Minnesota Journal of Law, Science & Technology

Volume 19 | Issue 2 Article 4

6-2018

Securing the Internet of Healthcare

Scott J. Shackelford

Michael Mattioli
Indiana University Maurer School of Law

Steve Myers

Austin Brady

Follow this and additional works at: https://scholarship.law.umn.edu/mjlst

Part of the Computer Law Commons, Health Law and Policy Commons, Internet Law Commons, and the Science and Technology Law Commons

Recommended Citation
Scott J. Shackelford, Michael Mattioli, Steve Myers & Austin Brady, *Securing the Internet of Healthcare*, 19 MINN. J.L. SCI. & TECH. 405 (2018).
Available at: https://scholarship.law.umn.edu/mjlst/vol19/iss2/4

The Minnesota Journal of Law, Science & Technology is published by the University of Minnesota Libraries Publishing.

Securing the Internet of Healthcare

Scott J. Shackelford, JD, PhD*, Michael Mattioli, JD, Steve Myers, PhD***, Austin Brady****, Yvette Wang***** & Stephanie Wong******

Cybersecurity, which includes the security of information technology (IT), is critical to ensuring that society trusts, and therefore can benefit from, modern technology. Problematically, though, rarely a day goes by without a news story related to how critical data has been exposed, exfiltrated, or otherwise inappropriately used or accessed as a result of supply chain vulnerabilities. From the Russian government's campaign to influence the 2016 U.S. presidential election to the September 2017 Equifax breach of more than 140 million Americans' credit reports, cyber risk has become a topic of conversation in boardrooms and the White House, on Wall Street and main street. But these discussions often miss the problems replete in the expansive supply chains on which many of these products and services we depend on are built; this is particularly true in the medical device context. The problem recently made national news with the voluntary recall of more than 400,000 pacemakers that were found to be vulnerable to hackers, necessitating a firmware update. This Article explores the myriad vulnerabilities in the supply chain for medical devices, investigates existing FDA cybersecurity and privacy regulations to identify any potential governance gaps, and suggests a path forward to boost

---

© 2018 Scott J. Shackelford, Michael Mattioli, Steve Myers, Austin Brady, Yvette Wang & Stephanie Wong

* Chair, Indiana University-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Associate Professor, Indiana University Kelley School of Business.

** Associate Professor of Law, Maurer School of Law.

*** Associate Professor, Indiana University School of Informatics, Computing, and Engineering.

**** JD Candidate, Maurer School of Law.

***** JD Candidate, Maurer School of Law.

****** JD Candidate, Maurer School of Law.

cybersecurity due diligence for manufacturers by making use of new approaches and technologies, including blockchain.

I. Introduction 406
II. Key Issues in Securing the Internet of Healthcare.....409
III. How Blockchain Technology Can Improve Supply Chain Management and Security 414
IV. Medical Device Case Study 421
A. Overview of Modern Pacemaker Systems..... 423
B. Pacemaker Security Vulnerabilities 427
C. FDA Regulation of Medical Devices..... 429
D. HIPAA Security Rule..... 437
E. Federal Trade Commission Enforcement 438
V. Implications for Managers and Policymakers.....439
A. A Look at Medical Industry Cybersecurity Best Practices 440
B. AdvaMed Illustrative Example 448
C. Eskenazi Experience..... 450
D. A Global Note 451
VI. Conclusion.....453

I. INTRODUCTION

Cybersecurity, including the security of information technology (IT), is critical to ensuring that society trusts, and therefore can benefit from, modern technology. Problematically, though, rarely a day goes by without a news story related to how critical data has been exposed, exfiltrated, or otherwise inappropriately used or accessed resulting in that trust being undermined. From the Russian government's campaign to influence the 2016 U.S. presidential election[1] to the September 2017 Equifax breach of more than 140 million Americans' credit reports,[2] mitigating cyber risk has become a topic of conversation in boardrooms and the White House, on Wall Street and main street. This is increasingly the case, troublingly, among healthcare providers as both small practices and clinics

1. *See, e.g.*, Scott Shane & Mark Mazzetti, *Inside a 3-Year Russian Campaign to Influence U.S. Voters*, N.Y. TIMES (Feb. 16, 2018), https://www.nytimes.com/2018/02/16/us/politics/russia-mueller-election.html.

2. Seena Greesin, *The Equifax Data Breach: What to Do*, FED. TRADE COMMISSION (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

and major hospitals have been recent targets of ransomware campaigns. One variety, known as "Locky," is among the "most prolific types of ransomware" infecting, for example, the Hollywood Presbyterian Medical Center, resulting in "an 'internal emergency.'"[3]

Despite the gravity of cyber risk facing healthcare providers and patients, commentators seldom discuss an important source of such risk: the often-expansive supply chains medical device manufacturers depend upon.[4] Manufacturers of devices such as pacemaker systems purchase their components (e.g., microchips and software libraries) from multiple suppliers. As the number of such suppliers grows, so too does the number of opportunities potential wrongdoers can exploit. As the old proverb goes, a chain is only as strong as its weakest link. The problem recently made national news when the Food and Drug Administration (FDA) suggested a voluntary recall of more than 400,000 pacemakers that were found to be vulnerable to hackers, necessitating a firmware update.[5] This Article explores the vulnerabilities replete in the supply chain for medical devices, investigates both existing FDA cybersecurity and privacy regulations as well as industry codes of conduct to identify any potential governance gaps, and suggests a path forward to boost

---

3. Charlie Osborne, *Locky Ransomware Used to Target Hospitals Evolves*, ZDNET (Nov. 7, 2017, 9:00 AM PST), http://www.zdnet.com/article/locky-ransomware-used-to-target-hospitals-evolves/.

4. *See, e.g.*, Andy Greenberg, *Software Has a Serious Supply-Chain Security Problem*, WIRED (Sept. 18, 2017), https://www.wired.com/story/ccleaner-malware-supply-chain-software-security?mbid=nl_091817_daily&CNDID=%25%25CUST_ID%25%25 (explaining that consumers often hear warnings about websites or attachments in emails but are rarely warned about issues "further up the software supply chain").

5. *See* Press Release, FDA, Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (Formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication (Aug. 29, 2017), https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm [hereinafter Firmware Update]. However, some, such as Professor Kevin Fu have questioned the veracity of these claims. *See* Eliza Strickland, *Expert Questions Claim that St. Jude Pacemaker Was Hacked*, IEEE SPECTRUM (Sept. 2, 2016), https://spectrum.ieee.org/the-human-os/biomedical/devices/were-pacemakers-from-st-jude-medical-really-hacked; *see also* Lars Noah, *Turn the Beat Around: Deactivating Implanted Cardiac-Assist Devices*, 39 WM. MITCHELL L. REV. 1229, 1243 (2013) (investigating pacemaker vulnerabilities); W. Nicholson Price II, *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421, 461 (2017) ("FDA has expressed some interest in expanding this approach to some medical software, describing in mid-2017 a possible program where trusted software developers could face lighter premarket security.").

cybersecurity due diligence for manufacturers by making use of new approaches and technologies, including blockchain.

Myriad vulnerabilities exist in securing the Internet of Healthcare, from the 3D printing of medical devices[6] to foreign nation states interested in personal health records.[7] The problem is far too broad to meaningfully explore in a single article, underscoring the need for additional research in this area. To help narrow our investigation, we focus on the suitability of blockchain technology to help: (1) promote cybersecurity due diligence in vulnerable supply chains, and (2) better secure and anonymize health records. The investigation is structured as follows. Part I summarizes security issues facing the Internet of Healthcare, including the literature on the "Internet of Bodies," before focusing on supply chain concerns. Part II analyzes how blockchain technology can help address these security lapses. Part III reviews the lifecycle of a particular medical device—a pacemaker—and reviews the applicable federal and state cybersecurity requirements on manufacturers and hospitals using this device, along with how the Advanced Medical Technology Association (AdvaMed) is helping to create a cybersecurity code of conduct for industry. Part III also dives into the experience of one hospital, Eskenazi Health in Indianapolis, Indiana, to see how its administrators have implemented various safeguards to better secure their systems. Finally, Part IV focuses on implications for managers and policymakers interested in promoting cybersecurity due diligence in the healthcare industry. Ultimately, we propose that blockchain is a useful tool to help healthcare providers and manufactures mitigate certain supply chain and security risks but only as part of a larger universe of reforms needed to secure the Internet of Healthcare.

---

6. *See, e.g.*, Press Release, FDA, Statement by FDA Commissioner Scott Gottlieb, M.D., on FDA Ushering in New Era of 3D Printing of Medical Products; Provides Guidance to Manufacturers of Medical Devices (Dec. 4, 2017), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm587547.htm (discussing the FDA's work to regulate innovative medical technology, including 3D printing).

7. *See, e.g.*, Drew Harwell & Ellen Nakashima, *China Suspected in Major Hacking of Health Insurer*, WASH. POST (Feb. 5, 2018), https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html?noredirect=on&utm_term=.c7992683386c.

II. KEY ISSUES IN SECURING THE INTERNET OF HEALTHCARE

It is easy to summon up a potential "parade of horribles" when considering the myriad risks to the Internet of Healthcare generally, or the Internet of Medical Devices in particular. According to Zach Rothstein of the trade group AdvaMed, the scale and gravity of such risks is an open and "very loaded question."[8] Ben Esslinger, a clinical engineer at Eskenazi Health, agrees: "Cybersecurity is an emergency management issue. This is an epidemic in which vulnerabilities are being exploited, and it can directly impact patient care."[9] But what sorts of vulnerabilities concern hospital administrators and medical device manufacturers most? Everything from issues with integrating multiple devices and sensors with different operating systems, which at times are no longer being patched with security updates, to protecting vital systems from ransomware campaigns.[10] Privacy concerns can also complicate both the extent and manner in which data is stored on these disparate devices.[11]

To help balance security and privacy concerns in the healthcare setting, most organizations have adopted a risk-management approach, such as the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF).[12] However, it is difficult to reduce risk in the realm of

---

8. Interview with Zach Rothstein, AdvaMed, in Washington, D.C. (Jan. 22, 2018); *see About AdvaMed*, ADVAMED, https://www.advamed.org/about-advamed (last visited Feb. 16, 2018) ("The Advanced Medical Technology Association (AdvaMed), is a trade association that leads the effort to advance medical technology in order to achieve healthier lives and healthier economies around the world. AdvaMed's membership has reached nearly 300 members and more than 80 employees with a global presence in countries including Europe, India, China, Brazil, and Japan.").

9. Interview with Ben Esslinger, Clinical Engineer, Eskenazi Health, in Indianapolis, Ind. (Jan. 23, 2018).

10. *See* HEALTH CARE INDUS. CYBERSEC. TASK FORCE, REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY 2, 28 (2017), https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

11. *Id.* at 9–11.

12. For more on the NIST Cybersecurity Framework, see Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305 (2015).

medical information technology. Reasons for this include: (1) differing regulatory regimes of devices, as explored in Part III; (2) complicated systems of device use that include both physicians and patients as well as hospital IT groups; (3) the personal and private nature of many of the pieces of information that these devices can collect, broadcast, and manipulate; (4) lethal or otherwise catastrophic failure modes for some of these devices; and (5) unique constraints on computational ability and power due to the need for a device to be portable and possibly even embedded in a person for medical reasons.[13] Yet, despite these risks, the medical industry has been criticized for not being at the cybersecurity vanguard, as evidenced by the fact that many devices are now known to be susceptible to attacks.[14] Although evangelist groups such as "I Am The Cavalry" have been trying to publicize the issue for several years, the public has only just begun to appreciate these problems.[15] The recent ransomware attacks on the U.K.'s health system[16] seem to have raised the profile of the issue. Hollywood has also taken note: the show "Grey's Anatomy" recently featured a two-part episode about a hospital that succumbs to a combination of malware and ransomware.[17]

We next consider why cybersecurity risk reduction has been difficult in settings outside of healthcare, and explore why these problems may be further exacerbated in the medical field. The chief problems include: supply chain concerns, patching, management, and design. First, we need to consider the patient

---

13. HEALTH CARE INDUS. CYBERSEC. TASK FORCE, *supra* note 10, at 8–16, 18.

14. *See* Patrick Nohe, *The Healthcare Industry Is Lagging Behind on Cybersecurity*, SSL STORE (Feb. 14, 2018), https://www.thesslstore.com/blog/healthcare-industry-cybersecurity-2018/ (citing a 2018 Security Scorecard report that ranks the healthcare industry "fifteenth in terms of cybersecurity health when compared to 17 other major U. S. industries"); *see also* Firmware Update, *supra* note 5.

