September 9, 2016

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to submit comment on the National Institute of Standards and Technology (NIST) Request for Information (RFI), "Information on Current and Future States of Cybersecurity in the Digital Economy," published in the *Federal Register* on August 10, 2016.

I. Executive Summary

Our thoughts and recommendations are summarized below:

1. **CHIME and AEHIS are pleased to see:**
    a. Greater attention being placed on the need to secure health information, including:
        i. Work being done by the Health Care Industry Cybersecurity Task Force, which is charged with studying and making recommendations around how the healthcare sector can better defend itself against cyber threats.
        ii. NIST's risk management framework being updated.
        iii. The Food and Drug Administration focusing more on cybersecurity.
        iv. Growing attention by C-suite executives and the federal government.

2. **We see the following barriers and challenges to protecting patient information and safety from cyberattacks:**
    a. Federal agencies need to improve transparency of known threats in order for the healthcare industry to better implement risk mitigation strategies.
    b. More actionable and plain English guidance about current threats.
    c. Since a growing number of medical devices are now connected to the internet and hospital networks, cybersecurity needs to be seen as a business issue related to patient safety, not just an Information Technology problem.
    d. Compliance:
        i. Providers need guidance for assessing threats that they can control as opposed to those that are out of their domain.
        ii. Audits by the Office for Civil Rights (OCR) are perceived as being punitive and not assisting the organization to recover and learn from a breach.
        iii. OCR should acknowledge and recognize provider efforts and investments to safeguard information and information systems when assessing the scope and magnitude of enforcement actions.

e. More help is needed for under-resourced providers.
f. More attention on maximizing protections allowed under business associates agreements (BAAs), by redistributing responsibility for security more evenly among covered entities and their business associates (BAs).
g. An effort needs to be made to reduce and or remove the financial incentive to steal healthcare information. This may include better monitoring of suspect financial transactions, as well as reducing the reliance on Social Security Numbers (SSNs) for patient identification.
h. Patient safety and patient data should be viewed as a public good; protecting those things should be viewed as national priority.
i. Cyberattacks that are highly disruptive or crippling to healthcare entities should be given the same consideration as other critical infrastructure sectors (e.g., Energy, Water, Financial Services, etc.) where federal government support and collaboration is available if requested.

II. Background

The Commission on Enhancing National Cybersecurity requests information about current and future states of cybersecurity in the digital economy. As directed by Executive Order 13718, ‘‘Commission on Enhancing National Cybersecurity’’ (the ‘‘Executive Order’’), the Commission will make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between Federal, State and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices. NIST has been tasked with providing the Commission with such expertise, services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission.”

Based on the Executive Order and the Commission’s initial deliberations, the Commission is seeking information on the following topics: Critical Infrastructure Cybersecurity, Cybersecurity Insurance, Cybersecurity Research and Development, Cybersecurity Workforce, Federal Governance, Identity and Access Management, International Markets, Internet of Things, Public Awareness and Education, and State and Local Government Cybersecurity. For the purposes of this RFI CHIME’s comments are focused on specific cyber threats facing healthcare providers and healthcare as critical infrastructure.

III. Responses to NIST’s Topics and Questions

1. Current and future trends and challenges in healthcare as critical infrastructure.

Trends

CHIME and AEHIS are pleased to see that the conversation around the need to secure health information is garnering heightened attention. The Department of Homeland Security (DHS) deems healthcare one of the nation’s 16 critical infrastructure sectors, yet, it has traditionally fallen behind several other sectors. The healthcare sector’s ability to stay ahead of threats from nation state threat actors and cyber-criminal enterprises has been challenging, especially as cyberattacks continue to advance in sophistication and persistence. This issue is further

exacerbated by the mass digitization of healthcare information making the sector an enticing target for threat actors.

