United States Department of
Health & Human Services
Office of the Assistant Secretary for Preparedness and Response

ASPR
ASSISTANT SECRETARY FOR
PREPAREDNESS AND RESPONSE

Health Care Industry Cybersecurity (HCIC) Task Force Meeting

Meeting Information

Date: Thursday, December 15, 2016, 3:00pm-5:00pm
Location: Deloitte Facility 1919 N. Lynn Street, Arlington, VA, 22209

Key Highlights

Held a public session that included briefings from America's Health Insurance Plans (AHIP), HIMSS, and Medical Device Innovation, Safety and Security Consortium (MDISS).

Discussion Summary

AHIP Presentation

Marilyn Zigmund Luke – Vice President, Special Projects, Executive Office, AHIP

Ms. Marilyn Zigmund Luke stated that AHIP is a trade association that represents a majority of the nation's health insurance providers to include employer-sponsored coverage, individual coverage, and public programs. Part of AHIP's goal is to expand access to affordable health care coverage for all Americans while offering choice, quality, and innovation. Ms. Luke stated that the membership supports and is well-versed in the *Health Insurance Portability and Accountability Act* (HIPAA) and the *Health Information Technology for Economic and Clinical Health Act* (HITECH).

Ms. Luke acknowledged the challenges related to organizational size, availability of resources, and standards in place that can affect an organization's ability to effectively implement cybersecurity controls. She also noted AHIP's desire to participate in efforts related to standards development and members current role in helping to identify common principles, certification and accreditation programs, offer education and information programs, and conduct testing based on best practices. She added that AHIP has partnered with many agencies to coordinate and collaborate on issues related to cybersecurity and AHIP has encouraged its member to remain up-to-date on cybersecurity issues.

Ms. Luke stated that AHIP members work with the Information Sharing and Analysis Centers (ISAC), National Association for Insurance Commissioners to examine and develop cybersecurity standards, and with the National Governors Association to help governors and states understand cybersecurity and identify best practices. At the Federal level, AHIP works with the U.S. Department of Health and Human Services (HHS), the Office of the National Coordinator for Health Information Technology (ONC), the Centers for Medicare & Medicaid Services, and the Office of Personnel Management.

Ms. Luke stated that AHIP would like the Task Force to consider several recommendations:

- Standards should not be prescriptive and the use of different models should be encouraged. Organizations need the flexibility to assess their own operating environments and the ability to use processes and standards that are best suited for their customization.
- New legal requirements should align to existing requirements. Members have spent a great deal of time and resources to leverage HIPAA and HITECH requirements. These laws serve as a solid framework to improve security posture that the industry should continue to be able to leverage.
- Private organizations should receive safe harbor and penalties should not be the primary enforcement technique for those organizations who make good faith compliance efforts before, during, and after a cyber event.

- Coordinate Federal and state activities to ensure consistency and a national framework for cyber and data security.
- Increase the level of educational resources and distribution of lessons learned.

A Task Force member asked what AHIP sees and the conflict between the Federal and state levels. Ms. Luke replied that states can enact regulations that are more stringent than Federal laws, as long as they do not conflict with those laws. Member concerns include a 50 state patchwork of standards where organizations have to comply with different standards in different states. A Task Force member referenced the comment about keeping HIPAA and HITECH intact and offered that the Task Force could keep the best characteristics of each and augment with more palatable characteristics. Ms. Luke replied that she believes both HIPAA and HITECH are effective and that the focus should be on educating people about the vulnerabilities with the implementation of new technologies.

A Task Force member questioned how to define what acting in good faith for cybersecurity means. Ms. Luke replied acting in good faith would include an organization being compliant with applicable standards and regulations, conducting risk assessments and knowing the risks to your organization, developing policies and procedures, training staff, and implementing contractual vendor requirements for a compliance. She added that no entity can be completely safe from attack, but that those organizations who have taken these preventative steps should not also become victims and incur penalties as this will not prevent attacks from occurring in the future.

