Health Law Daily Wrap Up, STRATEGIC PERSPECTIVES: Hacked: A new kind of heart attack, (Mar. 16, 2018)

Health Law Daily Wrap Up

Click to open document in a browser

By Bryant Storm, J.D.

The health care industry is growing accustomed to the reality of cyberattacks. As storehouses of valuable data, health care providers are increasingly falling under threat of hackers, ransomware, and other network-based attacks. But cyberattacks do not begin and end at the facility level. As medical devices become more connected and network-reliant, they too are exposed to cyber threats. This Strategic Perspective highlights not only the growing risk of medical device cyber vulnerability, but also regulatory attempts to limit those vulnerabilities in both the U.S. and abroad.

Ways in Which the Threat Has Presented Itself

The idea of hackable medical devices first rose into national consciousness in 2013 when former Vice President Dick Cheney revealed that, in 2007, at the advice of his physician, he ordered the wireless functionality of his implanted defibrillator be turned off to thwart potential assassination attempts—a fear that was fictionalized in the television series *Homeland.* While early reactions relegated the idea of a hacked heart implant into the realm of the sensational and paranoid, the risks are real and growing. Medical devices *are* vulnerable to cyberattacks—a dismaying fact that has now been demonstrated in the lab as well as the real world (see *Medical device cybersecurity: Staying safe in the midst of change*, August 11, 2017).

Research. Researchers in Belgium and the United Kingdom set out to determine whether implantable medical devices—things like pacemakers, defibrillators, and insulin pumps—could be subject to life-threatening or fatal network-based attacks. In December 2016, the researchers concluded that the latest generation of Implantable Cardioverter Defibrillators (ICDs) could be reverse-engineered using "commercial and inexpensive equipment." In the course of the study, researchers were able to conduct attacks designed to drain a device's battery life and violate patient privacy.

Early warnings. In 2015, the FDA and the Department of Homeland Security warned of security vulnerabilities in an infusion pump system (see *Dump hackable drug pump, FDA says*, August 3, 2015).

Cardiac equipment. In May 2017, a hospital's radiology equipment was allegedly infected with WannaCry ransomware—the first time such an attack was known to affect a medical device, putting to bed any doubts about the real-world vulnerability of devices.

Simulated hacking. In June 2017, the University of Arizona Medical School in Phoenix held a simulated cyberattack where "white-hat hackers" (ethical, rather than criminal, hackers) attacked a simulated hospital and its three mock patients. The white-hat attackers succeeded in hacking a bedside infusion pump, a pacemaker, and an insulin pump. The hacked devices were caused to malfunction and administer inappropriate doses.

Pacemaker. In August, 2017, in another first and following a class action complaint from a patient implanted with the device, the FDA issued a firmware related recall on an Implantable Cardiac Pacemaker (see *Class action complaint filed as St. Jude's Medical responds to cybersecurity allegations*, August 31, 2016). In its announcement, the FDA called the move "a corrective action, to reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities." Specifically—and with startling similarity to the findings of the UK study and Arizona simulation—the FDA received evidence that someone other than a patient's physician could access a patient's device using commercially available equipment. Such access "could be used to modify programming commands to the implanted pacemaker, which could result in patient harm from rapid battery

depletion or administration of inappropriate pacing," the FDA said (see *Cyberattack possible against doctors monitoring patients with St. Jude cardiac devices*, February 8, 2017).

FDA Guidance

Despite the clear evidence of cyber risk for medical devices, regulators are only beginning to address this nascent threat. While some legislative attempts (discussed below) have been put forth by lawmakers, for now, most of oversight of medical device vulnerability stems from guidance and recommendations, some of which is based upon extant medical device and privacy laws, like the Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191) and the federal Food, Drug, and Cosmetic Act (FDC Act) (21 U.S.C. §301 et seq.). The most concrete action taken to date by the FDA is a guidance: *Postmarket Management of Cybersecurity in Medical Devices*. The guidance was finalized on December 28, 2016. The guidance encourages manufacturers "to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device." The guidance pertains to both medical devices that contain software and software that is a medical device. According to the guidance, manufacturers "should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices." The agency notes, however, that most medical device cybersecurity updates and patches constitute routine updates that do not require reporting under 21 C.F.R. part 806 (see *FDA focuses on postmarket cybersecurity for medical devices*, December 28, 2016; *FDA tackles postmarket medical device cybersecurity*, April 29, 2016).

