2014 ISSUE 2 A POINT OF VIEW ON INDUSTRY ISSUES

LIFE SCIENCES POV℠

Medical Device Cybersecurity: An Emerging Area of Risk

By Gretchen A. Ramos

The U.S. Food and Drug Administration (FDA) defines cybersecurity as the "process of preventing unauthorized modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient."[1]

Cybersecurity incidents most commonly involve disclosure of financial data or protected health information (PHI). Such security breaches have grown steadily over the last decade. The Identity Theft Resource Center reports that more than 4,000 recorded breaches have occurred since 2005, resulting in disclosure of approximately 600 million individual records. Healthcare accounted for more incidents than any other industry, with the 267 reported healthcare-related breaches in 2013 resulting in close to 5 million records being disclosed.[2] The average cost of a healthcare organization breach incident is $2.4 million.[3]

Disclosure of sensitive data is not the only potential healthcare cybersecurity hazard. Many medical devices – such as ventilators, imaging equipment, patient monitors and infusion pumps – may be vulnerable to hackers, as they contain configurable embedded software and are accessible via wireless technology or hospital networks. A medical device breach thus could result in bodily injury or death – a concern that is garnering increased attention.[4]

While the FDA has not identified any patient injuries or deaths associated with cybersecurity incidents, medical device vulnerabilities have been documented.[5] In 2010, a Veterans Affairs (VA) official reported to Congress that during the prior 14 months, over 122 medical devices at VA facilities had been compromised by malware.[6] Furthermore, in June 2013, the FDA Center for Devices and Radiological Health, together with the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), identified hard-coded password vulnerability affecting about 300 devices from 40 vendors, which could be exploited to potentially change critical settings or modify device firmware.[7] And an information technology research and consulting group predicts that by 2016, "patients will be harmed or placed at risk by a medical device security breach."[8]

Many medical devices may be vulnerable to hackers, as they contain configurable embedded software and are accessible via wireless technology or hospital networks.

1 "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Draft Guidance for Industry and Food and Drug Administration Staff" (June 14, 2013), available at **http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm**. Last accessed February 5, 2014.

2 "Data Breaches," 2005 to March 4, 2014, available at **http://www.idtheftcenter.org/id-theft/data-breaches.html**. Last accessed March 13, 2014.

3 *2013 Cost of Data Breach Study: Global Analysis*, a Ponemon Institute© Research Report (May 2013), available at **http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach**.

4 Examples of media attention include a *60 Minutes* report (October 20, 2013) that former Vice President Dick Cheney had the wireless feature on his implanted defibrillator disabled in 2007 to prevent possible assassination attempts; available at **http://www.cbsnews.com/news/dick-cheneys-heart/**. Last accessed February 4, 2014. The threat of medical device hacking has also been featured recently on popular television shows (e.g., "Homeland") and video games (e.g. "Arkham Origins"). See **http://www.massdevice.com/blogs/arezu-sarvestani/when-good-guys-hack-batman-can-hack-pacemakers**, (December 30, 2013). Last accessed February 5, 2014.

5 See the FDA's Medical Device Cybersecurity statement (updated November 1, 2013), available at **http://www.fda.gov/medicaldevices/productsandmedicalprocedures/connectedhealth/ucm373213.htm**.

6 Testimony of Roger W. Baker, Assistant Secretary for Information and Technology, U.S. Department of Veterans Affairs to the House Committee on Veterans' Affairs Subcommittee on Oversight and Investigations, May 19, 2010, at **http://www.va.gov/OCA/testimony/hvac/soi/100519RWB.asp.**

7 See ICS-ALERT-13-164-01: "Medical Devices Hard-Coded Passwords," revised October 29, 2013, available at **http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01**. Last accessed May 22, 2014.

8 See Gartner, Inc. press release, December 19, 2012, available at **http://www.gartner.com/newsroom/id/2282715**. Last accessed February 5, 2014.

UNDERSTANDING THE RISKS

Manufacturers of medical devices that are networked or contain embedded software may find themselves liable if they neglect to protect against possible cybersecurity attacks. For example, a hacker could:

- Remotely shut off an implantable medical device (such as an insulin pump) without the patient's knowledge.
- Manipulate a device's settings, in order to disturb or alter its functioning.
- Deny access to individual devices or to an entire device network.
- Eavesdrop on wireless communication.
- Obtain PHI or other personally identifiable information.

