Testimony before the United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Health

Hearing on "Examining the Reauthorization of the Pandemic and All-Hazards Preparedness Act"

2123 Rayburn Office Building

June 6, 2018

Statement of Erik Decker

Chief Security and Privacy Officer, University of Chicago Medicine

Advisory Board Chairman, Association for Executives in Healthcare Information Security

Industry Co-Chair, Cybersecurity Act of 2015 Section 405(d) Task Group on Aligning

Cybersecurity Best Practices to the Health and Public Health Sector

Summary of Testimony

Thank you, Chairman Burgess, Ranking Member Green and members of the subcommittee. It is an honor to testify on behalf of the Association for Executives in Healthcare Information Security (AEHIS), concerning the reauthorization of the Pandemic and All-Hazards Preparedness Act (PAHPA.)

Speaking on behalf of my colleagues, we support the reauthorization of the Pandemic and All-Hazards Preparedness Reauthorization Act of 2018. I appreciate the opportunity to discuss the need for maturing healthcare's cybersecurity resiliency and response across our nation.. We believe it is imperative that we continue to establish, modernize and mature the industry's resilience, and response, to these evolving cybersecurity threats. Specifically, we feel this reauthorization of PAHPA will address the following challenges:

1. The digital transformation of the healthcare industry that requires complicated technical platforms to achieve desired clinical outcomes;
2. The identification of modern day cybersecurity threats, and how these threats can cause significant harm to the Healthcare and Public Health Sector, and this digital platform;
3. The need for maturation of cybersecurity resiliency and capability within the industry, specifically relating to cyber programs and medical device security;
4. By leveraging ASPR as the Sector Specific Agency, encourage the coordination and deconfliction of best practices, guidance and enforcement expectations amongst the various U.S. Department of Health and Human Services (HHS) operating divisions such as OCR, FDA, CMS, and ONC; and
5. The need for further incentivization to the industry for adopting cybersecurity best practices.

Testimony

Witness Background

AEHIS is an organization that represents more than 850 Chief Information Security Officers (CISOs). Launched in 2014 under the auspices of the College of Healthcare Information Management Executives (CHIME), AEHIS provides education and professional development for senior IT security leaders in healthcare. CHIME and AEHIS members, the nation's Chief Information Officers and Chief Information Security Officers, take very seriously their responsibility to protect the privacy and security of patient data and devices networked to their systems.

In addition to serving as chairman of the AEHIS Advisory Board, I am the Chief Security and Privacy Officer at the University of Chicago Medicine. UChicago Medicine is an academic health system based in Chicago whose tripartite mission involves providing medical care to patients and the community, educating and training the next generation of physicians, and advancing medicine through innovation and scientific research.

Lastly, I serve as the co-chair and industry lead for the joint Healthcare Sector Coordinating Council (HSCC) and Government Coordinating Council (GCC) Task Group formed to improve cybersecurity in the Healthcare and Public Health sector, as required under the Cybersecurity Act of 2015 405(d) [1].

[1] *https://www.congress.gov/bill/114th-congress/senate-bill/754*

Current State of Digital Health

The healthcare industry is undergoing significant digital modernization and with that the methods clinicians practice medicine is changing. New innovations, techniques and capabilities have been introduced to improve health outcomes, such as precision medicine, digital health strategies, telemedicine and continued development of clinical decision support processes. 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.

This critical information is presented through the use of new technology platforms. As the healthcare professional has specialized, so are the technology stacks that support them. From primary to quaternary care, no longer are there single monolithic systems that provide support for all aspects of the healthcare system. Today in healthcare there are large teams that directly support the patient through diagnostic, therapeutic, revenue cycle and care management services. Indirectly, operational teams support the clinicians and the system’s ability to operate, such as supply chains, operations, legal, environmental and patient transport services, clinical/biomedical engineering and of course information technology.