15. *I Am the Cavalry*, I AM CAVALRY, https://www.iamthecavalry.org/ (last visited Jan. 16, 2018) (explaining that "I Am The Cavalry" is a global grassroots organization which focuses on the intersection of computer security and human life).

16. *NHS 'Could Have Prevented' WannaCry Ransomware Attack*, BBC (Oct. 27, 2017), http://www.bbc.com/news/technology-41753022.

17. *Grey's Anatomy: Out of Nowhere*, IMDB, http://www.imdb.com/title/tt7043730/?ref_=ttep_ep8 (last visited Apr. 8, 2018); *Grey's Anatomy: 1-800-799-7233*, IMDB, http://www.imdb.com/title/tt7043736/?ref_=ttep_ep9 (last visited Apr. 8, 2018).

as part of the supply chain, which is admittedly a difficult undertaking given how complex these systems already are. The manufacturing process for Apple's iPhone, for example, involves dozens of suppliers, all of which are shipping, assembling, and warehousing components before the final product is delivered to an Apple store, or your door.[18] However, the limited runs for medical devices, at least when compared to the large runs that major corporations such as Apple and Amazon use for consumer devices, incentivize the reuse of commercial off-the-shelf hardware and software components whenever possible, and presumably the lowest cost supplier will win any bids for components.[19] This may make medical devices more susceptible to attacks such as by supply chain components having embedded malware.[20] The applicability of blockchain to help address supply chain issues is discussed in Part II.

The practice of installing patches on FDA-approved devices has a rocky history. Initially, manufacturers were unclear as to whether patching a device for security reasons necessitated a recertification under FDA guidelines, as is discussed further in Part III. In 2016, the FDA clarified that patching for cybersecurity that did not significantly affect the operation of a

---

18. *See* Ian Barker, *The Global Supply Chain Behind the iPhone 6*, BETA NEWS, https://betanews.com/2014/09/23/the-global-supply-chain-behind-the-iphone-6/ (last visited Apr. 21, 2018). All of these steps introduce numerous opportunities for security problems to arise; recent research has even suggested hackers could use smartphone apps to destroy manufacturing equipment or even destroy entire factories. *See* Martin Giles, *Hackers Could Blow Up Factories Using Smartphone Apps*, MIT TECH. REV. (Jan. 11, 2018), https://www.technologyreview.com/s/609946/hackers-could-blow-up-factories-using-smartphone-apps/. Similar research was also published in an online article. *See* Scott J. Shackelford, *Guarding Against the Possible Spectre in Every Machine*, CONVERSATION (Jan. 22, 2018), https://theconversation.com/guarding-against-the-possible-spectre-in-every-machine-89825.

19. *See* Bill Graham, *Reducing the Risk of the Software Supply Chain in Medical Devices*, GRAMMATECH BLOG, http://blogs.grammatech.com/reducing-the-risk-of-the-software-supply-chain-in-medical-devices (explaining that static analysis is one way to limit the risks of using third-party software).

20. *See, e.g.*, Fahmida Y. Rashid, *HP's Malware-Laden Switches Illustrate Supply Chain Risks*, PC MAG. (Apr. 12, 2012), https://securitywatch.pcmag.com/pc-hardware/296547-hp-s-malware-laden-switches-illustrate-supply-chain-risks (discussing an example of a supply chain issue that occurred during the production of HP Switches, the switches were shipped with infected SD cards that could pose a risk to computers if they were repurposed).

medical device did not require recertification.[21] Although this guidance has eased concerns, secure patching remains problematic for several reasons. First, because many devices are not consistently connected to the Internet, automatic patch download and deployment, which is standard for modern operating systems, is not an option.[22] Second, some devices need specialized medical equipment or medical practitioners to be present for the patch to be applied. For example, pacemakers are embedded in the patient and need specialized radios to transmit updates; further, limited battery lives may limit the number of times one can perform a power-hungry update process.[23] Third, the embedded nature of some medical devices means that they need to last a lifetime on a single battery and make the most efficient use of power possible. This can imply that traditional security means for ensuring the integrity and legitimacy of a patch cannot be deployed on some devices.[24]

Yet another problematic aspect of patching medical devices is two-fold: long service lifespans combined with the inclusion of embedded non-programmable firmware. Currently, such long-lived IT systems in nonmedical fields suffer from being vulnerable to long-known vulnerabilities that can be exploited by hackers since these devices cannot be easily reprogrammed, and thus patched, due to their embedded firmware.[25] While security is achieved in many subsystems by replacing the item with a newer version of the product, this is not a suitable strategy for implanted medical devices such as pacemakers, discussed in Part III. Inconveniently, however, replacing a vulnerable device is sometimes the only solution. The recently

---

21. *See* FDA, POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES 9 (2016), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

22. *See* Nourhene Ellouze et al., *Security of Implantable Medical Devices: Limits, Requirements, and Proposals*, 7 SECURITY COMM. NETWORKS 2475, 2476–79 (2014), https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.939 (explaining that due to power consumption limitations, fixes to security issues in implanted medical devices can be challenging).

23. *See id.*

24. *See id.*

25. *See* Jeff Kampman, *AMD Says CTS Labs Vulnerabilities Can Be Patched with New Firmware*, TECH. REP. (Mar. 20, 2018), https://techreport.com/news/33400/amd-says-cts-labs-vulnerabilities-can-be-patched-with-new-firmware; Kim Zetter, *Why Firmware Is So Vulnerable to Hacking, and What Can Be Done About It*, WIRED (Feb. 24, 2015), https://www.wired.com/2015/02/firmware-vulnerable-hacking-can-done/.

discovered "Spectre" and "Meltdown" hardware bugs affecting nearly all CPUs, for instance, can only be entirely eliminated when affected chipsets eventually fall out of use. Replacing an implanted medical device affected by a hardware bug is not so easily done.[26]

Beyond the challenges of patching software, medical devices require routine maintenance to ensure proper functioning, including accuracy, security, and privacy. This presents some distinct challenges. Managing medical devices often requires specialized medical knowledge, for instance. Moreover, several independent groups are frequently necessary to properly manage such devices when compared to non-medical systems. The groups who need to manage a device may include: (1) the device manufacturer, (2) a technician at a hospital or clinic, (3) the physician, (4) a home care assistant or nursing staff, and (5) the patient. Many of these groups will have differing educations, technical and medical backgrounds, and knowledge of the patient's status. Increasing the number of individuals with which a system needs to interact in order to function properly, all of whom frequently have different security and privacy classifications, adds significant design requirements and constraints and makes constructing such systems more difficult, and thus more susceptible to attacks.[27] Further, as previously mentioned, many of these devices will not have consistent Internet access, preventing them from being continuously monitored and updated as necessary. The lack of such live connection also limits the ability to centralize management, a technique that has successfully been used to improve security postures on devices while driving down maintenance costs.[28]

A large number of traditional computer networking and defense techniques become unusable or problematic in health settings. We provide two examples. First, recently a court subpoenaed the audit logs on an individual's pacemaker in

---

26. *See* Shackelford, *supra* note 18; Lily Hay Newman, *Medical Devices Are the Next Security Nightmare*, WIRED (Mar. 2, 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.

27. *See* Jeff Clark, *Is Complexity the Downfall of IT Security?*, DATA CTR. J. (Feb. 3, 2015), http://www.datacenterjournal.com/complexity-downfall-security/.

28. *See* Antone Gonsalves, *Plans to Centralize Cybersecurity with DHS Seen as Step Forward*, CSO (July 25, 2013), https://www.csoonline.com/article/2133770/malware-cybercrime/plans-to-centralize-cybersecurity-with-dhs-seen-as-step-forward.html.

relation to an arson case.[29] Should this practice become widespread, one can expect that consumers will insist on devices with limited or no logs in order to maintain their privacy. Second, embedded medical devices that have wireless radios such as Bluetooth or Wi-Fi may have unique identifiers built into the radio system that are broadcast on a continuous basis as part of the underlying radio protocol. Such identifiers are prolific and allow individuals to be tracked and geo-located through a number of different techniques. While this might be acceptable in a standard IT device that can be chosen not to be used, it is ethically more problematic on a device that must be worn.[30]

In general, though, Rothstein reports that AdvaMed views healthcare cybersecurity as a "shared responsibility," which resonates with the growing sentiment with regards to the utility of treating cybersecurity not just as an exercise in cost-benefit analysis, but as a social responsibility.[31] Moreover, Rothstein reports some success in working with various partners toward this common goal, but challenges remain:

> Even if manufactures put the best security in place, if other parts of the system are insecure, these efforts might not matter. It has to be a joint effort, meaning that all players from designers to patients need to be involved. But getting all the players on the same page and working together is the toughest part.[32]

III. HOW BLOCKCHAIN TECHNOLOGY CAN IMPROVE SUPPLY CHAIN MANAGEMENT AND SECURITY

The beginning of 2018 brought news that highlighted a longtime concern for security researchers: technological vulnerabilities can be rooted in hardware as well as software. Indeed, the hardware at the heart of nearly every computer, smartphone, tablet and other electronic device is flawed in at

---

29. *See* Paul Rosenzweig, *The Tell-Tale Heart*, LAWFARE (July 14, 2017), https://www.lawfareblog.com/tell-tale-heart.

30. *See* Meghnan Neal, *The Internet of Bodies Is Coming, and You Could Get Hacked*, MOTHERBOARD (Mar. 13, 2014), https://motherboard.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked.

31. For more on this topic, see Scott J. Shackelford et al., *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995 (2016).

32. Interview with Zach Rothstein, *supra* note 8.

least two significant ways.[33] The newly discovered flaws, nicknamed "Meltdown" and "Spectre," are chip-based weaknesses that let one user of a computer spy on other users—even if they are using shared computer systems providing Internet services to large numbers of people, like iCloud, Amazon Web Services, Google Cloud Platform or Microsoft Azure.[34] Chip companies and computer firms are working to fix the vulnerabilities, but the repairs can reportedly slow down computers and mobile devices by as much as thirty percent.[35] Corporate and academic researchers are still investigating how the problems were created, and how they persisted, unfound and unfixed, through more than twenty years of chip innovation.[36] Regardless of their cause, the pertinent fact is that too few firms are adequately securing their supply chains.[37]

It is widely known that hackers can gain access to computer systems by exploiting software vulnerabilities or though "social engineering," such as phishing schemes and other ruses.[38] But another avenue of attack is by altering circuits that, like lines of

---

33. *See Meltdown and Spectre*, https://spectreattack.com/ (last visited Apr. 13, 2018); Michael Simon, *Meltdown and Spectre CPU Flaws Affect All iOS and Mac Devices, but Don't Panic*, MAC WORLD (Jan. 5, 2018), https://www.macworld.com/article/3245778/apple-phone/apple-meltdown-spectre-cpu-flaws-statement.html; *What Are Spectre and Meltdown CPU Vulnerabilities and Are You Affected?*, WINDOWS CLUB, http://www.thewindowsclub.com/what-is-spectre-and-meltdown-vulnerabilities (last visited Jan. 17, 2018).

