June 20, 2018

The Honorable Michael Burgess, M.D.
Chairman, Subcommittee on Health
Committee on Energy and Commerce
United States House of Representatives
2336 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gene Green
Ranking Member, Subcommittee on Health
Committee on Energy and Commerce
United States House of Representatives
2470 Rayburn House Office Building
Washington, D.C. 20515

Re: Cybersecurity Provisions in Section 401 of the draft Reauthorization of the Pandemic All-Hazards Preparedness Act

Dear Chairman Burgess and Ranking Member Green:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to support the inclusion of the cybersecurity provisions in Section 401 of the draft Pandemic All-Hazards Preparedness Reauthorization Act of 2018. This critical legislation recognizes the importance of ensuring the nation's health systems are better prepared and able to respond in the event of a cybersecurity incident.

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. Consisting of more than 2,600 members in 51 countries, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. AEHIS members are among the nation's foremost health IT experts, including on the topic of cybersecurity. Launched by CHIME in 2014, AEHIS represents more than 850 chief information security officers (CISOs) and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members take their responsibility to protect the privacy and security of patient data and devices networked to their system very seriously.

Healthcare has entered an era of ubiquitous connection, and the internet of things (IoT) is transforming healthcare along with the world's economy. Our members continue to worry about the threats to patient care and safety that cybersecurity attacks pose. New innovations, techniques and capabilities have been introduced to improve health outcomes, but they also introduce additional risk. With this evolution, the role of the clinician is also changing; they are becoming more reliant on availability of key critical information at the moment of care.

Attacks such as Petya and WannaCry brought widespread attention to the myriad of cybersecurity vulnerabilities in the healthcare sector and demonstrated the importance of improved preparedness and rapid response in the event of an incident. Cybersecurity threats are becoming more sophisticated and can be executed by organized crime groups, terrorist organizations or other nation states who are interested in sending our country's healthcare system into disarray. Techniques can include the theft and exchange of sensitive patient information or locking up ahealth system's ability to practice medicine through ransomware and demanding payment in cryptocurrency to restore system operations/

Ensuring cybersecurity threats and the recognition of their potential to disrupt healthcare delivery should be a consideration in the next iteration of the National Health Security Strategy. As the healthcare ecosystem

continues to digitize, these threats have the potential to be as much a patient safety issue as a pandemic or natural disaster.

Of great importance to our members is the ability to improve the preparedness and respond adequately in the event of a cybersecurity incident. We applaud the Committee's proposal to amend the Public Health Service Act to include "cybersecurity" in both "Improving State and Local Public Health Security" (42 U.S.C. 247d-3a) and "Partnerships for State and Regional Preparedness to Improve Surge Capacity" (42 U.S.C. 247d-3b.) Improving the cybersecurity posture of the industry is an important, but resource intensive process. It is critical that these policy proposals be funded properly.

We appreciate the intent of the draft bill to clarify which operating division within the Department of Health and Human Services (HHS) leads the Department's cybersecurity efforts. CHIME and AEHIS believe that clarity on where cybersecurity is to be managed within HHS is vital and builds upon the directive set forth in Section 405 of the Cybersecurity Act of 2015. If it is to be managed in the Office of the Assistant Secretary for Preparedness and Response (ASPR), or by another operating division, it is essential that the office be adequately funded and staffed with the right cybersecurity expertise to match the added functionality.

CHIME and AEHIS are proud to support the inclusion of cybersecurity provisions in the Pandemic All-Hazards Preparedness Reauthorization Act of 2018. We welcome the opportunity to offer our members' perspective and we appreciate your attention to this important issue. Should you have any questions or if we can be of assistance to the Committee, please contact Leslie Krigstein, Vice President of Congressional Affairs, at lkrigstein@chimecentral.org.

Sincerely,

Cletis Earle
Chair, CHIME Board of Trustees
Vice President and CIO
Kaleida Health

Erik Decker
Chair, AEHIS Advisory Board
CISO and Chief Privacy Officer
University of Chicago Medicine

cc:
The Honorable Greg Walden, Chairman, House Committee on Energy and Commerce
The Honorable Frank Pallone, Ranking Member, House Committee on Energy and Commerce
The Honorable Susan Brooks, Member, House Committee on Energy and Commerce
The Honorable Anna Eshoo, Member, House Committee on Energy and Commerce