AHLA WEEKLY
3/24/2017

Hacking of Medical Devices Is No Longer Just an Outlandish Movie Plot

By Erica Mallon, Carlton Fields

2016 was a big year for health care data breaches with 106 major hacker-attributed breaches reported to the federal government, exposing 13.5 million individuals' records.[1] According to a June Ponemon Institute/IBM report on data breaches, loss of a single record cost health care institutions an average of $402, which adds up to $2.8 billion spent on 2016 hacking incidents.[2]

Between November 2015 and August 2016, five entities alone agreed to pay the Department of Health and Human Services Office for Civil Rights (OCR) $16 million related to electronic patient data breaches.[3] 2015 was a busy year as well with 80 million Anthem members' data compromised in January, 11.2 million Premera BlueCross BlueShield members' and business affiliates' data compromised in March, and 1.1 million CareFirst BlueCross BlueShield members' data compromised in May. And on February 16, 2017, OCR announced a $5.5 million settlement with Memorial Healthcare System regarding potential violations of the Health Insurance Portability and Accountability Act (HIPAA), the second largest settlement in history for potential HIPAA violations.[4] Hackers are becoming more creative in their methods of infiltration, and there is significant concern that hacking of medical devices and hospital networks will be the tactic of the future.

According to a January 2015 Federal Trade Commission (FTC) report titled *Internet of Things: Privacy & Security in a Connected World*, in 2009, for the first time, the number of "things" connected to the Internet surpassed the number of people in the world.[5] In early 2016, technology consulting firm Gartner projected that 6.4 billion connected things would be in use worldwide by the end of the year, up 30% from the previous year, and that the number of connected things would grow by more than three times, to nearly 21 billion by the year 2020.[6] While these devices can significantly improve the lives and health of consumers worldwide, significant risks exist as well.

Experts have expressed concern that cybersecurity is not keeping pace with medical technology advancement, and that unlike the hacking of a bank account or email server, such cybersecurity risks can truly mean life or death for a victim. Some experts allege that one thing health care recruiters are missing, but their counterparts in other industries are not, is getting a head start on recruiting and developing cybersecurity talent specializing in the health care industry.[7] This is a niche industry for which there will be a growing need as medical technology continues to advance.

The issue of medical device hacking made headlines in August 2016 when cybersecurity and research company MedSec Holdings Ltd. (MedSec) discovered potential security vulnerabilities in St. Jude Medical Inc.'s (St. Jude) pacemakers and defibrillators.[8] Instead of disclosing these vulnerabilities, MedSec reportedly went to Muddy Waters Capital LLC, an investment firm, with a money-making proposal. MedSec reportedly suggested that it would provide data proving the medical devices were vulnerable to life-threatening hacking, with Muddy Waters short-selling St. Jude's stock after the vulnerability was announced.[9] According to published reports, MedSec's fee for the information increased as the price of St. Jude's shares fell, and both Muddy Waters and MedSec made a generous profit when more than 25 million shares were traded after the security vulnerability was announced.[10]

St. Jude disputed the vulnerability claims and filed suit alleging that the entire scheme had been made up to manipulate its stock price and that MedSec and Muddy Waters, as well as three other individuals, falsely reported such vulnerabilities and risks.[11] The Food and Drug Administration (FDA), in collaboration with the Department of Homeland Security, launched an investigation into the vulnerabilities in August 2016. On January 9, 2017, the FDA issued a Safety Communication confirming vulnerabilities in St. Jude Medical's implantable cardiac devices and Merlin@home Transmitter.[12] Shortly thereafter, St. Jude Medical, which has since been acquired by Abbott Laboratories (Abbott), released an update for certain medical devices containing a patch for vulnerabilities made public in the MedSec and Muddy Waters controversy. While no patients were injured by the alleged vulnerability, the allegation rocked St. Jude's reputation, threatened to derail its transaction with Abbott, and revealed a new money-making strategy for short-sellers and cybersecurity firms that uncover potential vulnerabilities.

As the St. Jude controversy unfolded, Johnson & Johnson became the first medical device manufacturer to warn patients about a cyber vulnerability when it advised patients in October 2016 that one of its older model insulin pumps had a cybersecurity bug that a hacker could exploit to overdose diabetic patients with insulin.[13] The company provided guidance on how patients could fix the problem to prevent hacking and no patients were injured.

While some of the concern lies with a risk to patients if their devices are hacked, perhaps the greatest risk lies in the ability of hackers to access hospital networks through the hacking of medical devices. Hospital networks are prime targets for hackers because many contain expansive amounts of highly personalized and confidential data.