34. *See* Joshua Long, *Meltdown and Spectre: What Apple Users Need to Know*, MAC SEC. BLOG (Jan. 8, 2018), https://www.intego.com/mac-security-blog/meltdown-and-spectre-what-apple-users-need-to-know/.

35. *See* Patrick Howell O'Neill, *Industry Braces for Critical Intel Security Flaw Impacting a Decade's Worth of Chips*, CYBER SCOOP (Jan. 3, 2018), https://www.cyberscoop.com/intel-chip-flaw-virtual-memory-microsoft-windows-linux/.

36. *See* Andy Greenberg, *Triple Meltdown: How So Many Researchers Found a 20-Year-Old Chip Flaw at the Same Time*, WIRED (Jan. 7, 2018), https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/.

37. *See* Dave Lewis, *Digital Supply Chain (In)Security*, FORBES (July 28, 2014, 6:32 AM), https://www.forbes.com/sites/davelewis/2014/07/28/digital-supply-chain-insecurity/#628e15933869.

38. *See, e.g.*, Arun Vishwanath, *'Spearphishing' Roiled the Presidential Campaign – Here's How to Protect Yourself*, CONVERSATION (Nov. 8, 2016), https://theconversation.com/spearphishing-roiled-the-presidential-campaign-heres-how-to-protect-yourself-68274.

code, most users will never see.[39] These physical devices that are the foundation of the complex supply chains involved in most high-tech manufacturing are very hard to secure, as was introduced in Part I.[40] Each link in a supply chain highlights opportunities for hackers to exploit, which could damage equipment or even disable factories.[41] But not all supply chain threats are malicious; sophisticated retailers like Amazon, for example, have been fooled by counterfeits.[42] In 2015, Lenovo installed advertising software on its computers, dangerously weakening system security.[43] But the focus here is on malicious supply chain vulnerabilities, as was highlighted in 2012 when Microsoft warned customers that Chinese computer factories were installing malware on PCs before they even left the production line.[44]

As the Internet of Everything expands, the growing scale of the threat from hackers could easily be eclipsed by excitement over lower costs and smarter tech.[45] A classic example of this

---

39. *See* Andy Greenberg, *This 'Demonically Clever' Backdoor Hides in a Tiny Slice of a Computer Chip*, WIRED (June 1, 2016), https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/.

40. *See* Barker, *supra* note 18.

41. *See* Martin Giles, *Hackers Could Blow Up Factories Using Smartphone Apps*, MIT TECH. REV. (Jan. 11, 2018), https://www.technologyreview.com/s/609946/hackers-could-blow-up-factories-using-smartphone-apps/.

42. *See* Ari Levy, *Amazon's Chinese Counterfeit Problem Is Getting Worse*, CNBC (July 8, 2016), https://www.cnbc.com/2016/07/08/amazons-chinese-counterfeit-problem-is-getting-worse.html.

43. *See* Joshua A.T. Fairfield, *The 'Internet of Things' Is Sending Us Back to the Middle Ages*, CONVERSATION (Sept. 5, 2017), https://theconversation.com/the-internet-of-things-is-sending-us-back-to-the-middle-ages-81435; Elizabeth Weise, *FTC Settles with Lenovo over a Built-in Snooping Software, $3.5 Million Fine*, USA TODAY (Sept. 5, 2017), https://www.usatoday.com/story/tech/2017/09/05/ftc-settles-lenovo-over-built-snooping-software-scanned-users-computers/632775001/.

44. *See Malware Being Installed on Computers in Supply Chain, Warns Microsoft*, GUARDIAN (Sept. 14, 2012), https://www.theguardian.com/technology/2012/sep/14/malware-installed-computers-factories-microsoft.

45. *See* Carl Franzen, *How to Find a Hack-Proof Baby Monitor*, OFFSPRING (Aug. 4, 2017), https://offspring.lifehacker.com/how-to-find-a-hack-proof-baby-monitor-1797534985; John Markoff, *Why Light Bulbs May Be the Next Hacker Target*, N.Y. TIMES (Nov. 3, 2016), https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=0; Charlie Osborne, *Smartwatch Security Fails to Impress: Top Devices Vulnerable to Cyberattack*, ZDNET (July 22, 2015), http://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/; Aaron Tilley, *How Hackers Could Use a Nest Thermostat as an Entry Point into Your Home*,

trend happened in 2009 when the U.S. Department of Defense bought 2,200 Sony PlayStation 3 gaming consoles to use as components in a military supercomputer under the commercial off-the-shelf program.[46] But many of those systems were manufactured abroad, making it difficult to verify that they were not tampered with prior to their integration into critical U.S. infrastructure.[47]

The Navy, at least, has learned from this mistake. The Naval Surface Warfare Center Crane Division, which is the third largest naval base in the world spread across more than 100 square miles of Southern Indiana, has pioneered automated inspections, using artificial intelligence to examine digital pictures of new circuit boards to detect unauthorized alterations.[48] The U.S. is rightly concerned about falling victim to this sort of attack—in part, because U.S. government agencies conduct them. Leaked documents have shown how the National Security Agency's Tailored Access Operations team routinely intercepts shipments of new computer and networking equipment.[49] Then, NSA workers modify the hardware to add vulnerabilities and secret access for NSA hackers to use later, and then put the equipment back in boxes to be delivered.[50]

As explained in the Introduction and Part I, one new way to secure supply chains involves blockchain technology—a secure database system stored and maintained across many computers

---

FORBES (Mar. 6, 2015), https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#235d0d693986.

46. *See* Rosa Golijan, *Department of Defense Buys 2,200 PS3s to Upgrade Supercomputer*, GIZMODO (Nov. 29, 2009), https://gizmodo.com/5414938/department-of-defense-buys-2200-ps3s-to-upgrade-supercomputer.

47. *See* Scott J. Shackelford, *How to Enhance Cybersecurity and Create American Jobs*, HUFFINGTON POST (July 16, 2012), https://www.huffingtonpost.com/scott-j-shackelford/how-to-enhance-cybersecurity_b_1673860.html.

48. Press Release, Joe Donnelly, U.S. Senator for Ind., Donnelly Meets with NSWC Crane Expert, Praises Crane as a Leader in Protecting Country's Critical Weapons and Cyber Systems Against Counterfeit Parts (Oct. 27, 2015), https://www.donnelly.senate.gov/newsroom/press/donnelly-meets-with-nswc-crane-expert-praises-crane-as-a-leader-in-protecting-countrys-critical-weapons-and-cyber-systems-against-counterfeit-parts. DARPA has pioneered a similar program utilizing blockchain tech. *See* Press Release, DARPA, DARPA Technology Identifies Counterfeit Microelectronics (Sept. 30, 2014), https://www.darpa.mil/news-events/2014-09-30.

49. *Documents Reveal Top NSA Hacking Unit*, SPIEGEL ONLINE (Dec. 29, 2013), http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

50. *See id.*

around the internet—to track and verify all aspects of a complicated supply chain like Apple's. IBM and the international shipping giant Maersk are experimenting with using blockchain systems to better secure and transparently track shipments, as well as automate payments.[51] This is one of the benefits of blockchain tech since the distributed smart contracts that these systems generate are automatically enforceable. Once a component part like a chip is delivered, for example, a blockchain verifies that fact and the supplier automatically is paid in dollars, or their cryptocurrency of choice.

For those who might recall it, the peer-to-peer file sharing service Napster can be a useful onramp for understanding blockchain;[52] indeed, the service spawned an array of popular services, from Skype to Spotify, as well as Bitcoin.[53] What these diverse companies have in common is that none of their information is centrally archived; instead, they utilize, to a greater or lesser extent, "global spreadsheet[s]" that leverages peer-to-peer technology to authenticate transactions.[54] Such a system enables transparency, and thus trust, in distributed systems that otherwise lack that invaluable feature.[55] For example, every 10 minutes, on average,[56] all new Bitcoin transactions are "verified, cleared, and stored in a block" that is, in turn "linked to the preceding block, thereby creating a

---

51. Press Release, IBM, Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain (Mar. 5, 2017), https://www-03.ibm.com/press/us/en/pressrelease/51712.wss.

52. Lance Koonce, *Are Blockchains the Second Coming of Napster? (Perspective)*, BLOOMBERG L.: BIG L. BUS. (Jan. 18, 2017), https://biglawbusiness.com/are-blockchains-the-second-coming-of-napster-perspective/; Don Tapscott & Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World*, TIME (May 6, 2016), http://time.com/4320254/blockchain-tech-behind-Bitcoin/.

53. Koonce, *supra* note 52. Spotify formerly used on peer-to-peer streaming for certain users, but has since eliminated that function, and relies wholly on server-based streaming. Romain Dillet, *Spotify Removes Peer-to-Peer Technology from Its Desktop Client*, TECHCRUNCH (Apr. 17, 2014), https://techcrunch.com/2014/04/17/spotify-removes-peer-to-peer-technology-from-its-desktop-client/.

54. *See* Nolan Bauerle, *How Does Blockchain Technology Work?*, COINDESK (last visited Apr. 1, 2018), https://www.coindesk.com/information/how-does-blockchain-technology-work/.

55. *Id.*

56. *See* Joseph Bonneau, *How Long Does It Take for a Bitcoin Transaction to Be Confirmed?*, COIN CENTER (Nov. 3, 2015), https://coincenter.org/entry/how-long-does-it-take-for-a-bitcoin-transaction-to-be-confirmed.

chain."[57] Blocks that are not appropriately integrated are deemed invalid.[58] In time, such blockchains can become a "World Wide Ledger of value."[59]

But no blockchain, nor any system on which a blockchain may be deployed, is one-hundred-percent secure; they are, for example, still susceptible to hardware vulnerabilities like Meltdown and Spectre.[60] Moreover, in many ways blockchain is even harder to apply in the medical device context than, say, prescription drugs, given the complexity involved in these supply chains, as has been noted, as well as potential nation-state motivations to compromise these devices,[61] and the need for continuous updating as was described in Part I.[62] There are also challenges with relying on this technology to help anonymize patient data.[63]

At best, then, blockchain systems can be part of companies' efforts to manage supply chain risks by making it much harder to tamper with products and easier to trade inputs such as by using RFID tags, as well as automating payment, warehousing, transport and delivery.[64] As an example of the kind of fraud that

---

57. Don Tapscott, *Blockchain: The Ledger that Will Record Everything of Value to Humankind*, WORLD. ECON. FORUM (July 5, 2017), https://www.weforum.org/agenda/2017/07/blockchain-the-ledger-that-will-record-everything-of-value/.

58. *See* Bauerle, *supra* note 54.

59. *See* Don Tapscott & Alex Tapscott, *Here's Why Blockchains Will Change the World*, FORTUNE (May 8, 2016), http://fortune.com/2016/05/08/why-blockchains-will-change-the-world/; *see also* Tapscott, *supra* note 57 (calling blockgain a "new digital ledger to record anything of value to humankind").

60. Edmund Lee, *Why Blockchains Can Be Really Bad. Or: How Techno-Futurists Can Ruin Things*, RECODE (June 19, 2016), https://www.recode.net/2016/6/19/11972818/dao-hacked-blockchain-ethereum.

61. *See, e.g.*, Patricia A.H. Williams & Andrew J. Woodward, *Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem*, 8 MED. DEVICES 305, 305 (2015).

62. Sitting atop these complications is the fact that, in many instances, incentives are not aligned for manufacturers to be forthcoming with regards to potential security defects, with a potential cautionary tale taking the form of the Volkswagen emissions scandal. *See* Russell Hotten, *Volkswagen: The Scandal Explained*, BBC (Dec. 10, 2015), http://www.bbc.com/news/business-34324772.

