Medical Device Cybersecurity

How the US Food and Drug Administration and Other Stakeholders Are Collaborating to Increase Patient Safety

by Sonali P. Gunawardhana and Margaret Horn

When one thinks of cybersecurity it is easy to think of villainous hackers portrayed in a variety of Hollywood thrillers. Cybersecurity breaches have been traditionally portrayed in films as hitting financial institutions causing devastating events to unfold. In some films the hacking is in aid of a masterful heist in which the main protagonist is trying to either thwart the robbery or possibly to jet off to a luxurious island with millions in tow. Most story plots do not revolve around hacking a medical device. The HBO series, Homeland, however, made what seemed implausible a truly possible risk. The plot revolved around the hacking of the Vice President's pacemaker to cause it to malfunction, eventually causing the Vice President's demise. The hacking of a medical device for monetary gain or to cause catastrophic events is not merely the stuff of fiction, but a tangible and constantly monitored risk. The US Food and Drug Administration (FDA) and several federal agencies are collaborating along with a variety of stakeholders to safeguard patients from possible cybersecurity risks.

Many of today's medical devices are increasingly connected

Sonali P. Gunawardhana is Counsel in Shook, Hardy & Bacon's Washington, DC Office. She advises clients with regulated products in the medical device, pharmaceutical and food industries.

Margaret Horn is an associate in Shook, Hardy & Bacon's Washington, DC Office. She counsels clients on regulatory matters including product labeling, marketing materials, recalls, and FDA compliance actions. She also defends life sciences clients in all stages of products liability litigation.

to the Internet, hospital networks, and other medical devices to provide features that enhance the ability of health care providers to treat patients and improve health outcomes. Unfortunately, these same features also increase the risk of potential cybersecurity threats—many high and moderate risk medical devices contain the capability to transmit data directly from the hospital's IT network or wirelessly communicate with other devices within the hospital or even through the medical professional's phone. Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device, which may lead to catastrophic health consequences.

Unfortunately, threats and vulnerabilities cannot be eliminated and reducing security risks can be challenging for all stakeholders, from the device manufacturer, to the hospital or the healthcare practitioner, and ultimately to the patient. The heath care environment is clearly multifaceted; therefore, it is imperative that medical device manufacturers, hospitals, and facilities work together to manage security risks. Many medical device manufacturers are now grappling with how best to ensure their devices are used solely for their intended use to care for patients and prevent harm by those with unscrupulous intentions. FDA, along with several sister agencies, are working together to develop a risk-based framework that relies on the varied stakeholders working together towards a goal of trust and transparency.

Initial Efforts by Key Federal Regulators to Address Cybersecurity Risks

FDA has been ramping up its cyber enforcement in recent years, starting in 2013 with the formation of a "cybersecurity working group" and the publication of guidance entitled, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,"[1] in 2014. The guidance outlines FDA expectations of manufacturers to develop long-term plans for medical device cybersecurity for the products being developed. The passage of the Food and Drug Administration Safety and Innovation Act of 2012[2] requires FDA to partner with several federal agencies given their shared regulatory oversight of these interconnected and wireless devices.

As a result, FDA worked closely with the Federal Communications Commission (FCC) and Office of the National Coordinator for Health IT (ONC) to propose a strategy on an appropriate, risk-based regulatory framework for health IT that promotes innovation, protects patient safety, and avoids unnecessary and duplicative regulation. On April 3, 2014, the FDA, FCC, and ONC released the FDASIA Health IT Report[3] outlining a proposed strategy for a risk-based framework.

FCC continues to support this relationship by adopting rules and policies that promote the development of wireless medical devices while implementing important technical standards. All wireless medical devices utilize a frequency within the electromagnetic radio spectrum and operate under a under a license from FCC. The Commission has incrementally allocated electromagnetic spectrum for wireless medical devices. For example, FCC has allocated ranges of the spectrum for: 1) wireless medical telemetry devices that measure patients health parameters (like wireless cardiac monitors); 2) MedRadio, implanted and body-worn wireless devices used for diagnostic and therapeutic purposes; and 3) medical body area networks (MBAN) technology, networks of wireless sensors that transmit patient health data to their healthcare providers.[4] Under its rulemaking power, FCC also ensures that medical devices may not be marketed until they have shown compliance with technical standards.[5]

To further its accessibility mission, FCC created the CONNECT2HEALTH Task Force to accelerate adoption of health care technologies in the areas of tele-health, mobile applications, and telemedicine by leveraging broadband and identifying regulatory barriers to overcome.[6] The Commission also released a Notice of Public Comment seeking input on accelerating adoption and accessibility for broadband-enabled health care solutions in 2017.[7] This aspect of FCC's mission focuses on access to broadband in rural areas—which is essential to providing telemedicine services, including remote review of patient health data by providers and remote medical consultations.