The Cybersecurity Information Sharing Act of 2015 (CISA) included language specific to improving the cybersecurity preparedness of the healthcare sector. CHIME and AEHIS supported the language included in CISA, which was enacted as part of the Omnibus spending package late last year, devoting more attention to cybersecurity in healthcare. **We are especially pleased that the new law mandated creation of the Health Care Industry Cybersecurity Task Force, which is charged with studying what other industries have done do improve cybersecurity and making recommendations to the Department of Health and Human Services (HHS) for improving protections in healthcare. The task force will also look at how information can be better shared, and barriers that must be overcome.**

We also know that many – including healthcare providers – look to the NIST cybersecurity framework to assess risks and create plans for managing them. We are encouraged that NIST is updating its framework, which CHIME and AEHIS commented on earlier this year. As noted by NIST in its recent draft, "Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk." **We believe NISTs risk framework is critical and our members highlight these activities as one piece of a larger effort around risk management.**

Challenges

In terms of challenges, there are few that rise to the top in every conversation. First, as noted above, we are very pleased to see more emphasis being placed on the healthcare sector. Despite this heightened attention, our members still find daily challenges around obtaining relevant and actionable information they need to defend themselves and protect their patients. Often, the information is either hard to come by or focused on meeting technical security standards that makes healthcare providers' ability to ward off threats challenging. Further, it's our understanding that information on cyber threats is not being shared by the federal government with device and technology manufacturers.

CHIME and AEHIS members report that they receive sensitive information from the federal government and that information can only be shared with certain staff. The FBI and other federal agencies are willing to share sensitive information; however, in certain instances the information is classified and only personnel with authorized security clearances are able to access it. Once access is provided, they are not able to share this information decreasing its usefulness to mitigate cyber security threats. We understand the need to ensure the protection of classified information for national security purposes; however, the majority of healthcare entities do not have people appropriately cleared to access this information unlike other critical infrastructure sectors.

We believe it important for the federal government to sponsor, allocate, and indoctrinate healthcare entities into these information sharing programs to ensure that threat information is being appropriately shared and to educate healthcare professionals on the threat landscape. **We recognize that certain information must not fall into the wrong hands, however, our members believe that more transparency is needed in order to truly enable providers to utilize the threat information they are receiving. Additionally, much of the federal government's current guidance on cybersecurity refer providers back to the NIST framework and other documents. However, healthcare organizations, especially smaller ones, lack the necessary resources and staffing to**

fully digest the NIST guidance. Instead, they need guidance that is easier for non-security professionals to understand, such as the need for password management software. Since attacking poorly managed credentials is often the easiest entry point into a provider's system, more training on the fundamentals will reap a number of positive benefits for the entire industry. While many of our members are making substantial investments into securing their systems, it's important to recognize that small physician practices and small hospitals, including critical access facilities, do not have the resources to shield themselves and their patients against cyberattacks. Nonetheless, more information that is easily digestible by an entity of any size is needed to help shore up their systems and protect their patients; **simplicity in what information is shared from our perspective is critical.**

Despite having limited resources to deploy cybersecurity, hospitals are making substantial investments to strengthen their systems. Given the small percentage of resources within a healthcare delivery organization dedicated to information technology, more specifically security spending, (which is just a subset of the health IT budget for a health system which is generally about 3.5%), the necessity of exploring ways to encourage investment through positive incentives for those who demonstrate a minimum level of cyberattack readiness and mature information risk management programs is vital. Providers and health systems are chastised for continued increases in healthcare costs, but security investments are not currently accounted for in traditional reimbursement mechanisms in an environment that is becoming more vulnerable by the day. The Administration should examine how meeting a minimum security threshold could be included in a value-based reimbursement calculation.