63. *See* Mike Orcutt, *Who Will Build the Health-Care Blockchain?*, MIT TECH. REV. (Sept. 15, 2017), https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/.

64. *How Blockchain Can Transform the Supply Chain*, LOGISTICS BUREAU (Nov. 15, 2017), http://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/.

could be avoided by using blockchain, consider so-called "fictitious pickups."[65] These happen when con artists show up at a shipper's dock, show faked identification documents, and take a shipment. A blockchain would make it much harder for such a scheme to succeed since it would require consent by all of the users on the network.[66] For example, in order for a delivery to Indianapolis to be cleared, each participant in the chain would have to affirmatively sign off on it by adding a new block to the chain. But this is just the tip of the iceberg of what's possible. As reported by Steve Banker in *Forbes*, a firm called Kouvala envisions a scheme whereby pallets fitted out with RFID tags would ship themselves from A to B by advertising their needs. Shipping firms would then bid for the right to ship the load, and the pallet would, in effect, pick the best deal, which would be tracked in a blockchain.[67]

To realize this dream, though, it is necessary to train people to use blockchains and agree on standards for data communication, encryption, and storage.[68] And while such a system would still face the problem of insider threats, the underlying blockchain technology would make such attempts more difficult.[69] What is needed is an all-out effort to leverage the work that leading organizations like Walmart,[70] and the Department of Defense, in particular the DARPA SHIELD program, have accomplished, such as building out smart contracts using blockchain to help crystallize industry best practices.[71] Public-private partnerships could start the process

---

65. Steve Banker, *Blockchain in the Supply Chain: Too Much Hype*, FORBES (Sept. 1, 2017), https://www.forbes.com/sites/stevebanker/2017/09/01/blockchain-in-the-supply-chain-too-much-hype/#7cfdf1c1198c.

66. *Id.*

67. *Id.*

68. An effort is now underway to take these steps by the Blockchain Governance Initiative, which is housed at the Indiana University Ostrom Workshop. *See New Ostrom Workshop Blockchain Governance Initiative*, OSTROM WORKSHOP, https://ostromworkshop.indiana.edu/resources/news/180412-new-blockchain.html (last visited Apr. 23, 2018).

69. Charlie Osborne, *How Blockchain Technology Can Transform the Security Industry*, ZDNET (Sept. 4, 2017), http://www.zdnet.com/article/how-blockchain-technology-can-transform-the-security-industry/.

70. Robert Hackett, *Walmart and 9 Food Giants Team Up on IBM Blockchain Plans*, FORTUNE (Aug. 22, 2017), http://fortune.com/2017/08/22/walmart-blockchain-ibm-food-nestle-unilever-tyson-dole/.

71. *See* Kerry Bernstein, *Supply Chain Hardware Integrity for Electronics Defense (SHIELD)*, DARPA, https://www.darpa.mil/program/supply-chain-

of laying out appropriate standards to boost supply chain security and help pave the way for blockchain to help us create much more secure products, along with figuring out better ways to measure, model, and insure against cyber-attacks targeting hardware, such as pacemakers—the focus of the next Section.

IV. MEDICAL DEVICE CASE STUDY

This Part provides an in-depth view of how the current legal and regulatory framework affects the security of implantable pacemakers. We selected the pacemaker as the subject of this case study, in part, because security vulnerabilities in such devices have recently drawn widespread attention.[72] Concerns about pacemaker software vulnerabilities date to at least 2007, when then-Vice President Dick Cheney deactivated some of the wireless capabilities of his pacemaker out of concern for his safety.[73] Since then, cybersecurity vulnerabilities in pacemakers have been widely documented. In early 2017, St. Jude, a leading medical device manufacturer, patched a security vulnerability in one of its pacemaker systems that reportedly could have allowed attackers to drain the device's battery, harmfully alter a wearer's heart pacing, or deliver electrical shocks.[74] More recently, an "exhaustive security evaluation of an implantable cardiac device ecosystem" published by two researchers in 2017

---

hardware-integrity-for-electronics-defense (last visited Jan. 17, 2018); *Strengthening DOD Supply Chain Management*, INNOVATEGOV (last visited Jan. 17, 2018), http://innovategov.org/2015/03/19/strengthening-dod-supply-chain-management/.

72. *See, e.g.*, Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139 (2014); John G. Browning & Shawn Tuma, *If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices*, 67 S.C. L. REV. 637, 638 (2016); Eduard Marin et al., *On the (In)Security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them*, PROC. 32ND ANNUAL CONF. ON COMPUTER SECURITY APPLICATIONS 226 (2016), https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf.

73. *See, e.g.*, *U.S. Government Probes Medical Devices for Possible Cyberflaws*, 21 WESTLAW J. MED. DEVICES 4 (2014).

74. *See, e.g.*, Tom Spring, *St. Jude Patches Additional Cardiac Device*, THREAT POST (Feb. 7, 2017, 1:15PM), https://threatpost.com/st-jude-patches-additional-cardiac-device/123596/; *see also* Newman, *supra* note 26; Firmware Update, *supra* note 5.

uncovered thousands of vulnerabilities and revealed unencrypted patient data.[75]

This case study seeks to examine how well the current legal framework reduces the risk of cybersecurity threats in pacemakers, before moving on to discuss whether, and to what extent, industry practices are helping to fill any governance gaps.[76] For that reason, the initial discussion focuses squarely on the FDA's efforts to (i) prevent the commercialization of insecure devices, and (ii) prevent widespread harm to the public if problems are uncovered in devices that are already on the market. There are, of course, many other sources of law and regulatory power that could be implicated *after* a cybersecurity event has caused harm. For instance, personal identifying information of pacemaker users could be exposed in a large-scale security attack. Such an event could, in theory, lead to civil liability for device manufacturers and possibly even hospitals and doctors under laws governing disclosure of patient data.[77] These topics are beyond the scope of this case study because their primary function is backward-looking—that is, they address harms that have already occurred, and do not prospectively establish acceptable levels of risk to the public. The following discussion opens with a brief explanation of what pacemaker systems are, how they work, and the supply chains that make these devices possible. With this technological and industrial picture in place, the focus shifts to FDA regulation and guidance before moving on to the HIPAA Security Rule and relevant Federal Trade Commission (FTC) action.

---

75. *See* Dan Goodin, *Radio-Controlled Pacemakers Aren't as Hard to Hack as You (May) Think*, ARSTECHNICA (May 26, 2017), https://arstechnica.com /information-technology/2017/05/radio-controlled-pacemakers-arent-as-hard-to-hack-as-you-may-think/.

76. For more on the overall security threat landscape facing medical devices, see generally Michael Woods, *Cardiac Defribillators Need to Have a Bulletproof Vest: The National Security Risk Posed by the Lack of Cybersecurity in Implantable Medical Devices*, 41 NOVA L. REV. 419, 419–27 (2017), which discusses the cybersecurity risk for implantable medical devices.

77. *See, e.g.*, The Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 C.F.R. § 164.514(e) (2013) (precluding healthcare providers from disclosing data such as names, zip codes, treatment dates, etc.).

A. OVERVIEW OF MODERN PACEMAKER SYSTEMS

Pacemakers are widely used, remarkably reliable, and yet so inconspicuous that they can easily be underappreciated.[78] For all their technological complexity, pacemakers rely upon a simple principle: through a pair of conductive wires attached to a user's heart tissue, the device can sense abnormal heart rhythms.[79] In response, the device supplies a gentle and carefully-timed electrical current to return the heart's rhythm back to normal. Simply put, a pacemaker is a computer-controlled metronome for the heart.[80]

Each year, millions of patients' lives are saved by pacemakers or implantable cardioverter defibrillators (ICD). According to 24/7 Wall Street, 235,567 peacemakers and 133,262 ICDs were implanted in the United States in 2009, and the average cost of each procedure was $20,000 and $40,000, respectively.[81] The risks are low: infection occurs in one to two percent of pacemaker surgeries and malfunctions involving the conductive leads occur at a rate of about four percent.[82] Concerns over the security and privacy vulnerabilities in these devices loom large, however.[83]

The technology that makes this elegant invention a reality is complex, but the most important components and their

---

78. *See, e.g.*, Amy Norton, *More Americans Getting Pacemakers*, REUTERS (Sept. 12, 2012), https://www.reuters.com/article/us-more-americans-getting-pacemakers/more-americans-getting-pacemakers-idUSBRE88P1LN20120926 (reporting millions of pacemakers installed as of 2009). Leading manufacturers of pacemakers include: Medtronic, St. Jude Medical (acquired by Abbott in 2017), Boston Scientific, Abbott Labs, Edwards Lifesciences, and Johnson & Johnson.

79. *Implantable Medical Devices*, AM. HEART ASS'N, (Sept. 16, 2016), http://www.heart.org/HEARTORG/Conditions/HeartAttack/TreatmentofaHeartAttack/Implantable-Medical-Devices_UCM_303940_Article.jsp.

80. VINOD KUMAR KHANNA, IMPLANTABLE MEDICAL ELECTRONICS: PROSTHETICS, DRUG DELIVERY, AND HEALTH MONITORING 267–70 (2016) (discussing cardiac pacemakers) ("The main function of a typical pacemaker is to detect and investigate the heartbeat of a person to find out if it is normal or irregular.").

81. Baxter Allen, *The Eleven Most Implanted Medical Devices in America*, 24/7 WALL ST. (July 18, 2011), https://247wallst.com/healthcare-economy/2011/07/18/the-eleven-most-implanted-medical-devices-in-america.

82. *Id.*

83. William H. Maisel & Tadayoshi Kohno, *Improving the Security and Privacy of Implantable Medical Devices*, 362 NEW ENG. J. MED. 1164, 1164 (2010).

functions are easily understood.[84] Pacemaker systems (sometimes referred to as "ecosystems"[85]) are constellations of devices, software, and services.[86] At the center of a pacemaker system is the implantable cardiac device.[87] No larger than a wristwatch, such machines contain small computer control units, as well as software or firmware that detects abnormal heart rhythms and generates the electrical pulses necessary to restore normal rhythm.[88] The implantable cardiac device also contains an antenna for sending diagnostic data to the outside world and for receiving commands.[89] These devices are typically powered by lithium/ion batteries and surgically installed beneath a wearer's skin.[90]

---

84. Pacemakers, first invented in 1950s, have been greatly improved in their designs including smaller devices, longer lasting batteries, and more sophisticated communication systems. The device has three main components: a pulse generator with battery, one or more wires connecting the heart and the pulse generator, and electrode on each wire. The pulse generator, supported by a sealed lithium battery with an average eight years of life, produces electrical impulses from a complex circuitry. And the wire carries the electrical impulses between the heart and the generator, so the pacemaker can monitor and pace the heart's rhythm. Once the pacemaker has been implanted, physicians would use a pacemaker programmer to test the device functionality and set patient therapy parameters. *See generally* BILLY RIOS & JONATHAN BUTTS, SECURITY EVALUATION OF THE IMPLANTABLE CARDIAC DEVICE ECOSYSTEM ARCHITECTURE AND IMPLEMENTATION INTERDEPENDENCIES 4–5 (2017), https://www.a51.nl/sites/default/files/pdf/Pacemaker%20Ecosystem%20Evaluation.pdf. A pacemaker programmer may vary from manufacturers to manufactures but is a critical tool to monitor and even reprogram the pacemaker. It communicates with the pacemaker via radio frequency (RF) technology. Similarly, patients can also choose to remotely transmit their data from their home monitoring device to clinical physicians and save their time to clinic visits. The remote monitoring relies on a patient support network that also allows vendors to register and upgrade the monitor device. *Id.* at 5.

85. Pacemakers and ICDs, together with physician programmers, home monitoring device, and patient support network comprise an interdependent implantable cardiac device ecosystem. *Id.* at 4.

86. *Id.*

87. *See, e.g.*, KHANNA, *supra* note 80.

