FDLI MEMBER MAGAZINE | WWW.FDLI.ORG | MAY/JUNE 2017

UPDATE

Food and Drug Law Institute

FDLI

2017 ANNUAL CONFERENCE RECAP

Momentum Builds for Medical Device Cybersecurity to Level Up

by Emily Strunk

The cybersecurity of medical devices is one of the hottest topics in healthcare and, not surprisingly, was of burning interest during the FDLI 2017 Annual Conference, where an entire panel was devoted to the topic: "Changing Landscape of IoT: Medical Device Privacy and Cybersecurity." Panelists included Suzanne Schwartz, FDA's Center for Devices and Radiological Health's (CDRH) Associate Director for Science, Matthew Barrett of the National Institutes of Standards and Technology (NIST), and Zachary Rothstein from the Advanced Medical Technology Association (AdvaMed), representing key stakeholders in the ongoing effort to ensure medical devices are protected from hackers. They discussed the myriad challenges and critical components of a robust medical device cybersecurity program. The consensus was that the cybersecurity of medical devices has made great progress in the last several years, but there are still many challenges and a long way to go before all of the millions of medical devices in the marketplace will be adequately protected from cyber attacks. Held at the beginning of May, the discussion could not have been more timely as one of the biggest months in cybersecurity policy unfolded against the backdrop of a massive worldwide cybersecurity attack that reached medical devices in U.S. hospitals and shut down entire departments in some U.K. hospitals.

Emily Strunk is a Litigation and Dispute Resolution associate in Mayer Brown's Washington, DC office. She focuses on regulatory matters and consumer protection issues, primarily as they relate to products regulated by FDA.

Connecting devices to each other and to the Internet of Things (IoT) allows for increased functionality and convenience, and can enhance patient health and safety. But the more connected we are, the more vulnerable we are to a seemingly infinite number of invisible and unpredictable threats. Accordingly, cybersecurity has become a paramount business practice and regulatory compliance issue, but expertise, policies, and culture are still catching up.

The consequences of inadequate cybersecurity for connected medical devices are perhaps some of the most dire, with the potential for serious harm or even death. Fortunately, there are no known cases of serious patient harm resulting from medical devices being hacked, but the threat is real and many agree it is only a matter of time before a serious adverse event results from a cyber threat. In November 2015, one expert estimated that medical devices lagged in adequate cybersecurity, by ten years or more.[1] FDA, industry, and other stakeholders are working to address this deficit, but the complexity of both the concerns and the solutions presents significant challenges.

A week after the Annual Conference, the WannaCry global ransomware cyber attack infected several hundred thousand computers in 150 countries by exploiting a vulnerability in Windows. The healthcare sector was significantly affected, with some hospitals shutting down entire departments; at least several medical devices were infected. By some reports, this was the first ransomware attack to infect medical devices in U.S. hospitals.[2] In addition to rattling the cybersecurity community in general, the attack increased awareness of cybersecurity issues in the context of medical devices and intensified stakeholders' resolve to tackle them. FDA, medical device manufacturers, and other players quickly came together to implement solutions and address affected devices and furthered the case for a permanent cyber attack response team that can be on standby to be better prepared to respond to future attacks. WannaCry added real-world context during a month that was rich with cybersecurity policy discussions and problem-solving.

The panelists at the FDLI Annual Conference discussed some of the greatest challenges facing the cybersecurity community, such as the sheer shortage of so-called "white hat hackers," or ethical hackers who work for companies to research weaknesses in cybersecurity. White hat hackers are critical to one of the most important elements of cybersecurity: identifying vulnerabilities so that they can be repaired before malicious hackers exploit them and put patient safety at risk. Panelists stressed the importance of "coordinated disclosure," where a hacker informs a medical device manufacturer of a vulnerability before publishing the information so that manufacturers know about and can remove the vulnerability before it goes public (and can be exploited by malicious hackers), and then sharing the vulnerability information with the larger cybersecurity community. In addition to the shortage of white hat hackers, other challenges include how to effectively incentivize coordinated disclosure and permanently overcoming language in the Digital Millennium Copyright Act (DCMA)[3] that prohibits cybersecurity researchers from reverse engineering protection systems that they did not create (though a temporary exemption is currently in place for individuals "acting in good faith"). Finally, human factors and creating a culture of cybersecurity are also problematic. As one panelist implied, people are often harder to change than processes or technology. WannaCry exploited a known vulnerability for which a patch had been created months before, but those who were affected had not downloaded and applied the patch to their technology, leaving the door wide open for a cyber attack.

