to the Question for the Record (QFR) submitted by the Honorable Nanette Barragán for the hearing titled "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack"

The impact of this cyberattack was felt across the healthcare system because the technology has been adopted by so many. Yet third-party technology and vendors, such as Change Healthcare, are not regulated the same way that hospitals and providers are. When a certain kind of technology becomes such an instrumental part of how our health care system functions, does this warrant stronger government regulation of that third party technology?

Congresswoman Barragán, thank you for your question. Third-party risk remains an enormous weak spot for the Healthcare and Public Health (HPH) sector and cannot be solved by imposing costly mandates on providers.

Third-parties that store, process and/or transmit protected health information (PHI) on behalf of Health Insurance Portability Accountability Act (HIPAA) covered entities (i.e., CHIME members) are a critical and necessary part of the HPH Sector. Yet, during each contract negotiation with healthcare providers, they create caps on their liability that shift multiple millions of dollars of liability for a cybersecurity breach back to those organizations and/or their providers. The number of technological factors and undiscovered vulnerabilities outside of a provider's control is significant and grows with new innovations made in healthcare. The size of a hospital or healthcare system and their ability to negotiate these responsibilities with third-parties should not matter. If we are to make meaningful improvements in our sector, this responsibility must be shared equally.

Whether located in a patient's room or the hospital laboratory, both medical devices and other devices – such as a patient's mobile device – rely on network connectivity for operations and maintenance. Additionally, nearly all the technological components in these devices are not developed by the HDO. These components include software, services, and hardware developed by third-party organizations.

One study found that the average number of third-parties that HDOs contracted with in 2021 was 1,950 and anticipated a 30% increase to an average of 2,541 in 2022. Further, it notes that: "Third-party products and services are a necessary and critical part of the HDO IT blueprint, but each brings another set of risk factors to the table. Some risks are inherent to the third-party such as security of operating systems and other embedded software in medical devices […] the risk created by the third-party or the HDO use of the third-party needs to be managed. The

burden is on the HDO to perform assessments throughout their relationship with the third-party (e.g., procurement, implementation, usage, updates, termination, etc.)."[1]

Payers and clearinghouses are also HIPAA covered entities. They both hold vast quantities of patient data and are integral partners in the healthcare system as evidenced by the Change Healthcare attack. It is imperative that they meet certain cybersecurity standards as well.

To put it simply, we recommend that anyone who is touching patient health data has an obligation to help protect it.

For years, our members have reported to us that they experience challenges with some medical device manufacturers refusing to sign business associate agreements (BAAs). Our members, as HIPAA-covered entities, are required to enter into BAAs with any third-party that handles PHI. Some of these medical devices contain PHI, and/or provide the manufacturers with access to PHI. Providers come to the "bargaining table" as the underdog and often find their requests to have business associates sign BAAs denied. We believe this critical issue warrants the attention of Congress.

We are aware that some lawmakers and the administration are considering ways to penalize hospitals for failure to have the right technology and protections in place to stop a cyber breach. Hospitals work hard – and are successful – at stopping threat actors from entering their systems every day. Penalizing them financially will only set them back further, especially small and safety-net providers. Threat actors – when successful – often penetrate hospitals by taking advantage of weakness in software and devices outside of their control (e.g. all networked devices and medical devices). If we are all to maintain the key objectives around safeguarding patients and protecting national security, then cyber responsibility in healthcare – as noted above – must be a shared one.

CHIME appreciates the opportunity to help inform the important work being done by members of the House Energy and Commerce Committee. Should you have questions about our position or if you would like to speak directly to one of our members with expertise in this issue, please contact Cassie Ballard, CHIME's Director of Congressional Affairs, at [redacted].

[1] Microsoft Word - Ponemon Research Report - The Impact of Ransomware on Healthcare During COVID-19 and Beyond.docx (website-files.com)