88. *Id.*

89. *Id.* at 283 (discussing wireless sending and receiving of information via antenna).

90. *See, e.g.*, *How Pacemakers Work*, BOS. SCI., http://www.bostonscientific.com/en-US/patients/about-your-device/pacemakers/how-pacemakers-work.html (last visited April 1, 2018).

A second important component is called a "programmer."[91] In simple terms, a programmer is a computer that doctors use in a clinical setting (e.g., a physician's office) to wirelessly communicate with an implanted cardiac device.[92] Although programmers are typically used to examine the functioning of a patient's heart, they also can be used to perform firmware upgrades—i.e., to send new firmware and installation commands to the computer control unit in an implanted cardiac device.[93]

Patients and doctors can also monitor pacemaker data outside of clinical settings with devices called "base stations."[94] Usually situated in a patient's home, a base station retrieves pacemaker data wirelessly from an implanted cardiac device, and transmits it (e.g., over the internet using Wi-Fi or cellular data connections) to a physician's office.[95] Often, the transmission of this data is mediated by a dedicated patient support network—an online service that routes pacemaker data (including alerts indicating abnormal heart rhythm) to patients and doctors.[96]

Since the first pacemakers were commercialized in the 1950s, the foregoing components have become smaller, more complex, and consequently, more vulnerable to security attacks. The recent introduction of smartphone apps to pacemaker systems has increased such risks. These apps allow a standard smartphone to function as a mobile base station that can retrieve data directly from a pacemaker and send it to a doctor over the internet.[97]

---

91. *See* KHANNA, *supra* note 80, at 284 (discussing programmers); *see also* Marin et al., *supra* note 72, at 226–36 (discussing vulnerabilities in programmers).

92. KHANNA, *supra* note 80, at 284; *see also* Preliminary Expert Report of Carl D. Livitt at 3, 18, 25, St. Jude Medical, Inc. v. Muddy Waters Consulting, Case No. 0:16-cv-03002 (DWF/JSM) (D. Minn. Oct. 23, 2016) (discussing exclusive use of programmer devices by physicians).

93. KHANNA, *supra* note 80, at 284.

94. *See, e.g.*, Marin et al., *supra* note 72, at 226–36 (" . . . base stations, installed in the patients' home, allow remote monitoring by gathering telemetry data from the ICD and sending this data to the hospital.").

95. *Id.*

96. *Id.*

97. *See., e.g.*, MEDTRONIC, *MyCarelink Smart U.S.*, http://www.medtronic.com/us-en/mobileapps/patient-caregiver/mycarelink-smart-us.html (last visited Apr. 1, 2018).

Pacemaker manufacturers rely on networks of suppliers for many of the electronic components and software packages that go into the devices they sell.[98] The widely-publicized 2017 pacemaker security report mentioned earlier reveals, for instance, off-the-shelf microprocessors used in home monitoring base stations, software libraries supplied by third parties, and removable third-party hard drives used in physician programmers.[99] Drawing on these examples and other publicly available information, Figure 1 below depicts a hypothetical pacemaker supply chain.

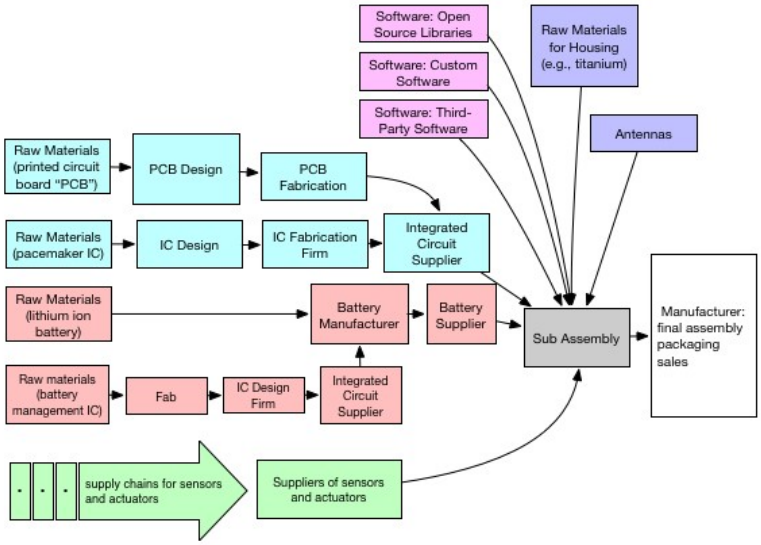

Figure 1: Hypothetical Pacemaker Supply Chain

Each rectangle in Figure 1 represents a unique company or institution that supplies a component or material that eventually is assembled and later packaged and sold by a manufacturer. As is evident, although perhaps not as complex and global as the supply chain for Apple's iPhone referenced in Part II, this manufacturing process still leaves plenty of space

98. Billy Rios & Jonathan Butts, *Understanding Pacemaker Systems Cybersecurity*, WHITESCOPE IO (May 23, 2017), http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html.

99. RIOS & BUTTS, *supra* note 84.

for security vulnerabilities and, as a result, has becoming increasingly regulated.

B. PACEMAKER SECURITY VULNERABILITIES

The device-to-device communications within a pacemaker ecosystem and the inherent vulnerabilities underlying the subsystems create security and privacy risks.[100] Ideally, manufacturers and vendors would implement robust safeguards to balance safety, reliability, complexity, power consumption, and cost. In reality, however, manufacturers have few incentives to improve security mechanisms that might slow down regulatory approval (discussed in the next sub-part).[101] In 2017, a report from WhiteScope highlighted industry-wide security weaknesses with pacemaker programmers: the researchers discovered over 8,000 vulnerabilities in outdated third-party libraries from four programmers built by four different vendors.[102] Among a long list of flaws, researchers found that pacemaker programmers do not authenticate to pacemaker devices and can reprogram any pacemaker from the same manufacturer; additionally, unencrypted patient data is stored on the programmers.[103] Focusing on radio-based (i.e., wireless) attacks, in 2008 another group of researchers showed that an unauthorized party equipped with a software radio within range of an implanted cardiac device could launch a denial-of-service attack, depleting the device's battery and exposing unencrypted patient information from RF signals.[104]

Although there have been some notable recalls of implantable cardiac devices in recent years, the massive 2017 recall of Abbott Laboratories' (formerly St. Jude Medical) 465,000 implanted pacemakers in the U.S. market is a stark example of the potential harm that a cyberattack on medical

---

100. *Id.* at 21–22.

101. Wayne Burleson et al., *Design Challenges for Secure Implantable Medical Devices* 1 (June 3–7, 2012), https://spqr.eecs.umich.edu/papers/49SS2-3_burleson.pdf (conference paper) (archived with the Security and Privacy Research Group at the University of Michigan).

102. RIOS & BUTTS, *supra* note 84, at 13.

103. *Id.* at 20.

104. Daniel Halperin et al., *Pacemaker and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, 2008 IEEE SYMP. ON SECURITY & PRIVACY 129, 136–38.

devices could do.[105] On August 29, 2017, The Food and Drug Administration (FDA) released a safety communication regarding the identified cybersecurity vulnerabilities in St. Jude Medical's pacemakers.[106] In the notice, the FDA recognized that as programmable medical devices become increasingly networked, there is an increased risk of exploitation of cybersecurity vulnerabilities.[107] A related report published by ICS-CERT, a special cybersecurity group within the Department of Homeland Security, indicated three vulnerabilities related to radio communications in the affected devices: (1) the pacemaker's authentication algorithm can be compromised or bypassed; (2) the pacemakers do not restrict the number of correctly formatted "RF wake-up" commands that can be received; (3) some models of pacemakers transmit unencrypted patient information to programmers and home monitoring units.[108] To exploit these vulnerabilities, an unauthorized user would send radio signals to modify a pacemaker's programming commands, which would result in patient harm from rapid battery depletion to inappropriate pacing.[109]

Fortunately, remedial steps have helped lower the risk of harm to pacemaker users. The FDA approved St. Jude Medical's firmware update as a corrective action (recall) to ensure that it addressed these vulnerabilities and reduced the risk of exploitation.[110] The firmware update will implement "RF wake-up" protections and limit the commands that can be issued to

---

105. Michael Mezher, *Abbott Recalls 465,000 Pacemakers for Cybersecurity Patch*, REG. AFF. PROFS. SOC'Y (Aug. 30, 2017), https://www.raps.org/regulatory-focus™/news-articles/2017/8/abbott-recalls-465,000-pacemakers-for-cybersecurity-patch. In 2007, Medtronic, an industry leader, issued a global recall of 235,000 Sprint Fidelis defibrillation leads because of the potential for lead fractures and identified thirteen deaths possibly related to the product. Thousands of product liability lawsuits ensued from the recall. Barry Meier, *Medtronic Links Device for Heart to 13 Deaths*, N.Y. TIMES (Mar. 13, 2009), http://www.nytimes.com/2009/03/14/business/14device.html?module=ArrowsNav&contentCollection=Business%20Day&action=keypress&region=FixedLeft&pgtype=article.

106. *See* Firmware Update, *supra* note 5.

107. *Id.*

108. *Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities*, ICS-CERT (Aug. 29, 2017), https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01.

109. *Id.*

110. Mezher, *supra* note 105.

pacemakers via RF communications.[111] In addition, the updated pacemaker firmware will prevent unencrypted transmission of patient information.[112] But the firmware update has to be applied during an in-person patient visit with a healthcare provider via the Merlin PCS Programmer.[113] As with any firmware update, physicians are recommended to consider the possible risk of an update malfunction along with the potential risk of a cybersecurity attack.[114] However, a replacement of implanted pacemaker is not recommended.[115] The FDA suggests that the implementation of the firmware update should be determined based on the physician's professional judgment and patient management considerations.[116]

The cybersecurity vulnerabilities in the St. Jude Medical's pacemakers may only reveal the tip of the iceberg. Designers in the implantable cardiac medical devices often face trade-offs between heightened cybersecurity posture and patient care considerations, such as safety, utility, and cost of power consumption.[117] Manufactures, vendors, and the healthcare industry writ large have not done enough to make their ecosystem resilient to cyber risks.[118] And they generally are not willing to share with public the security measures they may employ in their proprietary systems.[119] The next section investigates the potential of new regulations to address these security and privacy concerns in implantable cardiac medical devices.

C. FDA REGULATION OF MEDICAL DEVICES

Established in 1906, the Food and Drug Administration (FDA) is the primary federal agency responsible for overseeing the safety of medical devices such as pacemakers.[120] When

---

111. ICS-CERT, *supra* note 108.
112. *Id.*
113. *Id.*
114. *Id.*
115. Mezher, *supra* note 105.
116. ICS-CERT, *supra* note 108.
117. *See generally* Burleson et al., *supra* note 101.
118. *See id.* at 1.
119. *See id.* at 4.
120. In addition to the FDA, many state agencies also regulate their distribution. *See generally* M. Elizabeth Bierman & Michele L. Buenafe, *State Regulation of Medical Device Distribution: Strategic Planning Needed to Address Varying Requirements*, FOOD & DRUG L. INST. UPDATE, May/June

Congress granted the agency this authority in the 1930s, however, the term "medical device" typically referred to relatively simple tools used by doctors and surgeons at the time.[121] Since then, advances in mechanical engineering, computerization, and software design have enabled the development of sophisticated devices that address many types of medical problems.[122] This advancement is reflected in the Federal Food, Drug, and Cosmetic Act's broad definition of a medical device:

> [A]n instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease . . . or intended to affect the structure or any function of the body . . . [123]

This definition limits the scope the FDA is permitted to take by focusing only on devices that help heal or otherwise affect a patient's body as opposed to the constellation of devices that support a health provider's practice.[124] Working within these limitations, the FDA provides guidance to device manufacturers and healthcare providers on medical device cybersecurity.[125] This "total lifecycle product approach" places the FDA in the role of supervisor—monitoring device manufacturers to see if they market products with robust security protections, and whether or not they continue to update the devices with post-market patches.[126] Importantly, however, some software functions are expressly excluded from this definition.[127] The FDA tries to reduce the risk that dangerous devices are sold, in part, by

---

2009, at 20, https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/fdli_medicaldevicedistribution_may-june2009.ashx.