Hospitals are attempting to make investments in security while federal Meaningful Use standards and changes in reimbursement and care models are forcing them to significantly upgrade their data analytics and clinical systems. Driving better and more coordinated care will rely increasingly on a highly digitized environment where information is broadly shared, which also increases the risk surface for organizations to protect as well as increasing opportunities for cyber criminals. Unfortunately, little effort is being made to help providers navigate current threats. **Providers must receive credit for the investments they are making to secure patient information and increase patient safety. From our perspective, cybersecurity is not just about securing patient information – it is about making sure patients are safe.**

Finally, compliance is a continual challenge for our members. We understand that many in the federal government perceive healthcare providers as being behind in terms of cyber readiness. Yet, as noted above, many healthcare providers are working hard and investing substantially to protect patients and their information and there is a concern that these investments are not widely recognized. Providers feel challenged in two ways. **First, they have a hard time distinguishing whether they have done enough from a compliance standpoint.** Even with OCR desktop audits and resolution agreements, and updates from the Office of the National Coordinator for Health IT (ONC), it is still unclear to providers how much "is enough?". Providers are left with the impression that what they are doing is enough until they are breached and it was retroactively determined that they were at fault. This concern may push providers to look to ensure compliance without considering the bigger security orientation which is to manage risk. **Second, they report feeling "victimized" twice, once if they are successfully attacked; and again when audited by OCR.**

We recognize that because healthcare providers vary in size, complexity, and setting, it's hard to have a universal set of rules for managing risk in every situation. Nonetheless, we believe that there is a fundamental difference between negligence (i.e. leaving a laptop in car that is stolen or ignoring an ongoing well-known risk) and engaging in good cyber hygiene practices. Moreover, we do not believe penalties in these cases help better protect patients

and providers. **Therefore, we believe that compliance must be viewed through the lens of what an organization can control versus what is outside of its control.**

2. Progress being made to address the challenges.

Though much work remains, cybersecurity awareness and action is accelerating in the healthcare sector. This is indicated in the work underway at:

- NIST, which is updating its cybersecurity risk framework;
- The Food and Drug Administration's work around device security, which places more attention on the vendors, which is of paramount interest to our members;
- Passage of CISA and the work underway through the HHS Cybersecurity Taskforce which will culminate in a report to Congress early next year; and
- OCR's recently published guidance on ransomware that signals greater attention to cybersecurity.

3. The most promising approaches to addressing the challenges.

One of the most promising developments in addressing cybersecurity challenges in healthcare is the growing attention in the C-Suite. Increasingly, executives and boards are paying closer attention to these issues and the need to make investments in staffing and technology. Still, as noted above, there are limitations, especially for small physician practices and small and rural hospitals. Shrinking reimbursements impact how and where hospitals can allocate resources.

4. What can or should be done now or within the next 1–2 years to better address the challenges.

More help is needed for under-resourced providers. While our members report threat sharing services to be incredibly valuable tools in helping them combat cyber threats, many smaller providers need help understanding and prioritizing top threats since they cannot afford many of these services. Also, as noted earlier, there needs to be a distinction made between a risk-based approach to those items under the control of a provider versus things that are outside their control.

Additionally, we also believe that consideration should be given to what goes into BAAs. From a security standpoint, we believe consideration should be given to establishing a new level of the security framework that a BAs are presently using. Our members report that the variability and the details of these agreements vary widely, making it extremely difficult to negotiate individual agreements. This variability, and the large number of agreements, increase the challenges in auditing BA compliance with such regulations as HIPAA Security Rule 45 CFR part 164. Increasingly, organizations feel responsible for this type of audit on selected agreements in order to best assure that their business partner is performing appropriate due diligence related to cyber security. **Therefore, we believe more attention must be paid to the influence of certain BAs over providers.** Our members report that many manufacturers and third parties refuse to sign contracts where language places appropriate responsibility for ensuring products / devices are secure. The responsibility for securing patient data and protecting against cyber

threats cannot be borne by providers alone. Rather, we believe this must be a shared responsibility. Yet, our members frequently find that protections offered under HIPAA are erased in contracts and they are left with no other option than to sign a BAA that relieves the BA of certain responsibilities. Frequently, providers opt to sign a contract that leaves them with sole responsibility for managing security – even when some aspects are outside of their control -- in order to acquire and provide life-saving technologies to their patients. In the end, our members frequently feel they need to choose patient outcome needs over security.

5. **What should be done over the next decade to better address the challenges.**

As discussed earlier, we believe that increased collaboration from the federal government will go a long way in helping providers of all sizes effectively manage risk. We continue to have concerns that necessary threat intelligence is not making its way down to providers or vendors that could be used to defend their organizations from threats originating in cyberspace.