The modern healthcare system is hyper connected to support these healthcare models. From traditional technologies such as electronic health records, revenue cycle, imaging systems and enterprise resources planning (ERP) to the connected medical devices, specialty applications, and the cloud, all of these systems are involved in the care for the patient. Additionally, providers must be able to interoperate and share common patient information between various care providers, through health exchanges. There is increasing reliance on these data being available, and confidential, to support these nuanced clinical workflows. With the adoption of this technology, the technical ecosystem has exploded in complexity.

Current State of Cybersecurity Threats;

The healthcare industry has faced threats to the privacy of our patients' data since the inception of digital systems. In the recent past, these threats have evolved to include additional targets, namely the threats disrupting these highly interconnected digital systems and extorting the organization through ransom, and the threats to patient safety introduced through vulnerabilities in connected medical devices. Within the last year the healthcare industry has faced some significant cybersecurity attacks. Attacks like WannaCry in May of 2017 have demonstrated the necessity to being prepared for a national cybersecurity attack against our healthcare industry. The digitization of personal health information and the sharing of data encouraged by the Medicare and Medicaid EHR Incentive Program, has also led to an increase in the number and types of cybersecurity threats facing healthcare providers. Meanwhile, providers with limited resources, struggle to balance the ever-increasing demands for cybersecurity and information risk management programs.

One facet to the increase in cybersecurity attacks are due to introduction of new types of attackers. The sophistication of these attackers has dramatically shifted over the last several years, such as:

- organized crime has developed underground markets and exchanges of sensitive information and services (such as 'Hacking-as-a-Service'),

- sophisticated hacking groups who determined how to encrypt and lock up a systems digital environment and hold it for ransom,
- terrorist organizations who have a willingness to cause disruption and harm, and
- nation states interested on the theft of intellectual property for national economic advantages.

We can no longer think of preparedness relative only to natural disasters or pandemics; it's imperative that we acknowledge the criticality of cybersecurity threats levied against the nation's healthcare system.

Public-Private Collaboration

Many healthcare providers are under-resourced and need assistance navigating this new threat environment. Even those organizations who are better resourced can find the threat environment challenging. Therefore, many healthcare organizations look to their partners in the federal government for guidance to enhance preparedness and seek assistance in the event of an incident.

When the industry experienced the wide-scale attacks known as "WannaCry", the Department of Health and Human Services (HHS) acted rapidly. This response was spearheaded by the ASPR and the Healthcare Cybersecurity and Communications Integration Center (HCCIC.) The HCCIC rapidly disseminated information about the world-wide threats and hosted calls often lasting several hours open to the industry for the purpose of information sharing. The speed at which HHS acted and their inclusive approach of healthcare delivery organizations of all types and sizes should be commended. However, the HCCIC has since been the source of confusion for providers. Specifically, confusion exists regarding the purpose of the HCCIC, the Department of Homeland Security (DHS) run National Cybersecurity and Communications Integration Center (NCCIC), and the existing industry Information Sharing and Advisory Centers (ISACs) and Information Sharing and Advisory Organizations (ISAOs).

The passage of the Cybersecurity Act of 2015[2] in December 2015, specifically the inclusion of section 405, marked Congressional recognition of the need to evaluate and enhance the cybersecurity posture of the healthcare industry, something strongly supported by our members.

Within section 405, provision (d) instructed HHS and industry to “align health care industry security approaches” and develop “a common set of voluntary, consensus based, and industry-led guidelines, best practices, methodologies, procedures, and processes,” that are scalable and cost-effectively reduce risks for a range of healthcare organizations. In May of 2017, the so-called 405(d) task group was formed consisting of over 100 industry and government experts. The membership of this task group covers a large spectrum of our industry, from small practice providers, to large health system chief security officers, as well as a contingent of government agency representation from within HHS, DHS and the National Institute of Standards and Technology (NIST.)