121. *Cf.* Richard A. Merrill, *The Architecture of Government Regulation of Medical Products*, 82 VA. L. REV. 1753, 1803 (1996) ("Most medical equipment, such as leg braces and wheel chairs, posed little risk to patients.").

122. *See* Carol Rados, *Medical Device and Radiological Health Regulations Come of Age*, FDA, https://www.fda.gov/AboutFDA/WhatWeDo/History/ProductRegulation/ucm2017808.htm (last updated Feb. 1, 2018).

123. 21 U.S.C. § 321(h) (2016).

124. *See* 21st Century Cures Act, Pub. L. No. 114-255, § 3060, 130 Stat. 1033, 1130 (2016) (clarifying the definition and excluding some medical software).

125. Suzanne Schwartz, *FDA's Role in Medical Device Cybersecurity*, FDA BLOGS: FDA VOICE (Oct. 31, 2017), https://blogs.fda.gov/fdavoice/index.php/2017/10/fdas-role-in-medical-device-cybersecurity/.

126. *Id.*

127. 21 U.S.C. § 321(h); *see also* 21st Century Cures Act, Pub. L. No. 114-255, § 3060, 130 Stat. 1033, 1130 (2016).

requiring medical device manufacturers to demonstrate the safety of their products before selling them.[128] In connection with this function, the FDA often issues guidance and recommendations to manufacturers.[129] The FDA also has the authority to take remedial steps: if a device manufacturer discovers that its FDA-cleared product is unsafe, it must convey this information to the FDA, which then may take various regulatory actions including notifying the public or recalling the product.[130]

The backbone of the FDA's compliance framework for medical devices is a classification system comprised of three levels—Class I, Class II, and Class III—each of which signify the level of risk a device presents, and the corresponding level of oversight required.[131] According to guidance published by the FDA, Class I devices require only compliance with "general controls" that apply to all classes of medical devices.[132] Such controls include, for instance, good manufacturing practices or labeling requirements. The safety of Class II devices, by contrast, requires information not captured by the general controls that apply to Class I devices—for instance, evidence that the device meets specific performance standards or guidelines promulgated by the FDA.[133] Such information may be included within a premarket notification document (often called a "510(k)" document), demonstrating that the device to be marketed presents a low risk to consumers.[134] The safety of

---

128. Schwartz, *supra* note 125.

129. *Id.*

130. *Cf.* Merrill, *supra* note 121, at 1808. As Richard Merrill explained in a landmark paper on FDA oversight of medical devices, since the 1970s, the FDA has had the authority "to ban worthless or dangerous products administratively, and to require notification, replacement, and/or refund by makers of defective products." *Id.*

131. Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 ANNALS HEALTH L. 1, 20–21 (2017), http://www.annalsofhealthlaw.com/annalsofhealthlaw/vol__26_issue_1?pg=4#pg4.

132. FDA, THE 510(K) PROGRAM: EVALUATING SUBSTANTIAL EQUIVALENCE IN PREMARKET NOTIFICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 2 (2014), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM284443.pdf.

133. *Id.* at 2 n.2.

134. *Id.* at 2 n.1. Most Class II devices require the submission of a Premarket Notification. See *Overview of Device Regulation*, FDA (Mar. 27, 2018), https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/default.htm [hereinafter *Device Regulation*, FDA].

Class III devices, meanwhile, cannot be determined from general controls or from additional submissions relating to performance standards alone.[135] These devices must receive FDA approval before they can be commercialized.[136] The FDA classifies new medical devices—i.e., devices marketed after the Medical Devices Amendments of 1976 that are not substantially equivalent to a legally marketed device—as "Class III" by default.[137] As Charlotte A. Tschider has explained: "How the device is used and its connection to sustaining human life (in comparison to diagnostic or therapeutic uses) determines its final classification."[138]

In some respects, it easy to evaluate how a typical pacemaker system would be examined under this framework: The FDA has established and published classifications for approximately 1,700 generic medical devices, including pacemakers.[139] For instance, implantable pacemaker pulse generators, programmers used by doctors, and pacemaker repair or replacement materials are all classified under the regulations as "Class III" devices requiring FDA approval.[140] By contrast, devices used to test the proper functioning of a pacemaker are categorized under Class II, requiring only compliance with general controls and performance characteristics.[141] Likewise, electrical chargers used to wirelessly recharge the battery in a pacemaker are defined as Class I devices, requiring only compliance with general controls prior to commercial sale.[142]

---

135. *Id.* at 2.

136. FDA, *supra* note 132, at 2.

137. *Id.* at 3. *See also Device Classification Under Section 513(f)(2)(De Novo)*, FDA (May 7, 2018), https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpmn/denovo.cfm (describing "an alternate pathway to classify new devices into Class I or Class II that had automatically been placed in Class III after receiving a Not Substantially Equivalent (NSE) determination in response to a 510(k) submission").

138. Tschider, *supra* note 131, at 21.

139. *Classify Your Medical Device*, FDA (Mar. 27, 2018), https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/.

140. 21 C.F.R § 870.3610 (2017). Most Class III devices require the submission of a Premarket Notification. *See Device Regulation*, FDA, *supra* note 134.

141. 21 C.F.R. § 870.3630 (2017). Most Class II devices require the submimssion of a Premarket Notification. *See Device Regulation*, FDA, *supra* note 134.

142. 21 C.F.R. § 870.3670 (2017).

The FDA's oversight of software in a pacemaker system is more difficult to evaluate, however, and could be less rigorous than its evaluation of physical devices.[143] The FDA has long regulated certain kinds of software, and certain software functions are explicitly excluded from the FDA's definition of medical devices altogether. Against that backdrop, however, Congress recently passed legislation that indicates the FDA may, in its discretion, regulate software critical to patient health.[144] This suggests at the very least that algorithms (implemented in software or firmware) designed to detect abnormal heart rhythms or firmware controlling the generation of electrical pulses would likely be regulated "devices."

The evaluation of smartphone apps is less certain, however. In 2015, the agency published a document that set out to clarify "the subset of mobile apps to which the FDA intends to apply its authority."[145] The document explains that it plans to regulate "[m]obile apps that are an extension of one or more medical devices by connecting to such device(s) for purposes of controlling the device(s) or for use in active patient monitoring or analyzing medical device data."[146] This strongly suggests that an app used in connection with a pacemaker could be a regulated device. However, the FDA has indicated that it "may" decline to regulate "[m]obile apps that provide patients a portal into their own health information, such as access to information captured during a previous clinical visit or historical trending and comparison of vital signs (e.g., body temperature, heart rate, blood pressure, or respiratory rate)."[147] Ultimately, it seems that

---

143. Similar uncertainty looms over the FDA's oversight of other medical devices. In a 2002 article, Julia Scheeres reported on the FDA's finding that a small implantable microchip did not qualify as a "medical device" under the Act, and consequently, did not fall under the FDA's classification system. The device, Scheeres explained, had long been used to tag animals before more recent applications involving human users had been explored. Julia Scheeres, *ID Chip's Controversial Approval*, WIRED (Oct. 23, 2002, 12:00 PM), https://www.wired.com/2002/10/id-chips-controversial-approval/.

144. 21 U.S.C. § 321; *see also* 21st Century Cures Act, Pub. L. No. 114-255, § 3060, 130 Stat. 1033, 1130 (2016).

145. FDA, MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Feb. 9, 2015), https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm263366.pdf (last visited Feb 13, 2018) [hereinafter FDA, MOBILE GUIDANCE].

146. *Id.*

147. FDA, MOBILE GUIDANCE, *supra* note 145.

the FDA will not categorically regulate apps distributed for use with pacemakers; rather, whether a pacemaker app will be regulated, and the degree of regulation it might receive, will be determined in an ad hoc fashion, depending on the specific functions of the app.

Beyond the classification and regulation of devices, the FDA has treated cybersecurity concerns in pacemaker systems with a light touch. The agency has shown a preference for issuing general guidance rather than mandating security standards or subjecting devices to rigorous testing. In a 2005 advisory publication, for instance, the FDA laid out a largely hands-off approach to cybersecurity risks presented by off-the-shelf software, assuring manufacturers that there is typically no need to report software patches to the FDA prior to supplying such patches to consumers and doctors.[148] In 2014, the FDA published new cybersecurity guidance focused on how device manufacturers can best prepare their devices for commercialization.[149] Like the 2005 document, these guidelines were not legally enforceable, instead reflecting only the agency's "current thinking" on the topic.[150] The document encouraged device manufacturers to "consider" cybersecurity risks and reasonably preventative steps such as authentication systems to ensure that only authorized users and software can access devices. The FDA cautioned, however, against overly cumbersome security measures that "could unreasonably hinder access to a device intended to be used during an emergency situation."[151] In addition, the FDA encouraged device manufacturers to describe in premarket notifications any steps taken (e.g., design considerations and related analyses) to reduce cybersecurity risks.[152]

---

148. FDA, *Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* (Jan. 14, 2005), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf.

149. FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff* (Oct. 2, 2014), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

150. *Id.*

151. *Id.*

152. *Id.*

Acknowledging that cybersecurity risks cannot be eliminated entirely through premarket steps alone, the FDA published a set of post-market guidelines in 2016.[153] Like the 2014 document, these guidelines contained non-binding advice and suggestions. The guidelines advised manufacturers to "establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls."[154] A theme throughout the document was the need for manufacturers to make and follow clearly documented plans and procedures aimed at reducing patient risks: "Manufacturers should have a defined process to systematically conduct a risk evaluation and determine whether a cybersecurity vulnerability affecting a medical device presents an acceptable or unacceptable risk."[155]

Relevant to pacemaker manufacturers, the 2016 post-market guidelines offered advice on when new reporting to the FDA is necessary for software patches. The document explained that "*regularly scheduled* security updates or patches to a device, including upgrades to the software, firmware, programmable logic, hardware, or security of a device to increase device security, as well as updates or patches to address vulnerabilities associated with controlled risk" are considered by the FDA to be "enhancements" rather than "repairs" and, consequently, do not require notification.[156] By contrast, software patches that address urgent threats to patient safety—i.e., "where there is unacceptable residual risk of patient harm due to [the absence of additional] risk mitigations"—must be reported to the FDA.[157] In exchange for allowing manufacturers to manage postmarket security, the guidance states that the FDA strongly recommends manufacturer adoption of effective cybersecurity practices—notably, the NIST Framework for critical infrastructure.[158]

---

153. *See generally* FDA, *supra* note 21.

154. *Id.* at 15.

155. *Id.*

156. *Id.* at 9 (emphasis added). While uncontrolled risks require more disclosure requirements, the FDA explicitly states that they do not intend to enforce reporting requirements for remedied vulnerabilities that meet certain requirements, such as active participation by the manufacturer in an ISAO. *Id.* at 23.

157. *Id.* at 12.

158. *Id.* at 27–30.