FDA's Continued Efforts to Manage Post Market Cybersecurity Concerns

FDA continued its efforts to provide information that addressed legacy devices by issuing a guidance entitled "Postmarket Management of Cybersecurity in Medical Devices"[8] in January of 2016. FDA was concerned about health care delivery organizations that continue to use legacy generation devices that were not designed with the ability to receive timely cybersecurity updates. Many older devices were not designed with cybersecurity in mind, and they may use insecure software, hardware, or protocols, leaving them vulnerable to attack. This guidance addresses expectations of gathering and sharing cybersecurity threats and vulnerabilities with various stakeholders, unlike the premarket

guidance that was primarily concerned with security engineering conducted by the device manufacturer.

The recommendations made in the postmarket guidance were initially considered controversial by some because FDA called upon medical device manufacturers, healthcare providers, and whitehat hackers to share previously-guarded information in order to address shared cybersecurity vulnerabilities. In recent years, there have been numerous ransomware attacks on healthcare providers, including the devastating WannaCry attack which wreaked havoc on the United Kingdom's National Health Service (NHS) as well as on numerous hospitals here in the United States. These attacks, which used security flaws in Microsoft operating systems, highlighted just how unprepared hospitals and medical device manufacturers were in dealing with cybersecurity threats. The continued attacks to the healthcare system made it abundantly clear that these key players would need to partner in order to try to prevent future ransomware attacks. As a result, many that were impacted turned to the recommendations made in the postmarket guidance as a road map though some still felt that the recommendations were not comprehensive in nature.

In response to concerns that FDA's cybersecurity efforts in the postmarket arena did not go far enough, the Office of the Inspector General (OIG) conducted an audit of FDA's cybersecurity efforts. OIG issued a report[9] on its findings, outlining problems FDA faces with postmarket cybersecurity and recommending the following actions:

> We recommend that FDA do the following: (1) continually assess the cybersecurity risks to medical devices and update, as appropriate, its plans and strategies; (2) establish written procedures and practices for securely sharing sensitive information about cybersecurity events with key stakeholders who have a "need to know"; (3) enter into a formal agreement with Federal agency partners, namely the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, establishing roles and responsibilities as well as the support those agencies will provide to further FDA's mission related to medical device cybersecurity; and (4) ensure the establishment and maintenance of procedures for handling recalls of medical devices vulnerable to cybersecurity threats.[10]

To address OIG's recommendations and respond to the rapidly evolving nature of cyber threats, FDA updated its premarket guidance[11] to ensure the information contained in its recommendations reflects the current cybersecurity threat landscape so that manufacturers can be in the best position to proactively address cybersecurity concerns designing their devices. These recommendations also will assist in how manufacturers can better protect their products against different types of cybersecurity risks, from ransomware to a catastrophic attack on a health system. The fundamental idea woven through this guidance is that medical device manufacturers must adequately address device cybersecurity for the total product lifecycle in order to ensure patients are protected from cybersecurity threats. The updated recommendations in the guidance will also assist FDA in its premarket review process, which in turn will assist in ensuring that medical devices are designed to sufficiently address cybersecurity threats before the devices are available to patients.

The draft guidance incorporates other new recommendations, namely a "cybersecurity bill of materials," which is a list of commercial and/or off-the-shelf software and hardware components of a device that could be susceptible to vulnerabilities. FDA believes that a bill of materials will enable device users or owners, such as hospitals and health systems, to more efficiently evaluate their inventory, identify devices susceptible to cyber events, and prioritize risk mitigation. The guidance also outlines two tiers of devices: 1) those with higher cybersecurity risk, including implanted devices such as pacemakers or neurostimulation devices, and 2) those with standard cybersecurity risk, which includes devices that contain software based on potential harm to patients from cybersecurity threats.[12]

Agency Collaboration

In addition to the recently updated premarket guidance document, FDA and the U.S. Department of Homeland Security (DHS) recently announced a memorandum of agreement (MOU)[13] to implement a new framework for greater coordination and cooperation between the two agencies for addressing cybersecurity in medical devices. The purpose of this memorandum is to share information and better collaborate to stay a step ahead of constantly evolving medical device cybersecurity vulnerabilities as well as being well-situated to proactively respond when cyber vulnerabilities are identified.

