Statement from the College of Healthcare Information Management Executives and the Association for Executives in Healthcare Information Security

Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

Hearing on "Ransomware: Understanding the Threat and Exploring Solutions"

326 Dirksen Senate Office Building

May 18, 2016

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to submit a statement for the record of the May 18, 2016, Committee on the Judiciary Subcommittee on Crime and Terrorism hearing entitled, "Ransomware: Understanding the Threat and Exploring Solutions." We appreciate the committee's interest in this timely issue and welcome the opportunity to offer perspective from the nation's healthcare chief information officers and chief information security officers.

CHIME is an executive organization serving nearly 1,900 CIOs and other senior health information technology leaders at hospitals and clinics across the nation. CHIME members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. CHIME members are among the nation's foremost health IT experts including cybersecurity. Within CHIME is AEHIS, an organization launched in 2014 which represents more than 500 chief information security officers (CISOs) and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members take very seriously their responsibility to protect the privacy and security of patient data and devices networked to their systems.

Cybersecurity in the Healthcare Industry
The Department of Homeland Security deems healthcare one of the nation's 16 critical infrastructure sectors. Already highly-regulated, healthcare organizations are subject to divergent and duplicative guidance on data security and privacy by various federal entities, state regulators and business agreements. Through market pressures and regulatory requirements, including Meaningful Use and the shift to alternative payment models, CIOs and CISOs must transform their healthcare systems to become digital enterprises. This includes trying to balance the need for enabling providers with the capability for having immediate access to electronic protected health information (ePHI), while at the same time maintaining strict cybersecurity protocols.

This digitization of personal health information and the sharing of data encouraged by the Medicare and Medicaid EHR Incentive Program, has led to an increase in the number and types of cyber threats facing healthcare providers. Meanwhile, providers with very limited resources struggle to balance the huge demands for cybersecurity technology and information risk management programs. Threats to healthcare organizations are growing more sophisticated every day and too many health systems are not properly equipped to combat the myriad of attacks that could penetrate their networks. Even the largest healthcare delivery organizations, with the greatest investment in security programs, may still fall victim to bad actors as we have seen with some of the largest retail organizations, financial institutions and even the federal government suffering large-scale breaches. No industry can enable perfect security; rather the organizations must enumerate and manage their risks. The healthcare organization and IT security teams are challenged with understanding every avenue of attack by which a hacker

might gain access to the healthcare network, whereby the hacker only needs to find and exploit one weakness. In many cases, that one weakness is preying upon the behaviors of individuals through social engineering. As many studies have shown, and as many organizations that conduct penetration tests and other social engineering assessments will attest, it is impossible to prevent every human being in an organization from falling prey to such an attack.

There are several unique distinctions of the healthcare sector's data security environment that warrant consideration, including:

- Healthcare's highly-regulated environment
- The various settings where healthcare is delivered
- The range of resources available to devote to information technology and security
- Healthcare's unique financial models
- Frequency and volume of data exchange within healthcare delivery
- The increasingly mobile nature of healthcare technology and healthcare delivery

The recent spate of publically reported ransomware attacks has put healthcare in the national spotlight. Ransomware has become so commonplace that it was cited as a top new threat for 2016 in the Ponemon Institute report, "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data." To illustrate the ferocity of the bad actors, the CIO of a large East Coast, multibillion-dollar health system turned away more than one million ransomware-ridden emails during the month of March alone.

Ransomware vs. Other Threats

While ransomware is the topic of the day, it's important to take a step back and remember that it is only a subset of the broader cybersecurity threats facing the industry. Additionally, it is important to note that ransomware is just a subset of malware in general, and has been a threat to all industries for over 10 years. The surge in its current effectiveness is most likely entirely attributed to digital and untraceable currencies such as BitCoin. These currencies allow for an anonymous financial transaction which protects the criminal from financial forensic investigations by the Federal Bureau of Investigation (FBI) and other law enforcement entities.

For the second year in a row, criminal attacks were cited as the top cause of data breaches in the healthcare industry, with 50 percent of the breaches resulting from a criminal attack and 13 percent due to a malicious insider.[1] CIOs and CISOs face countless other malicious malware attacks on a daily basis, including Trojans, viruses, worms, and more. New threats will continue to arise, some can be anticipated while others will not, thus the notion of zero-day threats. Ransoming the data held by an organization is only one example of a goal for a system intrusion. The primary motive of these types of criminals is economic in nature, and it is this untraceable transaction that enables the threat. Today it is ransomware that is the delivery mechanism, tomorrow it could be something else entirely. There can be other goals of intrusions that impact system availability. These other goals may be to make systems generally unavailable such as a denial of service attack (DOS).

CHIME and AEHIS members point to inconsistencies in the enforcement of the laws governing privacy and security as a major impediment to being able to implement sound risk mitigation strategies. The existing enforcement paradigm is heavily focused on compliance with maintaining patient privacy, which can be a distraction or drain on already limited resources necessary to actually secure the numerous points of entry – medical devices, networks, EHRs. Variability in expectations of those that interact with healthcare data, including medical device manufacturers and business associates, will only contribute to the difficultly in securing each and every potential vulnerability.