HIMSS Presentation

Jeff Coughlin – Senior Director, Federal and State Affairs, HIMSS

Mr. Jeff Coughlin began by stating that HIMSS is a cause-based global enterprise that includes members from across the health care community and that focuses on health IT and enabling health care transformation. He reviewed the current environment, noting that current vulnerabilities can lead to increased opportunities for exploitation, cybercrime as a profession, and cybercriminals' attack techniques that are more sophisticated than our defense techniques. Mr. Coughlin stated that uncertainty remains within the community about what providers can do to address cybersecurity challenges, and that cybersecurity is often viewed as an IT problem. He emphasized that health care needs a holistic approach to address this problem.

Mr. Coughlin discussed the future state and said that the health care community needs to work in coordination with cyber experts from other sectors, and that all stakeholders should proactively share information about threats, actors, vulnerabilities, and mitigation techniques. He reviewed the three HIMSS cybersecurity calls to action: 1) adopt a universal information privacy and security framework for the health sector; 2) create an HHS cyber leader role; and 3) address shortage of qualified cybersecurity professionals. Mr. Coughlin emphasized that the HHS cyber leader role should coordinate the activities of the Office for Civil Rights, ONC, the Office of the Assistant Secretary for Preparedness and Response (ASPR), and other ongoing HHS projects. This individual would lead the sector specific action plan to ensure adequate threat and asset response, which would include the National Institute of Standards and Technology Framework and enhance the idea of bi-directional exchange of information and the benefits of timely cyber threat information – similar to the National Cybersecurity and Communications Integration Center. Mr. Coughlin reviewed recommendations to address the staffing shortage of qualified cybersecurity professionals and stated that HIMSS would encourage holding stakeholder meetings to identify the appropriate steps to address the issue in the short, medium, and long-term.

Mr. Coughlin concluded by offering HIMSS as a resource to the Task Force and noted that the organization disseminates a monthly environmental scan report that highlights the trends and predictions for cybersecurity. Task Force members asked if HIMSS had additional data regarding the workforce shortage whether HIMSS had a definition for appropriately trained. Mr. Coughlin stated he would try to provide this information back to the Task Force.

MDISS Discussion

Dr. Dale Nordenberg – Executive Director, MDISS

Dr. Dale Nordenberg highlighted the challenges for medical devices with 1 billion hospital and outpatient visits per year. When visits translate to people and the number of exposures, he estimated that over the next 10 years 100 billion exposures would occur between the patient and connect medical devices.
Dr. Nordenberg continued that MDISS is working with the National Health ISAC and the U.S. Food and Drug Administration (FDA) to stand up the medical device information sharing and analysis organization and a national health care technology cyber surveillance and safety network that is founded on public health best practices. He noted that 15 years ago, many doctors did not do informatics, but do now. Today many doctors do not know cybersecurity issues, but he predicted they will in the future because cyber and medical devices will become a common quality metric for health care systems.

Dr. Nordenberg reviewed conceptualization of the national health care technology cyber surveillance and safety network. He emphasized that it is a public-private partnership that originated so that stakeholders could access the required information in a single location. Through this model, MDISS will collect and apply data in multiple domains. A current challenge is that no data standards exist to share data. Dr. Nordenberg continued that the community can follow a classic public health approach to address issues related to cybersecurity, patient safety, and population health. MDISS is building information data systems, new ways to organize systems, and to conduct surveillance. He emphasized that finding vulnerabilities is interesting, but that finding vulnerabilities and pairing that with a mitigation approach is really interesting and can have large effects on patient safety and population health.

Dr. Nordenberg reviewed the recommendations and stated that to share data and information in this domain, and to link the device to the cyber characteristics and threats to the patient, there are different reporting mechanisms and standards. He stated that to advance use cases to mature the integration of data standards one needs to include cybersecurity threat intelligence, patient case reporting, population health reporting, and device adverse event reporting. When all of these elements come together, standing up a national surveillance system becomes possible.