In furtherance of their MOU, DHS, through its National Cybersecurity and Communications Integration Center (NCCIC), and FDA routinely work in

parallel to address medical device cyberattacks. In October 2018, cybersecurity vulnerabilities were discovered, which impacted Medtronic cardiac implantable electrophysiology devices (CIEDs). Both agencies released security alerts reflective of their respective missions. FDA's alert focused on communicating the vulnerabilities and recommendations to the health care community and assessed potential risks to patient health, as well as approving a Medtronic network update to address the vulnerability.[14] NCCIC's alert focused on conveying technical vulnerabilities and mitigation techniques to users.[15]

NCCIC offers many technical services to detect and mitigate threats in both the public and private sector through cybersecurity alerts, trainings, cybersecurity evaluation tools, and incidence response services. NCCIC also serves as the coordinator for information sharing on cybersecurity threats between device manufacturers, researchers, and FDA. In this coordinating capacity, NCCIC deals with global cyberattacks that may implicate critical infrastructure in many industries worldwide—including medical devices. For example, in 2017, NCCIC coordinated with other agencies and experts to combat the global ransomware campaign, WannaCry. This attack exploited a Windows vulnerability to remotely compromise victim systems across many industries, including certain medical devices running on Windows platforms.[16]

Medical device cybersecurity is just one task within the vast the purview of DHS's cybersecurity mandate. DHS serves as the nation's central cybersecurity risk-spotter, incident-responder, and operational integration center for all systemic cybersecurity issues in the US. The agency is charged with securing the entire U.S. critical infrastructure in cyberspace which covers everything from health care services to public utilities to financial services. Given the agency's huge cybersecurity mission, coordination with key stakeholders in the field on medical device cybersecurity efforts, including FDA, is crucial to addressing these threats.

Encouraging Further Collaboration Among Key Stakeholders

In addition to the issuance of guidance documents to assist industry, FDA also recently held a fourth public workshop on January 29 and 30, 2019, entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." This workshop sought not only to focus on the new draft premarket guidance that was issued in October but to also address the continued use of legacy devices and the importance of the medical device total product lifecycle in terms of advancing medical device cybersecurity and safety. The key principles of the workshop centered around the cornerstones of resilience, trustworthiness, and transparency, which require continued collaboration across government agencies, industry, security researchers, patients, and health care providers.[17] There were many attendees from diverse backgrounds, as well as numerous breakout sessions for attendees such as the following: Threat Modeling and Systems Approaches; Risk Assessment Approaches and Labeling; Leveraging Innovation and Collaboration in the Ecosystem to Advance Cyber Safety, and Establishing Trust, Embracing Transparency, Increasing Resilience: Best Practices and Tools.

FDA representatives also encouraged stakeholders at the workshop to participate in the upcoming DefCon Biohacking Village, scheduled to occur in early August of 2019 in Las Vegas, Nevada. Participation by FDA is being encouraged in order to increase medical device manufacturer presence, introduce cybersecurity issues to the clinical community, and further engage healthcare delivery organizations.[18] The DefCon Biohacking Village is a departure from the way FDA has traditionally approached a growing regulatory issue but this is not surprising given the intricacies the world of cybersecurity entails. The website for the BioHacking Village states that the "the Village brings together thousands of attendees, along with featured inventors, world-class makers, cybersecurity researchers, self-made entrepreneurs and workshop experts from around the world, to create real solutions for some of humanity's most pressing challenges and opportunities in the areas of health, education, security, and more."[19] The mission statement of this organization sounds so promising that it is difficult to think of a more suitable opportunity to collaborate.

FDA appears to truly appreciate the importance of continued collaboration due to the ever changing cybersecurity landscape. We believe it is safe to say that cybersecurity issues will remain a steadfast challenge due to the continued use of legacy devices in various healthcare delivery systems as well as the introduction of novel interconnected medical devices to provide better and more efficient healthcare for patients.

1. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.
2. Pub.L. 112–144.
3. https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf.
4. https://www.fcc.gov/general/

fcc-health-it-actions-and-activities-timeline.
5. https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf.
6. https://www.fcc.gov/general/fcc-health-it-actions-and-activities-timeline.
7. https://www.fcc.gov/document/fcc-seeks-comment-accelerating-broadband-health-tech-availability.
8. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.
9. https://oig.hhs.gov/oas/reports/region18/181630530.pdf.
10. https://oig.hhs.gov/oas/reports/region18/181630530.pdf.
11. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf.
12. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf.
13. https://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm623568.htm.
14. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm623184.htm.
15. https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-01.
16. https://ics-cert.us cert.gov/sites/default/files/Annual_Reports/NCCIC_Year_in_Review_2017_Final.pdf, last visited 3/5/2019.
17. https://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM630544.pdf.
18. https://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM632316.pdf.
19. https://www.villageb.io/who-we-are-what-we-do.