When considering the impact of the guidance, Ashley Thomas of Baker Donelson noted that manufacturers should remember that neither FDA nor Federal Trade Commission (FTC) guidance on the cybersecurity of medical devices "create legally enforceable responsibilities." However, she said, despite their non-mandatory nature, "manufacturers should still consider and study these documents and dedicate resources to preventing and mitigating cybersecurity threats."

Postmarket. The FDA has also issued a factsheet explaining its role in the oversight of medical device cybersecurity, however, the factsheet does not establish new protocols for medical device cybersecurity. Instead, the FDA answers basic questions about its regulations of devices, by clarifying that it does not test medical devices for cybersecurity and, according to the factsheet, the FDA "does not typically need to review changes made to medical devices solely to strengthen cybersecurity." Thomas said that while the FDA places the onus for premarket testing for cybersecurity of medical products on the manufacturer, "the FDA is more focused on monitoring and addressing cybersecurity vulnerabilities once the medical devices are on the market." Thus, she suggested, "in order to modify to FDA's role, congressional action will likely be needed to address some of these gaps."

Premarket. Diane Romza-Kutz, a partner at Thompson Coburn, noted that the FDA does not turn a blind eye on all premarket evaluation of device security. For example, "when the FDA, through its approval process for medical devices, reviews a device with a software component, it does review the safety and efficacy of the software as part of its total evaluation. In doing so, it looks to the safeguards that are in place to keep the data flowing through the device secure and free from hacking."

Additionally, while the FDA has, to date, only issued guidance on the subject, Romza-Kutz noted that "these actions, by far, outdistance other regulatory bodies in other jurisdictions/countries. Although other countries recognize the cybersecurity risks and have promulgated regulations and policies accordingly, the United States appears to be the most proactive in applying those more wide-ranging concerns directly to medical devices and software for those devices."

The current state of the FDA's guidance should not be seen as static. Romza-Kutz predicted that, "it is highly likely, particularly in light of the FDA's focus on digital health that guidance and oversight in this area will continue and likely evolve as risks are better identified and new breaches occur."

Addressing Cybersecurity in Other Jurisdictions

Although the regulation of medical device cybersecurity remains a new concept, different jurisdictions have begun to lay foundations for addressing the problem.

United Kingdom. In a move similar to the one employed by the University of Arizona, the United Kingdom's National Health Service reportedly is going to spend £20 million on a unit of ethical hackers whose job will be to monitor internet-related weaknesses in the health care system.

Europe. The European model of oversight, like the one in the U.S., is based largely on recommendations or interpretation of extant laws that bear some relation to device security. To date, there is little in the way of explicit medical device cybersecurity law or regulation.

ENISA recommendations. The European Union Agency for Network and Information Security (ENISA)—the European Union's group for information security expertise—developed baseline security recommendations for The Internet of Things (IoT). These high level recommendations cite the FDA's position (Guidance) regarding Medical device cybersecurity. The recommendations are designed, in part, to prepare manufacturers for the upcoming (May 25, 2018) implementation of the European General Data Protection Regulation (GDPR)—Europe's new data security law (see *The clock is ticking...Does your organization need to worry about GDPR compliance?*, February 23, 2018).

The recommendations note that privacy should be a "guiding principle" in device design and development. Additionally, privacy impact assessments should be conducted prior to the launch of new devices.

GDPR. Thomas warned that manufacturers should be cautious with the GDPR because it "will regulate some healthcare data that falls outside of HIPAA's scope." For example, "many organizations that collect health information fall outside the scope of HIPAA like companies that manufacture fitness trackers, mobile apps or cloud-based tools that store and share health information for individual users." Additionally, she cautioned that the "failure to comply with the GDPR can result in severe penalties, much steeper than penalties for HIPAA violations. For any non-compliance with key provisions of the GDPR, regulators have the authority to levy a fine in an amount that is up to the greater of €20 million or 4 percent of the company or organization's global revenue, which is the maximum fine possible for serious infringements."

Melissa Ventrone, partner and chair of the cybersecurity practice at Thompson Coburn and vice chair of the Cyber Security, Data Privacy and Technology Committee of the International Association of Defense Counsel, told Wolters Kluwer "while GDPR and HIPAA may not regulate medical devices directly, they do apply to the information collected by the medical devices." Ventrone raised an additional risk area that those familiar with HIPAA but unfamiliar with the GDPR might miss. She said, "GDPR, unlike HIPAA, has a 'right to be forgotten'—organizations that collect health data must be prepared to delete such information once the purpose for collecting or storing the data no longer exists. HIPAA does not contain any limitations on the deletions of such information—while inadvisable, organizations may store health information indefinitely."