Device manufacturers, for example, are not Health Insurance Portability and Accountability Act (HIPAA) covered entities, and CIOs and CISOs often describe scenarios in which medical devices are deployed with default passwords, some of which are unable to be changed by the providers, that can be easily penetrated by bad actors, potentially threatening the functionality and safety of the device. In other instances, inadequate technical controls exist to protect the medical devices that are already deployed. Additionally, some medical devices operate on private networks, not controlled by the providers, creating large holes in perimeters and firewalls. CHIME and AEHIS recommended in recent comments to the Food and Drug Administration (FDA) that enhanced collaboration between device manufacturers and healthcare delivery organizations is necessary, and that the FDA approval of

[1] *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (Rep. No. 6). (2016, May 12). Retrieved May 12, 2016, from Ponemon Institute LLC website: http://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1

high-risk devices should include an assurance that the data collected and shared by the device is secure and the device is not an easy entry point to a health system's network, as has been proven to be the case today.[2]

Healthcare records are rich with personal information that enable bad actors to execute identity theft and fraud with the information mined from the industry. Unfortunately, organization's must often request a patient's Social Security number (SSN) to use as an identifier as the patient moves through the treatment continuum. CHIME is a leading advocate for improving patient identification to not only minimize security risks, but to also improve patient safety and quality of care. Reducing the use of such personally identifiable information as SSNs is essential for decreasing the value of health records for bad actors. Knowing that we have the right patient matched with the right information is the first step toward effectively protecting and securing identities and mitigating fraud, which is a key driver of CHIME's National Patient ID Challenge, a $1 million global competition aimed at incentivizing innovators to accelerate the creation and adoption of a solution for ensuring 100 percent accuracy in identifying patients with their healthcare records in the United States.

Improving Security of the Industry

To better safeguard healthcare systems, we must improve threat and incident information sharing across the industry. No single sector of the healthcare ecosystem can solve the problem alone. Only by pulling together and sharing best practices can we thwart cyber criminals and protect patients. This type of collaboration is vital towards remaining nimble to the threats of today, for every day a new threat is introduced into the industry. Today it is ransoming an institutions data or operations, tomorrow it could be holding hostage the ability to deliver care through medical devices. The vehicle by which the threat is delivered will change, but we know for a fact that criminals will look at introducing "new markets" for extorting money above and beyond what they are doing today.

CHIME and AEHIS are pleased with the important advances recommended in the Cybersecurity Information Sharing Act of 2015. The healthcare-specific directives, particularly the cyber resources that are to be scalable to the entire industry and the coordination plan across the Department of Health and Human Services (HHS) will be important to move the industry forward. In addition, discussions and clarification on what Information Sharing Analytics Organizations (ISAO) can and cannot share will be very beneficial. Many ISAO participants are concerned about minimum necessary and appropriate use guidelines in a CISA/ISAO environment.

Further, we have seen proactive initiatives from the administration, including efforts to evaluate needed enhancements to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, a crosswalk of HIPAA to the NIST Framework and draft guidance from FDA on the post-market cybersecurity management of medical devices. It will be imperative for the industry to work in conjunction with the administration and Congress to ensure healthcare providers are best positioned to combat cyber threats.

CHIME and AEHIS offer some suggestions for lawmakers to consider as the sector matures in its efforts to improve cyber hygiene and fight bad actors:

- Enabling the Use of a Healthcare-Specific Identification Solution – Reducing the reliance on SSNs and other identifiable information that help bad actors execute fraud will immediately devalue health records on the black market. The need for a healthcare identification solution, that if stolen does not have the same potential for fraud and abuse, is essential, thus Congress should remove the language in the Labor-HHS Appropriations bill that prohibits HHS (in Sec. 510) from using any federal funds to "*promulgate or adopt any final standard …. providing for the assignment of a unique health identifier for an individual*." Technology has provided for alternatives to a numeric or alphanumeric identifier as a solution, and the government does not need to be the arbiter of the identification solution, but HHS must be able to provide technical assistance to private sector initiatives. Unfortunately, HHS has interpreted the annual funding ban to prohibit them from collaborating or assisting with private sector efforts to improve patient identification on a national level.
- Incentives for Security - Given the low degree of spending/resources for IT spending and security spending in particular (which is just a subset of the health IT budget for a health system which is generally about 3.5%), policymakers should look for ways to encourage investment through positive incentives for those who demonstrate a minimum level of cyberattack readiness and mature information risk management programs.

[2] *Postmarket Management of Cybersecurity in Medical Device* [Letter sent April 21, 2016 to R. Califf, Commissioner, Food and Drug Administration]. Retrieved from https://chimecentral.org/wp-content/uploads/2014/11/CHIME-AEHIS-Letter-to-FDA-on-Device-Cyber.pdf

- Security as Factor in Reimbursement - CMS currently employs value-based reimbursement modifiers; Congress should allow CMS to consider a similar principle to be applied to healthcare enterprises investing in security. Similarly, improving an organization's cybersecurity readiness should be considered a recognized activity under the Clinical Practice Improvement performance category under the Medicare Access and CHIP Reauthorization Act Merit-based Incentive Payment System (MIPS) reimbursement scheme.
- Reduce Regulatory Complexity - Congress should pursue legislation that harmonizes other privacy, security and information risk management requirements to eliminate the complex patchwork of regulations across industries and state lines. Currently healthcare organizations dedicate highly valuable resources on navigating these complexities to demonstrate compliance with its regulators; if a streamlined regulatory framework were in place these resources could focus more time on actively monitoring and protecting against the daily variable threats.
- Workforce Development Programs - Policymakers should support ways to develop security experts to address both cyber concerns and general information security challenges. A Workforce Development Program, that focuses on healthcare cybersecurity, could leverage community colleges and professional certification programs to develop a skilled workforce to combat ongoing workforce shortages in healthcare information security.

As the committee continues to evaluate the cyber threat landscape, we urge members to ensure healthcare providers face a reasonable and predictable regulatory environment that can allow them to focus on adopting industry-best security practices, rather than taking a check-the-box compliance approach. A more proactive policy management process is vital for healthcare organizations to keep pace with these variable threats. A secure healthcare system will ultimately enable greater consumer confidence and will spur better care coordination, enhanced information exchange and improved patient care.