A Task Force member commented that there are massive blind spots in the collection of common vulnerability exposures (CVE) for medical equipment and industrial control systems technologies due to who the who the issuing authorities are, prioritization based on market share, and the *Digital Millennium Copyright Act* (DCMA). The Task Force member continued that the recent lift of DCMA and post-market guidance encouraging voluntary coordinated disclosure policies should prompt more individuals and organizations to report vulnerabilities. Additionally, the Task Force member noted the need to relook at the common vulnerability scoring system (CVSS) and make more of an investment in CVE creation and CVSS for the medical community to promote the collection of additional data points. Dr. Nordenberg questioned whether the availability of medical devices for research is an issue. Mr. Corman replied yes, that many research devices are old, cheap, and only available on eBay; larger devices receive little scrutiny because people cannot gain access to them.

A Task Force member asked how an item in the FDA's Manufacturer and User Facility Device Experience (MAUDE) Database would feed into the national system. Dr. Nordenberg stated that they do not have that answer yet. He described the different types of surveillance (convenience sampling, passive surveillance, and active surveillance) and noted that for MDISS to conduct active surveillance they would enroll hospitals, know the denominator, create a mechanism for hospitals to report, and use data from the MAUDE database to qualify the data and use it as data points. A Task Force member noted that there is no forensic examination of equipment following a patient's death. Dr. Nordenberg agreed, saying that it is astounding that no one examines the device to ensure it is functional; he added that he believed this will change within the next two years.

A Task Force member stated that he was concerned that the sector was implementing things in the right order and was not concerned about the rate of implementation. Dr. Nordenberg replied that the calculus for the "right" order is not simple and that the premise is that connectivity improves quality of care. He continued that health care matures in a complicated manner and that he believes manufacturers have remarkably mature programs. As time progresses, hospitals will be fine based on the manufactures intent as well as their capability.

Task Force Member Attendance

Table 1 Task Force Member Attendance

LAST NAME	FIRST NAME	ORGANIZATION
Corman	Joshua	I Am The Cavalry
Csulak	Emery	Centers for Medicare and Medicaid Services
Dzierzanowski	James	Kaiser Permanente Health Plan (representing George DeCesare)
Finn	David	Symantec Corp.
Laybourn	Laura	U.S. Department of Homeland Security
McNeil	Michael	Philips Healthcare
McWhorter	Dan	FireEye, Inc.
Meadows	Theresa	Cook Children's Health Care System
Monson	Jacki	Sutter Health
Ramadoss	Ram	Catholic Health Initiatives
Rice	Terry	Merck & Co.
Sardanopoli	Vito	Quest Diagnostics
Stine	Kevin	National Institute of Standards and Technology
Suarez	Roberto	BD (Becton, Dickinson and Company)
Sublett	Christine	Augmedix, Inc.
Thompson	Lauren	U.S. Department of Defense/Department of Veteran Affairs
Ting	David	Imprivata, Inc.
Trotter	Fred	CareSet Systems

Non-Member Attendance

Table 2 Non-Member Attendance

LAST NAME	FIRST NAME	ORGANIZATION
Centola	Joanna	Deloitte
Chase	Penny	MITRE
Coughlin	Jeff	HIMSS
Curren	Steve	ASPR
Edison	Nicole	ASPR
Hoover Thompson	Kelly	PA eHealth Partnership
Leitsch	Darren	Deloitte
Luke	Marilyn Zigmund	AHIP
Marinella	Ryan	Deloitte
Marsh	William	U.S. Department of Defense/Department of Veteran Affairs
Nordenberg	Dale	MDISS
Odderstol	Thad	U.S. Department of Health and Human Services
Ross	Aftin	U.S. Food and Drug Administration
Savickis	Mari	CHIME
Schwartz	Suzanne	U.S. Food and Drug Administration
Smith	Malikah	ONC
Todd	Nickol	ASPR
Trumpoldt	Ken	Deloitte
Wellington	David	U.S. Department of Defense/Department of Veteran Affairs
Zuk	Margie	MITRE