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

House Committee on Energy and Commerce
Subcommittee on Communications and Technology and Subcommittee on Commerce, Manufacturing and Trade

Hearing on "*Understanding the Role of Connected Devices in Recent Cyber Attacks*"

2322 Rayburn House Office Building

November 16, 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 November 16, 2016, Committee on Energy and Commerce joint hearing with the Subcommittee on Communications and Technology and the Subcommittee on Commerce, Manufacturing and Trade entitled, "Understanding the Role of Connected Devices in Recent Cyber Attacks." 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 more than 2,000 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 600 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 both 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 have been working feverishly over the past decade to 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.

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
- Limited 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

Healthcare has entered an era of ubiquitous connection, and the internet of things (IoT) is transforming healthcare along with the world's economy. Just in healthcare alone, the growth of IoT connections from 2014 to 2015 increased by 26 percent.[1] Smart devices at the point of care (i.e. heart monitors, infusion pumps, fitness trackers) and throughout the entire healthcare system (i.e. smart toasters and vending machines), are often connected to the same broader network. Wearables and additional devices are being connect to electronic health record (EHR) systems, which generates additional data for clinical decision making but also increases the threat surface with the addition of yet another device. Patient records are accessed remotely on clinician laptops and are stored in the cloud, which introduces another realm of security threats. The lines between commercial consumer devices and medical devices are blurring rapidly, thus it is vital to view the recent cyber attacks holistically and recognize the importance of coordination across all critical infrastructure sectors.

Much of the attention in healthcare when it comes to cybersecurity is centered on data breaches and threats to patient information. Unfortunately, medical devices also present and expand threat attack surfaces, as these devices can be directly connected or implanted in a patient. Often, these devices are connected to the hospital network and upload vital information to electronic health records. Medical device vendors use the internet to link to their machines to install updates or patches. Unfortunately, weak security protocols make medical devices prime candidates for us in distributed denial of service (DDoS) attacks like that on Dyn. These attacks can be extremely detrimental and have grave consequences on patient care.

Networked Medical Devices

Tens-of-thousands of medical devices can be used throughout large healthcare systems, many of which, as stated above, are connected directly to the patient or serving to provide information to inform clinical decision making. The lifecycle of a medical device within a healthcare institution can be lengthy as the cost to replace them can be crippling. Given the intent to employ devices for upwards of 10 to 15 years, many of the devices in place today were not developed or intended to be networked, yet the U.S. Chamber of Commerce Technology Engagement Center/ Morning Consult survey says 61% of respondents believe that in the near future it will be "important" or "somewhat important" that medical devices that monitor your heart rate to be connected to the internet.[2] Given the consumer expectations about devices being networked, we must ensure proper security management, including thorough risk assessments and risk treatment, are incorporated in the device's design. Meanwhile, wearables and remote monitoring technologies are on the uptick making blurring the links between what are strictly consumer devices and what is a medical device. As more connected devices enter the healthcare realm, additional attack surfaces and vulnerabilities become available to bad actors.

The highly interconnected nature of medical devices, combined with the constraints of inconsistent patching cycles, has created an ecosystem ripe with technical vulnerabilities that cannot be managed with standard processes and procedures. Some examples of existing challenges posed by networked medical devices within healthcare delivery organizations include:

- Medical devices are being released into the marketplace often without basic security requirements in place such as: encryption, access control mechanisms, passwords that can be changed by healthcare organizations, and the ability to restrict access controls.
- Known vulnerabilities within medical devices cannot be patched or mitigated in a timely manner due to the requirement that device manufacturers follow extensive quality control processes. Additionally, in many cases it is not possible to patch a device without first investing in an upgrade to newer versions, and threats of device warranties being voided if patches are done by the healthcare provider. Upgrades can be quite costly and usually require long planning cycles in order to secure the correct budget. Purchasing new equipment to remediate security vulnerabilities is not always the best or most realistic answer for the healthcare industry.
- Medical devices are increasing their storage capacities, which potentially increases the amount of patient data stored on these devices. This creates significant risk to patient privacy and compliance challenges with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH).
- There are no expiration dates on Food and Drug Administration (FDA) pre-market approvals for medical IT devices despite medical device manufacturer and FDA knowledge of end of support dates for major operating systems.