In light of the recent revelations about pacemaker vulnerabilities, legal commentators have criticized the FDA for not taking a firmer stand on cybersecurity. One commentator recently summarized the FDA's posture in this regard as follows:

> Indeed, the FDA heavily relies on guidance to oversee software. Agency documents that summarize the FDA's approach generally cite to the same cluster of five guidances. Together, these documents form a cascade of quasi-regulation, recommendations, and "current thinking," but offer few firm rules. Software does not stand on terra firma with the FDA.[159]

This comment is representative of a vein of recent scholarly criticism directed at the FDA's reliance on guidance in place of notice and comment rulemaking.[160]

This brief look at pacemaker security suggests that at least some level of concern is well-founded: recent security reports have clearly documented security flaws in pacemakers that have been widely sold and installed by doctors. These flaws are highly technical, but an engineering degree is not needed to understand their sources: modern pacemaker systems rely upon complex supply chains, sophisticated software, along with Internet control and access. To help address them, the FDA entered into a Memorandum of Understanding with the National Health Information Sharing and Analysis Center and the Medical Device Innovation, Safety, and Security Consortium. By "enabl[ing] an operational framework for medical device vulnerability information-sharing," the partnership allows the FDA to continue to stay abreast of vulnerability fixes that are not subject to the premarket review process.[161] This approach is consistent with the information sharing approach adopted by other departments such as DHS's Critical Infrastructure

---

159. Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175, 194 (2014).

160. *See, e.g.*, Lars Noah, *Guidance Gone Wild? FDA's Regrettable Retreat From Legislative Rulemaking*, 30 LEGAL BACKGROUNDER (Oct. 9, 2015) ("Although the Administrative Procedure Act (APA) plainly allows for the practice, the agency may have gotten a little carried away with this mechanism, and, at times, it improperly treats these guidance documents as if they were regulations adopted after notice-and-comment rulemaking."); Browning & Tuma, *supra* note 72, at 671 ("In fact, a legitimate criticism could be levied that up until very recently, the FDA was more concerned about cybersecurity measures interfering with an IMD's utility. For example, in 2014 the FDA alerted manufacturers that cybersecurity measures should not 'unreasonably hinder' a device's function.").

161. *Cybersecurity*, FDA (Mar. 7, 2018), https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.

Protection[162] and the Treasury's FinCEN Exchange for financial crimes.[163]

These observations are all the more concerning when considered alongside the FDA's preference for an advisory role on cybersecurity matters and its somewhat vague indications concerning future oversight of software. In summary, cybersecurity risks to pacemakers are likely higher than consumers might wish, but the FDA appears disinterested at present in adopting a more assertive stance. But, it is not the only game in town.

D. HIPAA SECURITY RULE

Regulation of Internet of Things (IoT) devices in the healthcare arena comes from two primary sources, FDA regulation and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.[164] This section discusses why HIPAA's security rule may be a useful tool for regulators seeking to secure a covered entity's network. It is important to note that HIPAA's Security Rule may apply to regulation of the medical IoT supply chain in a roundabout way. The Security Rule requires appropriate measures be taken to safeguard any electronic protected health information (PHI).[165] IoT devices that do not meet the definition of medical devices do not generally store PHI, making the security rule seem inapplicable.[166] That is, unless one accounts for the attack vector that insecure IoT devices provide. For example, should a hospital install smart thermostats or lights, those IoT devices would understandably avoid any application of the medical device definition. However, because the thermostat is connected to the hospital's network, it provides an avenue for attackers to infiltrate the network and gain access to the PHI stored within.

---

162. *Information Sharing: A Vital Resource for Critical Infrastructure Security and Resilience*, U.S. DEP'T HOMELAND SECURITY (Jan. 9, 2018), https://www.dhs.gov/information-sharing-vital-resource.

163. *FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing*, FINCEN (Dec. 4, 2017), https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing.

164. 45 C.F.R. 160; 45 C.F.R. 164(A); 45 C.F.R. 164(C); *The Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (May 12, 2017), https://www.hhs.gov/hipaa/for-professionals/security/index.html.

165. *Id.*

166. *See id.*

In this way, the Security Rule can fill in the gaps left by the narrower definition of medical devices.

While the Security Rule only applies to covered entities, such as healthcare providers, and does not apply to medical device manufacturers,[167] it may nonetheless help spur device manufacturers to design with security in mind. If a healthcare provider does not feel that a given IoT device is secure enough, and, for example, could open them up to liability for a breach of the security rule, they will likely decline to allow the device on their network. As health providers continue becoming more sophisticated and savvy about their overall network security,[168] medical device manufacturers and regulators should consider the impact of the Security Rule on IoT devices in the healthcare supply chain as part of a broader universe of reforms needed.

E. FEDERAL TRADE COMMISSION ENFORCEMENT

If a device manufacturer is not one of HIPAA's covered entities, and the IoT device does not meet the definition of a medical device,[169] a manufacturer may still be subject to the FTC Act. In fact, the FTC sees its role as co-partners with the Department of Health and Human Services (HHS), filling in the gaps where HIPAA is absent: "Indeed, the FTC Act is currently the primary federal statute applicable to the privacy and security practices of non-HIPAA covered businesses that collect individually identifiable health information."[170] As a result, it is highly relevant to any study of cybersecurity in the healthcare context.

The FTC has adopted a reasonableness standard for regulating the security practices for non-HIPAA covered entities.[171] In this way, unlike HIPAA's binary approach, industry norms have the potential to affect federal enforcement

---

167. *Covered Entities and Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

168. *See infra* Part IV(C).

169. That is, the device is not part of the diagnosis, cure, or treatment of a medical condition—such as an Apple Watch or other health monitor.

170. Thomas Pahl, Fed. Trade Comm'n, Cybersecurity & the Healthcare Industry: The FTC's Tools for Tackling New Threats, Opening Remarks Before the University of Maryland Medical Systems Board Cybersecurity Retreat 4 (Mar. 29, 2017), https://www.ftc.gov/system/files/documents/public_statements/1229863/pahl_-_umms_opening_remarks_3-29-17.pdf.

171. "In the data security world, all roads lead to reasonableness." *Id.* at 3.

practices. The FTC Act's prohibition against "unfair or deceptive trade practices"[172] results in enforcement against companies that break their promises to consumers through a failure to implement "reasonable" security practices or by going beyond the scope of consent.[173] Generally, these failures occur as the result of a data breach, but are just as likely to stem from security failures in IoT devices.[174]

The reasonableness standard means that following FTC recommendations can help device manufacturers avoid liability. In 2017, Acting Director Thomas Pahl's recommendations included: (1) "don't misrepresent the level of security you provide"; (2) "protect against well-known, foreseeable threats"; and (3) "take advantage of" guidance issued by federal agencies.[175] The FTC's earlier IoT report in 2015 provided specific security guidelines including "security by design," promoting a culture of security, secure third-party service providers, "defense in depth," and reasonable access control measures.[176] It is likely that as implementation of these practices and others become industry norms, failure to adopt them will place non-HIPAA covered entities in unreasonable territory—risking FTC scrutiny.

V. IMPLICATIONS FOR MANAGERS AND POLICYMAKERS

Despite the efforts of U.S. regulatory agencies, particularly the FDA, as has been made clear, there are security gaps remaining that, in some cases, are being filled by industry codes of conduct. This final Part examines the extent to which industry norm entrepreneurs can succeed where other stakeholders have thus far failed to secure vulnerable medical devices, particularly pacemakers. The Part begins with an overview of industry best

---

172. 15 U.S.C. § 45 (2006).

173. *See, e.g.*, *In re* PaymentsMD, LLC, 159 F.T.C. 241 (2015) (decision and order) (punishing collection of data beyond the scope of consumers' consent); *In re* Rite Aid Corp., 150 F.T.C. 694 (2010) (decision and order) (punishing Rite Aid's corporate policies which failed to secure PII).

174. Pahl, *supra* note 170, at 6.

175. *Id.* at 7–8.

176. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 28–31 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

practices before taking a deep dive focusing on the experiences of AdvaMed and Eskenazi Health and concluding with an analysis of global developments as they pertain to cybersecurity due diligence.

A. A LOOK AT MEDICAL INDUSTRY CYBERSECURITY BEST PRACTICES

When it comes to best practices, we must remind ourselves that they are just that—practices rather than rules. Yet as more and more medical devices are created to connect with one another, the increase in connectivity enlarges the risk to data and increases the value of cybersecurity weak points for those with malicious intent. That being said, the ever-changing landscape forces medical device companies, healthcare delivery organizations, and the industry in general to be conscious contributors in putting forth recommendations and enacting security-prone changes on the individual level[177] to constantly spur ideas on how to take positive prophylactic measures.

Today, the public's expectations for medical devices' capabilities far exceed those of earlier times.[178] Whereas early devices were standalone, today's are connected to a broad ecosystem, as discussed in Part III. Users can, and oftentimes desire to, connect to their healthcare providers, biomedical engineers, or other devices to provide a cumulative and comprehensive view of their health to others participating in delivering the highest levels of care.[179] But the cost of this exponential connectivity creates many points susceptible to cybersecurity threats in various stages, ranging from the chain of device creation and production, to connecting with healthcare providers and entities, to performing the device's intended function. The preceding section on adapting the NIST CSF and following FDA pre- and post-market guidance provide some of the strongest defense mechanisms in the campaign against cybersecurity threats, but this section aims to further detail best practices as seen in the industry of medical devices specifically.

Starting with the inception of a medical device, manufacturers can and should have the foresight to understand

---

177. *See infra* Part IV(C).

178. *See generally* HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, *supra* note 10.

179. *Id.*

the type of data and environment(s) in which their products intend to hold, create, transmit, or store information.[180] In our current climate, the best practice approach to gauging what information should be protected is to have the assumption "that assets requiring protection will always be under threat."[181] Many industry authorities, private and government, promulgate the concept that testing for risk and safety analyses throughout the lifecycle of manufacture is a critical way to detect and mitigate present and future threats and vulnerabilities.[182] The best way to plan for an inevitable cybersecurity threat is to embed defensive infrastructure during the design phase(s), rather than posing threats and recovery options as afterthoughts; in other words, the best firms build in cybersecurity from the start, they do not bolt it on as an afterthought.[183] Industry professionals have supported strategies to secure medical device software through strengthening the operating system and implementing security technologies like firewalls.[184] From a physical standpoint, manufacturers should minimize attack surface of devices requiring them to contain the minimal components needed for design as well as closing any ports that would otherwise remain open.[185] Every phase throughout a medical device's life, from creation to disposal, needs to be tested and accounted for in terms of risks.

The responsibility of designing and building secure devices can be executed through contractual agreements deferring responsibility to manufacturers rather than consumers, whether

---

180. Fubin Wu & Sherman Eagles, *Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality*, 50 BIOMED. INSTRUMENTATION & TECH. 23, 25–26 (2016), http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/BIT/2016_BIT_JF_Cybersecurity Manufacturers.pdf (explaining cybersecurity risk analysis).

181. *Id.*

182. *See generally* HEALTH CARE INDUS. CYBERSEC. TASK FORCE, *supra* note 10; Wu & Eagles, *supra* note 180.

183. HEALTH CARE INDUS. CYBERSEC. TASK FORCE, *supra* note 10, at 38; Kevin Fu & James Blum, *Controlling for Cybersecurity Risks of Medical Device Software*, HORIZONS, Spring 2014, at 38, http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/HT_Cybersecurity/2014_HorSpr_Software_Risks.pdf.

184. Ron Mehring & Axel Wirth, Medical Device Patch Management: Factors for Strategy and Execution, Speech at HIMSS Conference (Mar. 1, 2016), http://www.himssconference.org/sites/himssconference/files/pdf/20.pdf.

185. *Id.*

that be hospitals or other types of healthcare delivery organizations. Contracts that put the responsibility to design information security and privacy standards on manufacturers will place the onus on the medical device industry to take cybersecurity into consideration at all levels of product research and design, hopefully in greater emphasis than what attention is dedicated to cybersecurity now.[186] Through these responsibility agreements, every system level of a medical device can be penetration-tested during the design and manufacture, even verified with certification, to ensure the integrity, security, and privacy of the device before it is released on the market.[187] If weaknesses or flaws are revealed throughout the process, consumers can work with manufacturers, in order to stress and uphold the principles of protecting patient safety and the integrity of the technology.

