End of Year Recap on Cybersecurity Activities
December 2018

Backdrop

Throughout 2018, there has been a flurry of activity across a variety of federal agencies working to address cybersecurity in the healthcare sector, with much of the focus on medical devices. With the growing use of wireless and connected devices in the healthcare system, cybersecurity threats have become more serious and it's garnering increased attention from policymakers in Washington, D.C. In April, the Food and Drug Administration (FDA) released a Medical Device Safety Action Plan laying out future actions the agency plans to make to increase the cyber resiliency of devices in healthcare. Several other agencies are also engaged in cybersecurity efforts in healthcare. Meanwhile, the Health Sector Coordinating Council has been very active in 2018 re-energizing our sector's cybersecurity efforts.

Food and Drug Administration (FDA)

An FDA-penned blog describes the plethora of FDA action being taken to ensure that device security is managed as a truly shared responsibility across industry stakeholders. The blog described several highlights of interest to our members:

- **FDA Pre-Market Guidance:** In October, the FDA released a revision to the guidance document titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" – last updated in October of 2014. In the aforementioned blog post, the agency indicates that "the rapidly evolving landscape, and the increased understanding of threats and their potential mitigations necessitated an updated approach" to cybersecurity practices regarding medical devices. The new, draft pre-market guidance outlines details on device design, labeling and documentation must be included for devices with cybersecurity risk being submitted to the FDA for approval. Comments are due to the FDA on March 18th. CHIME and AEHIS plan on commenting.
- **FDA Workshop:** On the 29th and 30th of January, the FDA will hold a Public Workshop to discuss the updated pre-market guidance and facilitate dialogue on the subject. Monitor CHIME's Monday policy eNewsletter – the Washington Debrief – for more information.
- **FDA-DHS Collaboration:** The Department of Homeland Security (DHS) and the FDA recently have come to an agreement formalizing the roles and responsibilities of each agency regarding information sharing related to cyber threats and vulnerabilities to the healthcare critical infrastructure. The cooperation will primarily take place between the FDA and DHS' National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC will facilitate and coordinate information sharing between researchers, device manufacturers and the FDA in the event of cybersecurity vulnerabilities being identified by DHS.
- **Two new Medical Device ISAOs:** In conjunction with the FDA, two new medical device ISAOs have been formed. These new ISAOs are MedISAO and Sensato.
- **MITRE Playbook:** In October, the MITRE Corporation, an FDA contractor, released a document titled "The Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook" that outlines a framework for organizations in the healthcare industry to plan for and respond to cybersecurity incidents relating to medical devices.

Department of Health and Human Services (HHS)

In October, The Department of Health and Human Services (HHS) scrapped the existing Healthcare Cybersecurity Communications and Integration Center (HCCIC) in favor of the new Health Sector Cybersecurity Coordination Center (HC3). The role of the HC3, as described in the press release, is to "work with the sector, including practitioners, organizations, and cybersecurity information sharing organizations to understand the threats it faces, learn the bad guys' patterns and trends, and provide information and approaches on how the sector can better defend itself."

National Institute for Standards and Technology (NIST)

Many know the National Institute for Standards and Technology (NIST) from their work in developing the popular Cybersecurity Framework, now on version 1.1. This year, they've introduced efforts to secure the telehealth remote patient monitoring ecosystem and the preliminary steps of their first privacy framework.

- **NCCoE Telehealth RPM RFI:** In November, the National Cybersecurity Center of Excellence (NCCoE), a part of NIST, released a request for information (RFI) on "Securing the Telehealth Remote Patient Monitoring Ecosystem." With expanded reimbursement for communication technology-based services and various forms of telemedicine, patients are able to receive increased levels of care from within their own home, creating a new and unique cybersecurity challenge.
- **Privacy Framework:** NIST is currently in the process of developing an enterprise risk management tool to help organizations manage individuals' privacy. In November, NIST released their request for information on developing their risk based, outcome-based, voluntary and non-prescriptive framework. Throughout the process, NIST has held a workshop and a webinar regarding their initial request for information.

Health Sector Coordinating Council (HSCC)

More than 200 organizations across the industry spectrum have joined the Healthcare and Public Health Sector Coordinating Council's (HSCC) Cybersecurity Working Groups which includes 13 Task Groups, all with the intended goal of strengthening our industry's posture protecting patient safety and privacy. CHIME and AEHIS are very involved with this public-private partnership that includes the FDA. We want to bring to our members attention a few of their activities:

- **Voluntary best practices:** HHS and our AEHIS chair, Erik Decker, co-chair this effort. The "405(d)" Task Group is named for a section of the Cybersecurity Act of 2015 and will offer consensus-based guidelines, practices, and methodologies to strengthen tour sector's cybersecurity posture against cyber threats. The tool will be aimed at providers of varying sizes. Look for this soon. A fact sheet can be found here.
- **Medical Technology Cybersecurity Risk Management:** The FDA co-chairs the Medical Technology and Health IT Task Group along with forward-leaning industry and health care delivery organization (HDO) leads. The task group will be releasing a joint security plan shortly that describes best practices for implementing medical device cybersecurity and resilience recommendations, and further demonstrates the capabilities of medical device manufacturers working together with healthcare provider organizations to articulate a common vision to further safeguard patients.
- **Workforce Development:** The Workforce Development Task Group, is co-chaired by an AEHIS member. Recently, at a NIST conference on workforce, members of the group presented. Beginning on slide 14 is a compelling narrative about the cybersecurity workforce needs in the healthcare sector. The slides can be found here.