Increased Policy Focus on Medical Device Cybersecurity

The U.S. Department of Health and Human Services (HHS) Cyber Task Force May 3, 2017 report to Congress listed healthcare cybersecurity in "critical condition" and, as the second of six imperatives, stressed the need to "increase the security and resilience of medical devices and health IT."[4] The report is 88 pages and contains more than 100 action items across six areas. Noteworthy recommendations for medical devices include as an initial matter securing legacy devices. That effort would require inventorying clinical environments to document unsupported devices and either replacing or upgrading them with supported alternatives, or, if they need to be retired, developing a timeline for doing so and implementing risk reduction strategies for the remainder of their use. Another recommendation is that manufacturers and developers should create a "bill of materials" describing a device or application's components and any associated cyber risks, actively participate in information sharing programs, and adopt and engage in coordinated vulnerability disclosure consistent with recognized standards. The report also calls for a Medical Computer Emergency Readiness Team (MedCERT) to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures. This team is distinct from the Health Cybersecurity and Communications Integration Center (HCCIC) that HHS plans to launch in June 2017 to educate patients and healthcare organizations about the risks associated with using mobile data and apps.[5]

Just a week after the Cyber Task Force report was issued and on the eve of the WannaCry ransomware attack, President Trump signed Executive Order (EO), "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,"[6] his first significant action addressing cybersecurity. The EO lays out policies for addressing cybersecurity for federal networks, critical infrastructure, and the nation overall and builds upon the existing federal framework for addressing cybersecurity risk management, while also calling for broad policy reviews by multiple U.S. government departments and agencies. While the EO does not specifically mention healthcare or medical devices, its policies will reach these industries.

On the heels of WannaCry, FDA held a long-planned third public workshop[7] to continue working through the challenges specific to cybersecurity in medical devices. WannaCry, still being resolved during the days of the workshop, provided real-world context to discuss the most pressing medical device cybersecurity challenges, such as the lifespan of a device exceeding the length of time support is offered for software applications, and smaller entities' lack of resources to address the large task of patching, updating, and otherwise maintaining a copious number of medical devices. Participants also discussed how cybersecurity features, such as frequent log-ins, affect clinical workflow and the need to work with healthcare professionals to ensure cybersecurity features do not compromise patient care.

A few days after the FDA public workshop, HHS launched the first meeting of a new public-private partnership to develop a "common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes addressing cybersecurity in the healthcare sector" as required under the Cybersecurity Act of 2015.[8] In line with conclusions at FDA's cybersecurity workshop, participants agreed that the partnership's efforts should focus on small healthcare entities, which are more vulnerable to, and less equipped to handle, cyber threats. Meeting participants will develop draft guidelines for further discussion at future working group meetings.

The month of May represented a crescendo in medical device cybersecurity policy discussion, which was not entirely surprising given the momentum that has been building in the last several years alongside increasingly sophisticated threats. While there still are more questions than answers, HHS and FDA are making progress towards a more secure cyber space for medical devices and the healthcare sector generally.

Making Medical Devices More Secure

At the core of medical device cybersecurity is a constellation of government entities, non-government organizations, and industry actors working together to develop a system that will prevent patient harm, protect patient privacy, and secure data. Key to this effort are FDA, NIST, Information Sharing and Analysis Organizations (ISAOs), and industry, often represented by AdvaMed.

FDA has been regulating medical device software for decades, but only began officially addressing cybersecurity with guidance documents issued in 2005 that addressed patient safety considerations specific to software.[9] In 2014 and 2016, FDA finalized guidance that more specifically prescribed how medical device manufacturers should integrate cybersecurity as part of their premarket process[10] and postmarket compliance programs,[11] respectively. In premarket submissions, medical device software must be proactively designed to prevent cybersecurity vulnerabilities and exploits. Postmarket management should include a comprehensive cybersecurity risk management program to monitor, identify, and address cybersecurity exploits, consistent with the Quality Systems Regulation (QSR). Taken together, the goal is to account for cybersecurity throughout the lifecycle of the device, an element applauded by the HHS Cyber Security Task Force Report.