Once targeted, medical device manufacturers could encounter problems ranging from data theft and malicious tampering to device malfunction. Potential consequences of such an occurrence include, but are not limited to, the following:

- Regulatory enforcement actions, monetary penalties and / or criminal prosecution.
- Lawsuits and class actions alleging breach of privacy.
- Negative publicity that could adversely affect brand image, value or reputation.
- Product liability claims alleging bodily injury or economic loss.
- Business interruption caused by a data security breach, resulting in loss of revenue.
- Negligence *per se* claims alleging failure to follow FDA and other standards.
- Recall and other incident mitigation efforts and expenses.
- Costs associated with complying with breach notification requirements.
- Securities fraud class action lawsuits filed by shareholders.

REGULATORY DEVELOPMENTS

A number of different federal regulatory agencies – including the FDA, the Federal Communications Commission, the Federal Trade Commission, the Office of the National Coordinator for Health Information Technology, the Office for Civil Rights of the U.S. Department of Health & Human Services (HHS), and the Securities and Exchange Commission (SEC) – have promulgated standards for medical device privacy and security. The National Institute of Standards and Technology then works to develop consistent, cross-agency standards. Individual states also have adopted related regulations.

Notable recent regulatory changes affecting medical device privacy and security include the following:

- The FDA's "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (cited on page 1) encourages device manufacturers to consider cybersecurity issues during the design phase. Among other recommendations, the guidance instructs manufacturers to limit access to trusted users, restrict software and firmware updates to authenticated code, and use "fail safe" and recovery features that protect the device's critical functionality even when security is compromised. In addition, manufacturers are advised to define and document cybersecurity measures to be included in premarket submissions, and include information on antivirus software in instructions for use and specifications.
- "FDA Safety Communication, Cybersecurity for Medical Devices and Hospital Networks" notes that medical device manufacturers are responsible for "identifying risks and hazards associated with their medical devices, including risks related to cybersecurity, and are responsible for putting appropriate mitigations in place to address patient safety and assure proper device performance."[9] The draft guidance also signals some regulatory flexibility, stating that "FDA typically does not need to review or approve medical device software changes made solely to strengthen cybersecurity."
- In 2013, the FDA released final guidance on incorporating protective measures into devices equipped with radio frequency (RF) wireless technology.[10] The agency recommends that manufacturers "address known safety issues involving RF wireless technologies early in the device design and development process" – language nearly identical to that used in its cybersecurity guidance.

9 This FDA Safety Communication (June 13, 2013) is available at **http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm**. Last accessed February 4, 2014.

10 "Radio Frequency Wireless Technology in Medical Devices – Guidance for Industry and Food and Drug Administration Staff" (August 13, 2013) is available at **http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm077210.htm**. Last accessed February 5, 2014.

- The FDA announced the final rule for the Unique Device Identification (UDI) system on September 23, 2013, which will make it easier for manufacturers and regulators to identify problems with medical devices via adverse event reports.[11] The UDI system has two core elements: a number assigned by the device manufacturer to each version or model of a device, and the Global Unique Device Identification Database (GUDID), which will serve as a reference catalog for every device with such an identifier. The UDI system will enable companies to more easily notify individual users when a manufacturer issues a product recall or safety notice. The system also will permit individuals to more easily identify the manufacturer of an injury-causing product, and help regulators identify adverse trends associated with a particular device. The GUDID will be made accessible to the public and will contain no information about individual users.
- HHS extended HIPAA's privacy and security requirements to contractors, subcontractors and other entities that capture protected health data in their work on behalf of a HIPAA-covered entity.[12] Although the June 2013 FDA Draft Guidance does not specifically mention HIPAA or HITECH, the agency may consider an organization's degree of compliance with these acts when evaluating medical device cybersecurity. In assessing whether HIPAA and / or HITECH apply, a medical device manufacturer must determine whether the information it collects is PHI, if a "covered entity" is involved and if a "business associate" relationship exists with the covered entity.[13] HHS has noted that medical device companies qualify as business associates if their work with covered entities requires the use or disclosure of PHI. When acting in this capacity, medical device manufacturers must enter into a business associate agreement with the covered entity customer. Prior to passage of HITECH, a business associate was only contractually liable to a covered entity. Now, however, business associates are *directly* subject to significant portions of HIPAA's privacy, security and breach notification rules, and they may face civil or criminal penalties if they fail to comply with HIPAA.
- The FDA released a new list of updated medical device standards, which clarify current good manufacturing practices and other review requirements.[14] Some of the standards – e.g., those relating to establishing roles and responsibilities for IT networks, communicating device security needs and risks, and securing wireless networks – involve cybersecurity concerns.
- While it does not establish a new requirement, the SEC's 2011 "CF Disclosure Guidance" outlines the Division of Corporation Finance's views regarding the disclosure obligations of publicly traded companies relating to cybersecurity risks and cyber incidents.[15] The SEC requires disclosure of:
  - Known or threatened cyberattacks.
  - Cyber incidents that have materially affected a company's products, services or relationships with customers.
  - Costs related to a cyber incident.
  - Any related legal proceedings.
  - Relevant insurance coverage with respect to potential cyber exposures.