The FDA has increased its focus on the critical issues surrounding cybersecurity of medical devices and their impact on patient safety. From a healthcare provider perspective, the ever increasing interconnectedness of

---

[1] *State of the Market: Internet of Things 2016,* https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf

[2] *Internet of Things, Most Americans Don't Know What Caused Recent Internet Outages,* http://ctecintelligence.com/

medical devices into a health systems operating network has become an area of great concern. We believe an increased and formalized collaboration between the medical device manufacturers and healthcare organizations is critical. For several decades, there has been a tension between the identification of medical device vulnerabilities and the device manufacturer's capability to mitigate or manage those risks. Generally speaking, when a device vulnerability is discovered or enumerated, these vulnerabilities cannot be easily rectified due to costly quality control mechanisms, such as 21 CFR Section 806.

This has become even more of a problem as general operating systems, such as Microsoft Windows, are considered integral components of the medical device architecture and must be managed through these same quality control mechanisms. Security vulnerabilities resulting from these types of operating systems are occurring at a much higher frequency than manufacturers can resolve. CIOs and CISOs are generally left with managing devices on isolated and segregated networks with the hopes of reducing their exposure to threats. This, however, has proven to be ineffective.

Improving Security of Networked Medical Devices

To better safeguard healthcare systems and the patient data they have been entrusted to protect, 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 as dictated by HIPAA 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.

The recent spate of publically reported networked medical device vulnerabilities disclosed by security researchers has garnered attention from patients, providers and most recently lawmakers[3]. With the changes finalized by the U.S. Copyright Office of the Library of Congress in October 2015, which contained several exemptions to the Digital Millennium Copyright Act, including expanded access to medical device computer programs and the patient data they generate, it is anticipated to that the detection of new device vulnerabilities will increase.

CHIME and AEHIS offer some suggestions for consideration as the sector matures in its efforts to improve the cyber hygiene of networked medical devices:

1. Signal that the security of a device must be considered when evaluating the safety and efficacy of its performance. In conjunction with the FDA, Congress should ensure that manufacturers configure their devices according to an industry accepted security standard that accounts for the basic principles of cybersecurity controls and alleviates risks. Manufacturers should, as part of the pre-market approval process, be required to undergo a level of security validation in order to provide healthcare providers with a very simple and easy to implement mechanism for managing its security.
2. Ensure that the FDA is able to oversee vulnerability submissions and notification of risks to providers, as all known device risks should be reported to the healthcare delivery organizations that own said devices. "Controlled" risks should be reported on a regular basis (i.e. quarterly) and "uncontrolled" risks on an immediate basis. The definition of controlled vs. uncontrolled risks should encompass both patient safety and patient privacy issues. Cybersecurity risks in the medical device space should be classified either as "risks to patient safety" or "risks to patient privacy" to provide a more holistic view of the cybersecurity ecosystem.

[3] *Letter from Representatives Diana DeGetter and Susan Brooks to FDA Commissioner Califf and CDRH Director Shuren, November 3, 2016*

3. Support the expansion of programs similar to the NIS National Cybersecurity Center of Excellence (NCCoE)'s work to investigate how to improve the wireless intravenous (IV) medical infusion pump security by focusing on device security risk assessment and risk management.

As the committee continues to evaluate the cyber threat landscape, we urge members to ensure that networked medical devices factor into the broader conversation of consumer-facing devices that could be leveraged in a denial of service cyber-attack or manipulated to cause harm to patients. A more proactive policy management process is vital for healthcare organizations. Viewing security as a component of safety and efficacy of device functions is necessary 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.