The premarket guidance supplements the 2005 guidance documents and directs manufacturers to consider cybersecurity risks when designing and developing their medical devices–including design inputs, software validation, and risk analysis–to better mitigate patient risks. As part of these considerations, manufacturers should: (1) identify assets, threats, vulnerabilities; (2) assess the impact of threats/vulnerabilities on device functionality and patients (end users); (3) assess likelihood of a threat and of a vulnerability being exploited; (3) determine risk levels and suitable mitigation strategies; and (4) assess residual risk and risk acceptance criteria. The guidance additionally enumerates the cybersecurity functions that are consistent with the NIST Framework and the required cybersecurity-related documentation and recognized standards.

Once on the market, the manufacturer's postmarket compliance program must adequately address cybersecurity issues that may lead to safety or effectiveness concerns. The postmarket guidance is somewhat complex and takes into account that cybersecurity risks are continuously evolving and impossible to mitigate through premarket controls alone. FDA asserts that a comprehensive cybersecurity risk management program should: (1) Apply the NIST Cybersecurity Framework; (2) Monitor cybersecurity information sources to identify and detect cybersecurity vulnerabilities and risks; (3) Maintain robust software lifecycle processes that incorporate monitoring third-party software, and verifying and validating software updates and patches; (4) Understand, assess, and detect the presence and impact of vulnerabilities; (5) Establish and educate on processes for vulnerability intake and handling; (6) Use threat modeling to clearly define how to maintain safety and essential performance; (7) Establish a process to assess the severity of patient harm and residual risk; (8) Develop mitigations that protect, respond, and recover from cyber risks; (9) Adopt a coordinated vulnerability disclosure policy and practice; and (10) Deploy mitigations that address cybersecurity risks early and prior to exploitation.

Separate from, but incorporated into, FDA's postmarket guidance, the NIST Cybersecurity Framework, developed at the direction of a 2013 Executive Order, "Improving Critical Infrastructure Cybersecurity,"[12] has become one industry standard. The Framework is a "voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk"[13] and consists of five concurrent and continuous Functions: Identify, Protect, Detect, Respond, and Recover. FDA discusses the applicability of these functions in the postmarket guidance and encourages manufacturers to adopt the framework as part of its postmarket management of cybersecurity, but ultimately does not require it. NIST works closely with FDA and industry on cybersecurity issues and how to best adapt the framework to medical devices. A draft update to the Framework is in progress, but has not yet been implemented.

Information sharing is widely viewed as a critical component of cyber risk management. An ISAO is a collaborative group in which public and private sector members share cybersecurity information. To encourage participation, information shared through ISAOs is protected from release under the Freedom of Information Act (FOIA). FDA signed a memorandum of understanding (MOU) with the National Health Information Sharing and Analysis Center (NH-ISAC) and Medical Device Innovation, Safety and Security Consortium (MDISS) to help create an environment conducive to industry participation. Additionally, for companies that voluntarily participate in an ISAO (as defined by FDA) and follow recommendations in postmarket guidance, FDA will not enforce certain reporting requirements in cases where there are no serious adverse events or deaths associated with the vulnerability.

Industry participation is also crucial, particularly since information sharing depends on it to share cyber threat information. Manufacturers are often best positioned to discover vulnerabilities and can provide valuable input on the practicalities of cybersecurity programs and the manufacturer's limitations. Speaking at FDLI's Annual Conference, AdvaMed Associate Vice President for Technology and Regulatory Affairs, Zachary Rothstein, emphasized that all stakeholders within the medical device community, including consumers, need to work together. Manufacturers play a significant role, but as soon as a device is hooked into a customer's network and used by their personnel, there are deficiencies and variables that manufacturers cannot always account for or proactively address. Referencing AdvaMed Medical Device Cybersecurity Foundational Principles,[14] designed to help manufacturers build a cybersecurity program to develop and deploy secure medical devices, Mr. Rothstein underscored the need for all stakeholders within the larger system to work together to ensure its integrity. He said that AdvaMed is also developing a cybersecurity checklist for premarket submissions to help standardize what medical device manufacturers include.