Business associates are now directly subject to significant portions of HIPAA's privacy, security and breach notification rules, and they may face civil or criminal penalties if they fail to comply with HIPAA.

11 The FDA's "UDI Rule and GUDID Guidance" is available at **http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/**. Last accessed February 5, 2014.

12 "Modifications to the HIPAA Privacy Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules," *Federal Register*, January 25, 2013, Volume 78:17, pages 5565-5702, Rules and Regulations. Available at **https://federalregister.gov/a/2013-01073**.

13 HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414. Available at **http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html**,

14 "Food and Drug Administration Modernization Act of 1997: Modifications to the List of Recognized Standards, Recognition List Number: 032" (August 6, 2013), available at **http://www.gpo.gov/fdsys/pkg/FR-2013-08-06/pdf/2013-19020.pdf**. Last accessed February 5, 2014.

15 "CF Disclosure Guidance: Topic No. 2, Cybersecurity" (October 13, 2011), available at **http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm**. Last accessed March 14, 2014.

RISK MANAGEMENT STRATEGIES

The following suggestions can assist manufacturers of networked and wireless healthcare devices in reducing exposure to cybersecurity-related liability:

- *Work with an insurance broker to evaluate exposure to the full range of cybersecurity risks,* as well as current insurance coverage. Remember that emerging cybersecurity threats may not be covered under existing insurance policies.
- *Conduct a hazard analysis of existing medical device products,* including both intentional and unintentional cybersecurity risks. Although the FDA's draft cybersecurity guidance applies to premarket devices, consider extending it to devices already on the market, as it represents the agency's current views regarding best practices, and can serve as a baseline for addressing known risks and reducing liability exposure.
- *Address cybersecurity and interoperability concerns when designing and updating medical devices,* utilizing the regulatory and guidance material noted above, as well as industry resources.[16]
- *Consider the possibility of cyber attacks and related hazards* when investigating device-related adverse events.
- *Periodically assess the vulnerabilities of networked medical device products,* as well as their compliance with FDA regulations, HIPAA, HITECH and other applicable laws.
- *Review device instructions and labels* to ensure that they adequately warn of cybersecurity risks.
- *Develop a detailed incident response plan,* and have external security experts available for rapid response should an incident occur.
- *Document all actions taken* to address cybersecurity risks.

16 One source of information and resources is the Medical Device Innovation, Safety and Security Consortium (**http://www.mdiss.org/**), a nonprofit association dedicated to advancement of computer risk management practices.

Medical device cybersecurity is a large and growing concern. By developing sound, proactive risk management strategies, providers and facilities can enhance compliance, protect patients and reduce their liability exposure.

Gretchen A. Ramos is a litigation partner at Carroll Burdick & McDonough. She is a certified information privacy professional, who regularly counsels companies on U.S., European and worldwide data protection laws. She provides advice on privacy policies and procedures; security audits; data breaches; regulatory investigations; laws regarding commercial email, telemarketing, direct mail and advertising; cross-border data transfers; consumer protection laws; and data breach class actions.

CNA

For more information, please call us at 888-600-4776 or visit www.cna.com.