As co-lead of this task group, I am please to report we have developed a series of cybersecurity best practices for small, medium and large healthcare organizations which will help mitigate the top cybersecurity threats we face today. We expect to provide the best practices to the Secretary

[2] *https://docs.house.gov/billsthisweek/20151214/CPRT-114-HPRT-RU00-SAHR2029-AMNT1final.pdf*

for dissemination to the industry before the end of 2018. This effort has been a fantastic example of public-private partnerships and what is possible with an inclusive approach, leveraging the expertise of representatives from across the industry, with the backing of the federal government.

A separate directive from the Cybersecurity Act of 2015 was a mandate for HHS to issue a clear statement defining “the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry.” Today, AEHIS members cite confusion about who leads HHS’ cybersecurity programs and the correct way to communicate with the Department concerning cybersecurity-related issues. Additionally, AEHIS members cite concern about sharing information that might elicit an enforcement action from the regulatory arm of HHS. However, in this modern age of cybersecurity attacks, the need to share this information is vital for protecting our industry. We feel PAHPA clarifies the intent of creating a Sector Specific Agency that can work proactively and reactively with the Healthcare industry and help to coordinate and deconflict issues relating to regulation, guidance and best practices issued by the various HHS operating divisions. By example, having an impartial agency, such as ASPR, coordinate the intersection of cybersecurity challenges relating to medical devices and two regulatory bodies (FDA and OCR) would be incredibly beneficial for the industry. Navigating the guidance gaps and intersections today hinders the ability for industry to be nimble at its protection and response.

We agree that cybersecurity threats are just another type of hazard that must be managed. As such, we feel ASPR is well situated to be the appropriate operating division to coordinate these necessary national responses, as well as interfacing with regional and local public health departments as necessary, in the event of such a large-scale cybersecurity event. We do believe for ASPR to be successful in preparedness and response that specific cybersecurity expertise will be necessary, as well as the supporting financial resources.

These efforts should not duplicate existing successful industry practices, such as information sharing which should continue through the information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs). The ISACs and ISAOs are the preferred method for disseminating and sharing technically relevant cybersecurity threat and mitigation details. We believe ASPR, HCCIC or NCCIC, with the right authority, would be well suited for coordinating activities and leveraging existing resources, as needed.

Medical Devices

Given 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 safety the cybersecurity attacks pose. Tens of thousands of medical devices can be used throughout large healthcare systems, many of which are connected directly to the patient or serving to provide information to inform clinical decision making. Wearables and medical devices are being directly connected to electronic health record (EHR) systems, which generates additional data for clinical decision making but also increases the threat surface. Just in healthcare alone, the growth of IoT connections from 2014 to 2015 increased by 26 percent.[3]

[3] *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*

And, since a typical hospital bed has between 10-15 devices connected to it, the footprint to infiltrate a healthcare system and risks to patient safety are increasing.

With cyberattacks like Petya and WannaCry showing just how vulnerable some network connected devices can be, action must be taken to secure the healthcare industry. Viewing security as a component of safety and efficacy of device functions, and embracing "security by design", are 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.

Incentives

To further enhance proactive collaboration, we believe it important to incentivize the industry for the adoption of these cybersecurity practices. Incentives could come in many forms, such as monetary subsidy or safe harbors from enforcement actions. This will encourage the investment into cybersecurity from the providers in an age when it is understood no organization can prevent all cybersecurity attacks. Specifically, we encourage HHS offer enforcement flexibility for those providers who: 1) demonstrate adoption of the NIST Cybersecurity Framework; and 2) adopt the relevant best practices being delivered through the CSA 2015 405(d) Task Group.

The Committee's interest in this topic is timely, and efforts to enhance the cybersecurity of our nation's healthcare system are to be commended. On behalf of AEHIS and my colleague healthcare CISOs, I sincerely thank the Committee for allowing me to speak regarding the reauthorization of the Pandemic and All-Hazards Preparedness Act. I look forward to answering your questions.