6. **Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.**

One major challenge that needs to be addressed is paying more attention to managing electronic transactions and removing the incentive from those intent on causing harm from taking patient data. Today, this data is being stolen to file false claims, obtain credit cards using others' identities, and perpetuate other forms of healthcare fraud. To the degree that illegal payments can be stopped or slowed down, then the incentive to steal patient information will be removed or reduced. Thus, we believe this issue and possible solutions merit further study.

SSNs continue to hold a tremendous amount of value. **Reducing the reliance on SSNs and other identifiable information that help threat actors execute fraud will immediately devalue health records on the black market.** We need a healthcare identification solution that, if stolen, does not have the same potential for fraud and abuse.

7. **Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.**

Healthcare is increasingly becoming more interconnected. Consumers are using digital devices to monitor their steps, heartrate, and other vital signs. Also, in the future, many healthcare providers will be encouraged and/or required to accept patient-generated data and connect patients' apps to their electronic health records (EHRs) through application programming interfaces (APIs). This opens up the healthcare system to new and emerging vulnerabilities that can be used to access and potentially modify patient information, conduct a ransomware attack to hold an organization hostage or, at worst, lead to patient harm. The number of possible "tunnels" or entry points will scale well beyond the four walls of a hospital and will comprise an elaborate labyrinth of interconnectivity that will include mobile devices as well as devices in the home.

Finally, the focus on precision medicine will also open new doors of interest to nation states and criminals who are eager to exploit the rich data sets that are being aggregated for the purposes of stealing intellectual property (IP) and which present a treasure trove of life science data.

8. Economic and other incentives for enhancing cybersecurity.

See response to question 6 above.

9. Government-private sector coordination and cooperation on cybersecurity.

As noted earlier, we believe increased transparency by the federal government to providers and vendors / manufacturers will help mitigate some threats. Also, we believe threat information that is communicated more plainly will also better protect providers from threats.

10. The role(s) of the government in enhancing cybersecurity for the private sector.

We believe that protecting patients and their information should be a national priority and a public good. Just as the federal government works to protect the nation from military threats, we believe it should treat cyber threats with the same attention. We also believe that educating the American people more about cyber threats and how they can reduce the chances of falling victim or opening the healthcare system up to threats is necessary. Things as simple as increasing awareness around the security of wearables could be helpful.

Additionally, we believe that cyber liability insurance can be critical, though the costs to have it are high. Our members who do have cyber insurance say it can help mitigate the costs of breach notification, response and credit monitoring; however, many insurance policies simply are not enough to mitigate the costs that are incurred during a breach and those associated with class action lawsuits or feature exclusions that against nation state attacks that may in effect nullify the policy's intended value. Members also report that policies are oftentimes written such that an event is excluded from coverage due to the judgment of the insurer that the provider has not taken adequate steps to protect itself from harm and that these judgments are frequently arbitrary and not standards-based. We believe the federal government needs to examine cyber insurance policies more closely and review what it covers, where it leaves off and what might be done to mitigate damage by the federal government. For example, this should function similarly to the Department of Homeland Security, Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, which provides incentives for the development and deployment of anti-terrorism technologies by creating systems of risk and litigation management. Similar thoughts and approaches should be considered for the healthcare sector to provide indemnifications and protections for providers that are exercising appropriate due diligence and investments to safeguard their information and information systems.

IV. Conclusion

CHIME and AEHIS appreciate the opportunity to offer our feedback on this RFI and stand ready to engage in an ongoing dialogue with the Administration on any of the topics discussed in our letter and the broader state of healthcare cybersecurity. Should you have any questions or need additional information please contact Mari Savickis, Vice President of federal affairs at msavickis@chimecentral.org.

Sincerely,

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Marc Probst, CHCIO
Chair, CHIME Board of Trustees
CIO, Intermountain Healthcare

Deborah Stevens
Chair, AEHIS Board of Trustees
CSO, Tufts Health Plan