MDR. The European Medical Device Regulations (MDR) were published on May 5, 2017, and came into force on May 25, 2017. Manufacturers of currently approved medical devices have a transition time of three years until May 26, 2020, to meet the requirements of the MDR. The MDR does include some software requirements that address data-privacy and cybersecurity. Specifically, the MDR calls for "minimum requirements on hardware, [information technology] IT networks characteristics and IT security measures, including protection against unauthorized access."

International. There are ongoing initiatives intended to address some of the issues raised by global compliance, according to Ventrone. "The International Medical Device Regulators Forum (IMDRF) was founded in 2011 and is a voluntary group that is composed of regulatory officials with the goal to 'accelerate international medical device regulatory harmonization and convergence.'"

Standards and Recommendations

Standards organizations have had a strong influence on current device security oversight. Standards can serve as an important starting ground for regulation and are often widely adopted at regional and national levels. The influence of standards in the U.S. is apparent, with the FDA citing ISO 14971 in its guidance on the device

cybersecurity. The standard 14971 specifies a process for a manufacturer to identify the hazards associated with medical devices, including methods to evaluate, monitor, and control risks.

Other organizations have also weighed in on the issue. In June 2017, the Health Care Industry Cybersecurity Task Force issued its "Report on Improving Cybersecurity in the Health Care Industry," which provides recommendations and specific action items on how to secure medical devices (see *Task Force diagnosis: Health care cybersecurity in critical condition*, June 5, 2017). This report, along with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF), was cited by the FDA in its guidance.

Congressional Actions

The U.S. Congress has made some attempts to reach beyond guidance documents and standards to more substantially regulate the cybersecurity of devices.

MDCA. On July 27, 2017, Senator Richard Blumenthal (D-Conn) introduced the Medical Device Cybersecurity Act of 2017 (S.1656) in the Senate. The bill would amend the FDC Act to require the FDA to establish a cybersecurity report card for medical devices with network capabilities. If passed, the law would require the report card to contain "(1) information pertaining to the essential elements described in the most recent version of the Manufacturer Disclosure Statement for Medical Device Security; (2) a cybersecurity risk assessment conducted by the manufacturer or third party; and (3) whether the device is capable of being accessed remotely." Device manufacturers would be required to include completed device report cards as part of the device approval process.

Thomas said the proposed legislation "is a step in the right direction and did incorporate some recommendations from HHS' Health Care Industry Cybersecurity Task Force report." She noted that "it helps bolster the FDA's cybersecurity guidance and reinforce the necessity for implementing cybersecurity measures. The cyber report card may be helpful to hospitals and providers showing them which devices may pose more risk. However, there is a concern it will put more work on the FDA, when the agency's resources are already stretched out."

Echoing Thomas' position, Romza-Kutz and Ventrone said, "while this may not be the answer to all risks associated with the connectivity and cybersecurity of medical devices, especially in an area where technology is changing so quickly, it is certainly a good start."

IMTRPA. On October 5, 2017, the Internet of Medical Things Resilience Partnership Act of 2017 (IMTRPA) (H.R.3985) was introduced in the House. The legislation would establish an FDA-headed working group tasked with developing strategies for mitigating cybersecurity risks in medical technology. Under the law, the FDA would be required to report on its findings within 18 months of the passage of the law. Romza-Kutz and Ventrone believe that IMTRPA is a bill "which will most likely not pass."

Hearing. Additionally, the House Energy and Commerce Committee's Subcommittee on Oversight and Investigations convened a hearing in July 2017 on health care security efforts (see *Oversight subcommittee probes HHS health care cybersecurity efforts*, June 8, 2017).

The Future Security of Devices

The threat of cyberattacks has permeated the health care industry and reached medical devices. Stakeholders must act quickly to step up medical device security. Thomas put it this way: "There is an uncomfortable realization within the healthcare industry that it's not a matter if a cyberattack will happen but when it will happen thus making it making critical that health systems and device manufacturers implement security measures to diminish any harmful effects."

Attorneys: Ashley Thomas (Baker Donelson). Diane Romza-Kutz and Melissa Ventrone (Thompson Coburn LLP).

MainStory: StrategicPerspectives EnforcementNews FraudNews HITNews MDeviceNews SafetyNews