February 4, 2022

The Honorable Patty Murray
Chair
Committee on Health, Education, Labor, and Pensions
United States Senate
Washington, DC 20510

The Honorable Richard Burr
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate
Washington, DC 20510

Dear Chair Murray and Ranking Member Burr,

The College of Healthcare Information Management Executives (CHIME) welcomes the opportunity to provide feedback on the Prepare for and Respond to Existing Viruses, Emerging New Threats, and Pandemics Act (PREVENT Pandemics Act) draft legislation.

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. With over 5,000 members, 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.

CHIME applauds your commitment to bipartisanship and willingness to engage stakeholders. As you continue your work on building a stronger public health and medical preparedness and response system, we ask that you consider addressing the following areas that have widespread impact on the healthcare and public health sector in your final bill:

- **Cybersecurity:** cyberattacks on healthcare providers have escalated in both volume and sophistication during the COVID-19 pandemic.
- **Telehealth:** many of the current telehealth flexibilities are temporary and limited to the duration of the COVID-19 public health emergency.
- **Care Continuum**: barriers remain to information sharing across care settings.

Cybersecurity

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. A majority of breaches were due to hacking/IT incidents, including over 80% of breaches reported in December. Already in 2022, we are seeing continued active cyber activity in healthcare. Furthermore, criminals have increased their activities over the last two years taking advantage of the pandemic at a time when are 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.

CHIME and our affiliate organization, the Association for Executives in Healthcare Information Security (AEHIS), fielded a survey of its membership's chief information security officers (CISOs) 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. Additional findings are available here.

CHIME Recommendations:

The healthcare sector is only as strong as its weakest link and smaller organizations are not sufficiently resourced to fend off cyberattacks. Therefore, we propose adding language to the PREVENT Pandemics Act that would authorize the Secretary of HHS to carry out a grant program to assist small and under resourced providers to protect against, detect, respond to, or recover from cybersecurity threats. Recipients of grant funding could use the funding to adopt recognized cyber security practices such as HHS 405(d) which were recognized by Congress in H.R. 7898 signed into law on January 5, 2021,[4] replace legacy systems and devices, conduct a security risk assessment and generate an action plan for mitigating identified risks, or hire staff.

In addition, we recommend adding information security staff to the U.S. Government Accountability Office (GAO) study in Section 221 that seeks to identify existing gaps in the public health workforce. Further examination of how to improve the hiring and retention of healthcare information security professionals is needed as many hospital IT departments are under-resourced, and some do not even have a single full-time employee devoted to the oversight of cybersecurity. Often times cybersecurity personnel are not viewed as frontline or priority, when in reality they are often the first line of defense against costly and dangerous cybersecurity attacks.

Telehealth

Since the outbreak of COVID-19 began, we have heard from our members about the struggles and successes those on the front lines have experienced in fighting the pandemic. A common refrain from those members is that telehealth and the ability for patients to access care at a distance is critical to fighting this disease. Unfortunately, many

of the current telehealth flexibilities are temporary and limited to the duration of the COVID-19 public health emergency (PHE), something that must be renewed by HHS every 90 days.

CHIME Recommendation: CHIME believes the telehealth gains made in the U.S. since the start of the pandemic must continue to be supported if the healthcare system wants to remain resilient against the next pandemic. Earlier this week, CHIME, alongside more than 360 other organizations, sent a letter asking for Congress' leadership in facilitating a pathway to comprehensive permanent telehealth reform to ensure that patients continue to have access to high-quality affordable care via telehealth. Specifically, the letter asks Congress to authorize the continuation of all current telehealth waivers through December 31, 2024. The letter also asks Congress to require HHS to complete all feasible evaluations related to telehealth by fall 2023 and to combine findings into a single overarching dashboard to inform permanent, evidence-based telehealth legislation for implementation in 2024.

Care Continuum

Continually throughout the pandemic, long-term post-acute care (LTPAC) providers were left waiting for changes to rulemaking and laws to afford them the same COVID-19 flexibilities awarded to their other hospital and provider organization counterparts. This exclusion of LTPAC providers is not limited to just COVID-19 flexibilities either. Routinely, throughout the life of federal health IT policy making, LTPAC providers have been left without funding or the ability to participate in the wide-ranging health IT programs such as the ones implemented as part of the Health Information Technology and Clinical Health (HITECH) Act that was signed into law in 2009. Left on the sidelines of health technology development, LTPAC providers are unable to easily exchange health data with other provider organizations or be able to receive it. According to the HHS Office of the National Coordinator, "The ability for LTPAC providers to electronically exchange health data bi-directionally between care settings is paramount to the continuity and quality of patient care. Access to timely, comprehensive and accurate patient data allows for fully informed care decisions that improve patient safety, as well as decrease avoidable hospital readmissions, Emergency Department (ED) visits, length of stay and other adverse events."[5]

HITECH Act recipients were able to participate in programs that allowed them to offset the costs of purchasing and implementing electronic health records (EHRs) and received access to free assistance from Regional Extension Centers (RECs) to assist in speeding up the EHR adoption process. LTPAC providers and behavioral health providers, by virtue of not being able to participate in HITECH programs, did not have these benefits extended to them. As a result, most hospitals have nearly ubiquitous use of certified EHRs (96% in 2017),[6] while LTPAC EHR adoption has languished. According to 2017 data from the Office of the National Coordinator for Health Information Technology (ONC), only 78% of home health agencies and 66% of skilled nursing facilities adopted EHRs in 2017. [7]

COVID-19 highlighted just how vulnerable the entire health system is with these gaps in data sharing. As we know, nursing homes and other LTPAC facilities became the early epicenters of the pandemic with unchecked spread within the four walls of the facility contributing to numerous infections and loss of life. With better data exchange, its possible public health and other key entities would have been able to better understand and mitigate the spread of COVID-19 sooner.

As the pandemic continued and treatments for COVID-19 allowed patients to recover from the disease many more people were rapidly accessing LTPAC providers. At times this access was hindered without clear access to telehealth or access to a patient's full medical record. It meant patients struggling with COVID-19 needed to be transitioned to or from these care settings via manual processes and paper records. While many parts of the health system were able to lean on their EHR systems to bare this burden during the pandemic, LTPAC was forced to burden patients and providers with clunky outdated manual processes. If the nation wants to be prepared for the next pandemic and ensure the burden placed on the health system is not coming from bureaucratic processes because of government oversight, it is crucial for LTPAC providers to be included in all federal government health IT programs now and moving forward.

CHIME Recommendation: CHIME encourages Congress to work to provide federal funding for LTPAC and behavioral health providers to purchase and deploy certified EHRs as mature as the one's hospitals have, bringing their technology floor up to the level of other provider groups who previously received funding. This funding helps ensure LTPAC providers can participate in health information exchange and utilize technology that can help, not hinder, the U.S. health system when it responds to the next healthcare crisis.

We thank you for your efforts in preparing our nation for the next pandemic and appreciate the opportunity to share our recommendations with the Committee. Should you have any questions about our positions or if more information is needed, please contact Cassie Leonard, Director of Congressional Affairs, at cleonard@chimecentral.org.

Sincerely,

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

---

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

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

5 https://www.healthit.gov/sites/default/files/ltpac_providers_and_hie_082516_final_2.pdf

6 https://www.healthit.gov/data/quickstats/non-federal-acute-care-hospital-electronic-health-record-adoption

7 https://www.healthit.gov/sites/default/files/page/2018-11/Electronic-Health-Record-Adoption-and-Interoperability-among-U.S.-Skilled-Nursing-Facilities-and-Home-Health-Agencies-in-2017.pdf