March 02, 2022

Ms. Dawn O'Connell
Assistant Secretary for Preparedness and Response
The Hubert H. Humphrey Building
200 Independence Ave. SW
Washington, District of Columbia 20201

Comments Submitted Electronically via NHSS@hhs.gov

Dear Assistant Secretary O'Connell:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) welcomes the opportunity to submit comments in response to the Assistant Secretary for Preparedness and Response (ASPR) *2023-2026 National Health Security Strategy (NHSS)* Request for Information (RFI) published in the *Federal Register* on February 14, 2022. Our respective members remain on the frontlines fighting for a safer more cyber-secure healthcare system. Healthcare has never been under more persistent threat of compromise than it is today, and future projections only appear bleaker. An aggressive security strategy included as part of the 2023-2026 NHSS focused on increasing cyber resiliency will ensure the health system is ready to meet the looming cyber threats facing the nation in 2023 and beyond.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate for the effective use of information management to improve the health and healthcare in the communities they serve. Launched by CHIME in 2014, AEHIS represents chief information security officers (CISOs) and provides education and networking for senior IT security leaders in healthcare. Our combined more than 5,000 members are among the nation's foremost health IT experts, including on the topic of cybersecurity and they take their responsibility to protect the privacy and security of patient data and devices networked to their system incredibly seriously.

The barrage of cyberattacks lodged against healthcare providers during the COVID-19 pandemic continues to escalate, both in volume and sophistication. They pose a persistent threat to patient safety and our national security. In 2020, the first year of the pandemic, there were 642 data breaches of 500 or more healthcare records reported to the Health and Human Services (HHS) Office for Civil Rights (OCR), an average of 53 per month.[1] Last year, the number of healthcare data breaches increased 10.9% to 712, a new record. More than 45 million individuals were impacted. Most breaches were due to hacking/IT incidents, including over 80% of breaches reported in December.

Already in 2022, we are seeing heightened cyber activity in healthcare. Furthermore, criminals have increased their activities over the last two years taking advantage of the pandemic at a time when the healthcare system is already under enormous strain. According to the World Health Organization (WHO), cybersecurity attacks have seen a five-fold increase since the start if the pandemic.[2] Many consider the cybersecurity threats themselves to be an epidemic creating enormous strain on systems as they wage war against COVID-19 and these relentless attacks.

[1] https://www.hipaajournal.com/december-2021-healthcare-data-breach-report/
[2] https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

CHIME and AEHIS fielded a survey of its membership's chief information security officers (CISOs) in 2021 to determine the impact cybersecurity incidents had on healthcare in the last year.[3] Two-thirds of respondents reported having a security incident in the last year, with nearly half reporting they had been impacted by a phishing email or business email compromise and almost 30% saying they'd faced a system or electronic health record (EHR) outage. Most concerning, 15% of respondents reported a patient safety incident tied to a cyber event, and 10% experienced the need to divert patients to another care setting, a trend that has continued to rise in recent years.

The healthcare sector is only as strong as its weakest link and smaller organizations are not sufficiently resourced to fend off cyberattacks. **Therefore, as part of the 2023-2026 NHSS, we propose that ASPR create and prioritize programs designated to aid small and under resourced providers protect themselves against, detect, respond to, or recover from cybersecurity threats.** These programs can be successful by providing monetary aid or technical assistance to help eligible providers adopt recognized cybersecurity practices – such as HHS 405(d)[4], recognized by Congress in H.R. 7898 signed into law on January 5, 2021 – replace legacy systems and devices, conduct a security risk assessment, and generate an action plan for mitigating identified risks, or hire staff. By raising the security floor for all providers, including small providers, the whole health sector becomes safer. Patients will better trust the safety of their data and that will assist in creating the fully interoperable health system envisioned by health leaders for nearly two decades.

In addition to the development of the above program, ASPR should prioritize cybersecurity during budgetary activities. An increase in budgetary allocations towards cybersecurity activities within ASPR will assist in the implementation of the above program activities and will ensure that ASPR has the monetary resources needed to adequately assist the sector in cyber defense activities. As part of this increase in budgetary action, ASPR should also increase its cooperation with, and advocacy for, other cybersecurity programs within HHS, such as the Health Sector Cybersecurity Coordination Center (HC3) and the 405(d) Program and Task Group. By increasing monetary commitments and coordination, ASPR can ensure it is improving the nation's cybersecurity through all available avenues.

With the nation on the precipice of a new era in data sharing, trust in the security of health data is paramount. If patients do not trust the data their provider exchanges, or do not trust that what they tell their provider will stay private, then the ability to care for patients will be impacted significantly. It is time for the nation to treat the cybersecurity of health data the way it treats other crucial national security topics. If the nation is not able to secure the health system's data infrastructure from top to bottom, then trust in the system itself will begin to erode. Time is of the essence as cyber criminals continue to advance in their sophistication and foreign state actors increasingly have become active in the theatre of cybersecurity. We implore ASPR to begin planning to counter these threats by making healthcare cybersecurity equity a key priority now and in the future.

CHIME and AEHIS welcome any opportunity to partner with ASPR in the development of the 2023-2026 NHSS. Our members will remain vigilant as it relates to healthcare cybersecurity readiness and are willing to assist in whatever way possible to ensure providers nationwide have the resources they need to protect themselves. If you have any questions related to healthcare cybersecurity, or our letter, please contact Mari Savickis, Vice President of Public Policy, at mari.savickis@chimecentral.org.

Sincerely,

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

[3] https://chimecentral.org/survey-of-chime-and-aehis-membership-finds-widespread-cybersecurity-impacts-on-healthcare-need-for-more-government-support/
[4] https://405d.hhs.gov/Documents/HICP-Main-508.pdf