In June 2015, TrapX, a firm specializing in deception-based cybersecurity defense, released a report finding that attackers targeted and compromised blood gas analyzers and radiology picture archive and communications systems (PACS) to gain access to hospital networks.[14] Furthermore, TrapX suggested in its report that an attacker could remotely hack a hospital drug pump and modify the amount of medication to a fatal dose.

In early 2016, Hollywood Presbyterian Medical Center, a California hospital, paid a $16,664 ransom in bitcoins to hackers who infiltrated and disabled the hospital's computer network.[15] It is likely other similar attacks have occurred but not been publicized to help maintain public confidence in hospitals' ability to keep information private and secure.

Both the FDA and the FTC have provided guidance on cybersecurity in medical devices. In late 2014, the FDA issued guidance on premarket management of cybersecurity in medical devices, calling for manufacturers to consider cybersecurity risks in designing and developing medical devices.[16] In early 2015, the FTC issued guidance on best practices for privacy and security protection, including guidance on the design, deployment, and management of medical devices.[17] The FDA issued updated guidance in December 2016 on postmarket management of cybersecurity in medical devices.[18]

Neither the FTC nor the FDA guidance creates legally enforceable responsibilities related to cybersecurity of medical devices. However, mandatory regulations may be enacted in the future as the risks become more significant and palpable. And whether or not such responsibilities are legally enforceable, it is highly recommended that medical device manufacturers consider such guidance and dedicate significant energy and capital into protecting against cybersecurity threats.

All parties involved in the development and maintenance of medical devices should be aware of the applicable cybersecurity risks. The developers who create these devices, the providers who maintain them, and the consumers who use them need to take appropriate safeguards to ensure patients' safety and privacy. Compliance with the non-mandatory guidance and best practices issued by the FTC and FDA offer a good starting point.

Erica Mallon is an associate attorney in the health care practice group of Carlton Fields (Tampa, FL). She may be contacted at (813) 229-4129 or emallon@carltonfields.com.

[1] Joseph Conn, *Vital Signs: How America's Youth is Key to Fixing the Sad State of Cybersecurity*, Modern Healthcare, Jan. 20, 2017, *available at* www.modernhealthcare.com/article/20170120/BLOG/170129995/vital-signs-how-americas-youth-is-key-to-fixing-the-sad-state-of.

[2] IBM*, 2016 Cost of Data Breach Study: United States*, Ponemon Institute Research Report, June 2016.

[3] Dan Mangan, *Why 2016 Could be Banner Year for Health-Care Data Breach Fines*, CNBC*,* Aug. 5, 2016, *available at* www.cnbc.com/2016/08/05/why-2016-could-be-banner-year-for-health-care-data-breach-fines.html.

[4] U.S. Department of Health and Human Services*, $5.5 Million HIPAA Settlement Shines Light on the Importance of Audit Controls*, Feb. 16, 2017, *available at* https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html.

[5] U.S. Federal Trade Commission, *Internet of Things*, FTC Staff Report, Jan. 2015.

[6] Julia Boorstin, *An Internet of Things That Will Number Ten Billions*, CNBC*,* Feb. 1, 2016, *available at* www.cnbc.com/2016/02/01/an-internet-of-things-that-will-number-ten-billions.html.

[7] Conn, *supra* note 1.

[8] Jordan Robertson and Michael Rile, *Carson Block's Attack on St. Jude Reveals a New Front in Hacking for* Profit, Bloomberg, Aug. 25, 2016, *available at* www.bloomberg.com/news/articles/2016-08-25/in-an-unorthodox-move-hacking-firm-teams-up-with-short-sellers.

[9] *Id.*

[10] Id.

[11] *St. Jude Medical v. Muddy Waters Consulting*, No. 0:16-cv-03002 (D. Minn. Filed Sept. 7, 2016).

[12] U.S. Food & Drug Administration, *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter*, FDA Safety Communication, Jan. 9, 2017.

[13] *Insulin Pump Vulnerable to Hacking, Johnson & Johnson Warns*, NBC News*,* Reuters, Oct. 4, 2016, *available at* www.nbcnews.com/health/health-news/insulin-pump-vulnerable-hacking-johnson-johnson-warns-n659221.

[14] TrapX Labs, *Anatomy of an Attack*, Security Ledger*,* May 7, 2015.

[15] *California Hospital Paid $17,000 Ransom in Bitcoins to Hackers*, Chicago Trib., Feb. 17, 2016, *available at* www.chicagotribune.com/news/nationworld/ct-california-hospital-ransom-hackers-20160217-story.html.

[16] U.S. Food & Drug Administration Center for Devices and Radiological Health, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, Oct. 2, 2014.

[17] U.S. Federal Trade Commission, *supra* note 5.

[18] U.S. Food & Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff, Dec. 28, 2016.