March 29, 2023

Senator Bernard Sanders
Chair
Senate HELP Committee
Washington, DC 20510

Senator Bill Cassidy, M.D.
Ranking Member
Senate HELP Committee
Washington, DC 20510

Senator Robert P. Casey, Jr.
Member
Senate HELP Committee
Washington, DC 20510

Senator Mitt Romney
Member
Senate HELP Committee
Washington, DC 20510

Dear Senators Sanders, Cassidy, Casey, and Romney:

The College of Healthcare Information Management Executives (CHIME) is pleased to offer our ongoing thought leadership as Congress seeks to reauthorize the Pandemic and All-Hazards Preparedness Act (PAHPA).

CHIME is the professional organization for Chief Information Officers and other senior healthcare IT leaders. Our more than 5,000 members are among the nation's foremost health IT experts, including on the topics of cybersecurity and privacy – working on the frontline in hospitals and healthcare settings across the country and tasked with ensuring the security of patient and healthcare provider data and devices connecting to their networks.

We greatly appreciate your request for stakeholders' comments on 2023 PAHPA reauthorization efforts. As you know, PAHPA was first signed into law in 2006 to "improve the Nation's public health and medical preparedness and response capabilities for emergencies, whether deliberate, accidental, or natural" and has since been reauthorized twice, most recently in 2019.[1] CHIME provided comments during the last reauthorization and was pleased to see cybersecurity language (Section 703 of PL 116-22) included in the legislation for the first time.

However, the healthcare cybersecurity threat landscape has vastly changed since 2019 and a greater focus on cybersecurity is warranted to respond to these threats to the healthcare and public health (HPH) sector. In 2019, there were 510 data breaches of 500 or more healthcare records reported to the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR).[2] Last year, that number rose to 707, with 84.6% of breaches occurring as a result of hacking incidents.[3] Healthcare breaches were reported by HIPAA-regulated entities in nearly every state last year including Vermont (3), Louisiana (3), Pennsylvania (38), and Utah (5).

[1] https://aspr.hhs.gov/legal/pahpa/Pages/default.aspx
[2] https://www.hipaajournal.com/healthcare-data-breach-2019-report/
[3] https://www.hipaajournal.com/2022-healthcare-data-breach-report/

Question from the RFI:

1. What gaps do you see in the PAHPA framework, or how it has been implemented to date? (These gaps could be related to any of the programs noted above, or other aspects of the public health and medical preparedness and response ecosystem that are otherwise currently unaddressed.)

Answer:

Most healthcare settings in the U.S. are not-for-profit and many are small, and resources for them to fend off the multitude of cyberattacks are limited, if not non-existent. While some medium to larger healthcare systems are better resourced, there are still limits to what they can do. Healthcare delivery organizations are simply no match for sophisticated nation-state funded attacks. We strongly believe that cybersecurity is a shared responsibility. However, providers need additional support to defend themselves from the increasingly sophisticated attacks aimed at stealing intellectual property, extorting ransom payments, threatening patient safety by targeting medical devices connected to them, and hindering providers' ability to deliver care overall.

We propose adding a grant program or a voluntary incentive program to PAHPA to help offset the investments needed by healthcare providers to improve their cyber posture and reduce patient safety and national security risks. This was one of the recommendations included in the landmark report to Congress issued by the 2017 Health Care Industry Cybersecurity Task Force established under the Cybersecurity Act of 2015. We also have our own data that supports this.

In 2021, CHIME and the Association for Executives in Healthcare Information Security (AEHIS) fielded a survey of our membership's chief information security officers (CISOs) to determine the impact cybersecurity incidents had on healthcare in the last year. 40 percent of respondents reported needing additional help in terms of grants and federal assistance.[4] A cybersecurity incident should trigger the same level of response as a natural disaster or pandemic, because as we know, a cybersecurity incident can cripple a health system and jeopardize patient safety. 15 percent of respondents reported a patient safety incident tied to a cyber event, and 10 percent experienced the need to divert patients to another care setting, a trend that has continued to rise in recent years.

One existing program that could be amended is the hospital preparedness program (HPP), the only source of federal funding specifically for health care delivery system readiness.[5] This program is under the U.S. Department of Health and Human Services (HHS) Office of the Assistant Secretary for Preparedness and Response (ASPR) which leads the country in preparing for, responding to, and recovering from the adverse health effects of emergencies and disasters.[6] We believe that ASPR is a natural fit given their role as the sector

[4] https://chimecentral.org/content/2021-aehis-cybersecurity-survey
[5] https://aspr.hhs.gov/HealthCareReadiness/HPP/Pages/default.aspx
[6] https://aspr.hhs.gov/Pages/Home.aspx

risk management agency (SRMA) for the HPH sector, leading the Department's cybersecurity efforts. **However, any new authorities must come with additional resources.** To our knowledge, ASPR has never received funding to help them execute on their responsibility as the SRMA which is needed to support our sector.

Our members are committed to working to improve our sector's posture and reduce cybersecurity risks; however, we cannot do this alone. Congress must work to give providers the resources, education and funding they need to ensure that our healthcare system is protected against attacks that are crippling healthcare delivery systems, risking patient lives, and undermining trust in healthcare overall.

We thank you for your efforts to improve the Nation's public health and medical preparedness and response capabilities for emergencies and appreciate the opportunity to share our recommendations. Should you have questions about our position or require additional information, please contact Cassie Ballard, Director of Congressional Affairs, at cballard@chimecentral.org.

Sincerely,

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