At FDLI's Annual Conference, Suzanne Schwartz (CDRH, FDA) shared promising news for how all of these pieces are coming together: FDA is seeing evolution in the right direction. Industry is embracing cybersecurity principles, demonstrating an understanding of how to implement them, and leveraging the NIST Cybersecurity Framework to do so. There is increased collaboration and sharing and a majority of medical device premarket submissions now include cybersecurity information.

The Future of Cybersecurity in Medical Devices

Though many challenges and questions remain and there is much work ahead, the momentum towards a culture of cybersecurity and a suitable cybersecurity regime for medical devices seems to be picking up. While the optimism looking forward is encouraging, one pressing issue that requires us to look back is that many devices with vulnerabilities have already made it to market and are ripe for cyber attacks. This concern will need to be addressed before the medical device cyber space can truly be secured. At this time, most cyber attacks on medical devices have been benign, carried out simply because the system was open and not because the hacker was targeting a medical device. Now is an opportune time to level up and fix the system, before there are significant adverse events due to cybersecurity lapses, but FDA, industry, and their partners will need to maintain their momentum to secure the cyber space before this can happen.

What Exactly is Cybersecurity?

Cybersecurity uses standards, guidelines, and practices to protect critical infrastructure from unauthorized access and use. Although there are hundreds of terms relevant to cybersecurity, a few key terms[15] are critical to understanding the basics of how cybersecurity works to protect patients from cyber attacks.

- *Critical infrastructure*[16] is the systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.
- An *asset* is a person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.
- A *threat* is any circumstance or event with the potential to adversely impact the device, organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats exercise vulnerabilities, which may impact the safety or essential performance of the device.
- A *vulnerability* is a weakness in an information system, system security procedures, internal controls, human behavior, or implementation that could be exploited by a threat.
- An *exploit* is an instance where a vulnerability or vulnerabilities have been exercised (accidently or intentionally) by a threat and could impact the safety or essential performance of a medical device or use a medical device as a vector to compromise a connected device or system.

1. *It's Way Too Easy to Hack the Hospital*, M. Reel and J. Robertson, Bloomberg Businessweek, November 2015, https://www.bloomberg.com/features/2015-hospital-hack/ (last accessed May 31, 2017).
2. *Medical Devices Hit By Ransomware For The First Time In US Hospitals*, T. Fox-Brewster, May 17, 2017, https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#23e9aa6f425c (last accessed May 31, 2017).
3. 17 U.S.C. §1201.
4. *Report On Improving Cybersecurity In The Healthcare Industry*, The Healthcare Industry Cybersecurity Task Force, May 2017, https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2017/cs2017_0156.pdf (last accessed May 31, 2017).
5. HHS to stand up its own version of the NCCIC for health, N. Ogrysko, Federal News Radio, April 20, 2017, https://federalnewsradio.com/health-it/2017/04/hhs-to-stand-up-its-own-version-of-the-nccic-for-health/ (last accessed May 31, 2017).
6. *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800, May 11, 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (last accessed May 31, 2017).
7. *Public Workshop - Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis*, May 18-19, 2017 (https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm549732.htm) (last accessed on May 31, 2017).
8. Cybersecurity Act of 2015, Section 405 (6 U.S.C. §1533).
9. *Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*, January 14, 2005, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf (last accessed May 31, 2017) and *Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*, May 11, 2005, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf (last accessed May 31, 2017).
10. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff , October 2, 2014, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf (last accessed May 31, 2017).
11. *Postmarket Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug

Administration Staff, December 28, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf (last accessed May 31, 2017).

[12] *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (last accessed May 31, 2017).

[13] *Cybersecurity Framework FAQS Framework Basics*, https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics (last accessed May 31, 2017).

[14] AdvaMed Medical Device Cybersecurity Foundational Principles, https://www.advamed.org/sites/default/files/resource/advamed_medical_device_cybersecurity_principles_final.pdf (last accessed May 31, 2017).

[15] Definitions are taken from *Postmarket Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff, December 28, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf, unless otherwise noted.

[16] National Initiative For Cybersecurity Careers And Studies Glossary, https://niccs.us-cert.gov/glossary (last accessed May 31, 2017).