Once on the market, manufacturers should not be let off the hook in terms of assessing for potential threats and vulnerabilities. Assuming a medical device is securely designed and even more so in the event the device was not assessed for risk during its design, manufacturers should be involved with their healthcare delivery organizations in the lifecycle management of their medical devices. Best practices for manufacturers should include constant monitoring of threats and vulnerabilities to their devices in production and on the market, and then reporting such detected threats and vulnerabilities to their consumers and affected public.[188] Patches need to be developed by manufacturers in response, then need to be sent to the appropriate channels that can deploy them among the threatened devices to mitigate any risks moving forward.[189]

As was discussed in Part II, patching is easier said than done, but it is critical to maintaining an up-to-date secure medical device. For best practices purposes, disseminating and implementing patches by both the manufacture and healthcare delivery organization in a timely fashion is of the utmost

---

186. Ron Ross et al., *Security Systems Engineering* (NIST Special Pub. No. 800-160, 2018), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf (summarizing cybersecurity best practices for building trustworthy systems).

187. HEALTH CARE INDUS. CYBERSEC. TASK FORCE, *supra* note 10, at 19.

188. Mehring & Wirth, *supra* note 184, at 20.

189. *Id.*

importance.[190] A delayed patch deployment may result in a situation such as Wannacry; the patch that would have prevented the Wannacry incident was released over a month prior to the attack yet was not deployed by hospital administrators.[191] Granted, deploying patches in hospital operating systems may be relatively easy in comparison to certain medical devices (i.e. ones implanted in the human body), the same concept applies in that patching sooner than later is in the interest of the patient's safety. Industry professionals recommend, and some healthcare delivery organizations have gone as far as, to implement a patch management program, "triaging" risks and determining the order of patch deployment according to network and data exposure, likelihood of a breach occurring, and the potential impact it could have on the entity.[192]

Patching is even more important when considering the actual lifespans of medical devices. There is a common misconception that, because new medical devices are always being developed, these new products are being quickly adopted. In reality, medical devices (along with Electronic Health Record systems) are being used, in some cases, anywhere from ten to twenty or more years due to budgetary restraints faced by hospitals.[193] Operating systems may be newer or updated more frequently, but the vendors that supply the devices or their respective patchwork may have been developed according to previous versions of operating systems;[194] such misalignment jeopardizes strategic plans to secure the full lifecycles of medical devices. Thus, maintaining a relationship with vendors and manufacturers to provide the latest software updates compatible with the healthcare delivery organization or the medical device itself is crucial in protecting the longevity of devices.[195] Further, as long as the software patch is designed to address security issues and does not change the function of the medical device, manufacturers will not be burdened by having to attain

---

190. *Id.*

191. Mike Kelly, *Cybersecurity Best Practices for Healthcare Companies*, J.P. MORGAN CHASE & CO. (June 1, 2017), https://commercial.jpmorganchase.com/pages/commercial-banking/industry-expertise/cybersecurity-healthcare-companies.

192. Mehring & Wirth, *supra* note 184, at 23.

193. HEALTH CARE INDUS. CYBERSEC. TASK FORCE, *supra* note 10, at 28.

194. *Id.*

195. *Patch Management Tips Every HDO Should Know*, AAMI (July 25, 2017), http://www.aami.org/newsviews/newsdetail.aspx?ItemNumber=4873.

recertification or approval by the FDA; as was discussed in Part III, manufacturers only need to test the patch to ensure it does not have negative outcomes on the device.[196]

Cybersecurity threats and vulnerabilities will occur no matter how much a product is designed to withstand an attack or whether it is updated like clockwork with respect to appropriate patches. Security incidents will happen, but, at the very least, manufacturers should have a vulnerability disclosure policy in the event that an attack threatens the public safety of its consumers.[197] In October 2016, on the heels of the St. Jude pacemaker issues coming to light, Johnson & Johnson (J&J) may have been the first in its industry to proactively come forth in issuing a warning to patients about the "cyber vulnerability" of their OneTouch Ping insulin pumps.[198] The medical devices at stake were insulin pumps that connect to the patient's body and inject insulin through catheters controlled by a wireless remote.[199] Due to the device's communication not being encrypted, testing confirmed that a hacker could manipulate the pump to dose insulin, thus posing potentially life-threatening consequences.[200] While J&J believed there were no attempted hacks on any of the 114,000 patients who used the OneTouch Ping, J&J decided to warn all those patients and provide advice on how to fix the problem.[201] Ultimately, the FDA lauded J&J about their forthcomingness, supporting the hopeful transition from companies and organizations generally hiding negative "cyber vulnerabilities" to the practice of executing disclosure procedures about confirmed threats.[202] It should be best practice to disclose warnings and follow-up recommendations to remedy medical device vulnerabilities "in a way that best protects patients."[203]

Again, despite the lengths taken to assess and mitigate cybersecurity risks in design and through constant patching, cyber attacks are inevitable, and much is still to be learned about

---

196. *Id.*
197. Mehring & Wirth, *supra* note 184, at 20.
198. Jim Finkle, *J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking*, 23 No. 17 WESTLAW J. MED. DEVICES 6 (2016).
199. *Id.*
200. *Id.*
201. *Id.*
202. *Id.*
203. *Id.*

how to best react to adverse events. Information sharing as an industry-wide best practice has the potential to assist all types of healthcare organizations: large and small, public or private. Institutions like the National Health Information Sharing and Analysis Center (NH-ISAC) enable any non-profit or for-profit healthcare stakeholder—including healthcare providers, insurers, biotech firms, laboratories, medical schools, medical device manufacturers, and more—to participate in a "forum for sharing cyber and physical threat indicators, best practices and mitigation strategies."[204] NH-ISAC's goals include securing personal health information and complying with standards and regulations in HIPAA to further protect patient safety and lives while our world continues progress in healthcare through medical devices and such technology.[205]

Regardless of whether one is a voluntary member of NH-ISAC, information sharing can be helpful for any organization or healthcare stakeholder. Creating a baseline of information on cybersecurity risk management that any size or type of healthcare organization can tailor to their needs is a start.[206] Many healthcare organizations are small-to-medium-sized businesses that lack the staff, resources, and infrastructure to combat a potential cybersecurity incident, but if an information sharing system were in place, these smaller entities could greatly benefit whether in receiving information about real-time threat indicators or using the strategies of cybersecurity experts at other healthcare organizations that have already faced similar scenarios.[207] To have strength in numbers and share these strategies, the FDA has recognized the need for transparent dialogue, and, thus, does not intend to enforce certain reporting requirements of the Federal Food, Drug, and Cosmetic Act for companies that voluntarily participate in specific institutions, including the NH-ISAC.[208]

Ultimately, though, even if best practices are implemented by norm entrepreneurs, there will still be a gap, resulting in a

---

204. *NH-ISAC and MDISS Partner to Form Medical Device Security Information Sharing Initiative*, NH-ISAC (June 14, 2016), https://nhisac.org/events/announcements/nh-isac-and-mdiss-partner-to-form-medical-device-security-information-sharing-initiative/.

205. *Id.*

206. HEALTH CARE INDUS. CYBERSEC. TASK FORCE, *supra* note 10, at 51.

207. *Id.* at 50–51.

208. NH-ISAC, *supra* note 204.

lack of mandatory requirements to hold medical device manufacturers or healthcare delivery organizations accountable for security lapses. Between the FDA covering safety and effectiveness, HHS's enforcement of HIPAA, and the Joint Commission's Standard for Medical Equipment Safety, medical devices only need to abide by floor standards to avoid statutory breaches rather than being required to invest in proactive cybersecurity best practices.[209] While medical device cybersecurity legislation has yet to be passed, in 2017, the HHS's Health Care Industry Cybersecurity Task Force encouraged healthcare providers to collaborate among departments; including leadership, biomedical engineering teams, IT staff, and IT security, when it comes to the selection, deployment, and maintenance of medical devices.[210] The Task Force promotes the creation of a Medical Computer Emergency Readiness Team (MedCERT) within healthcare organizations, with teams specifically concentrated on medical devices to focus on potential impacts to patient safety when vulnerabilities to medical devices are disclosed and/or exploited.[211] The establishment of MedCERT teams is designed in the interest of protecting national security, as they would be the "go-team[s]" in the event of a medical device exploit tasked with "assess[ing] vulnerabilities, evaluat[ing] any patient safety risks, serv[ing] as an adjudicator between the vulnerability finder and the product manufacturer, assess[ing] proposed mitigations, and serv[ing] in a consultation role for organizations navigating the coordinated vulnerability process."[212] Just as privacy concerns exploded in the 1990s, in response to which HIPAA designated mandatory privacy officers in all healthcare organizations,[213] MedCERT might be the teams created in response to the rising levels of cyber threats to medical devices.

Looking ahead, the multi-faceted cyber threat to medical devices will likely continue to increase as the IoT universe

---

209. For more on this topic, see Amanda N. Craig, Scott J. Shackelford, & Janine Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 18 AM. BUS. L.J. 721, 722 (2015).

210. HEALTH CARE INDUS. CYBERSEC. TASK FORCE, *supra* note 10, at 33.

211. *Id.* at 34.

212. *Id.*

213. Office for Civil Rights, *Summary of HIPAA Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

expands. Public and private entities have already joined forces to innovate on the subject, such as the Medical Device Innovation Safety & Security Consortium (MDISS). Established in 2010, MDISS is a nonprofit, public/private partnership, and the first of its kind to focus exclusively on medical device cybersecurity.[214] Under a 1.8 million dollar contract with the Department of Homeland Security's Cybersecurity Division, MDISS has built a medical device cyber risk assessment platform furthering the collaboration and sharing of critical information between stakeholders like healthcare organizations, medical device manufacturers, technology firms, and even the NH-ISAC.[215] Moreover, in 2017, MDISS built over a dozen World Health Information Security Testing Labs (WHISTL), in which the "facilities will comprise a federated network of medical device security testing labs . . . . Enabling MDISS members to test devices in both physical and virtual environments, WHISTL facilities will focus on identifying and mitigating medical device vulnerabilities, sharing solutions and best practices, and device security education and awareness."[216] Successes of the organization's initiative have been tangibly measured in participant hospitals, including efforts by Eskenazi Health and its respective Certified Biomedical Equipment Technician Manager/Clinical Engineer, Benjamin Esslinger, which is shared later in greater detail.[217] The mission and goals of organizations like MDISS exemplify and execute best practice standards in upholding the cybersecurity of medical devices—from testing and developing safety protocols, sharing information on how to mitigate and react to threats, and even recognizing and acting on the importance of cross-collaboration between public, private, and government efforts—these practices help promote a future state in which expected cyber-attacks can be mitigated. Already, through the work of MDISS—along with AdvaMed, highlighted next—real progress is being made.

---

214. *See MDISS*, MDISS, https://www.mdiss.org/ (last visited Feb. 22, 2018).

215. *MDISS Launches 'Whistl' Network of Security Testing Labs for Medical Devices*, MDISS (July 27, 2017), https://www.mdiss.org/news/mdiss-launches-whistl-network-of-security-testing-labs-for-medical-devices.

216. *Id.*

217. *Id.*

B. ADVAMED ILLUSTRATIVE EXAMPLE

This section focuses in particular on the efforts of AdvaMed within the wider context of organizations working on the topic of healthcare cybersecurity. To be clear, AdvaMed is far from alone in this ecosystem. The Medical Device Manufacturers Association (MDMA) and the Medical Imaging and Technology Alliance (MITA) are also important partners, but the latter focuses mostly, unsurprisingly, on imaging technologies. Yet this group has important power when it comes to medical device cybersecurity due to the fact that it is a standards body. In particular, the Manufacturer Disclosure Statement for Medical Device Cybersecurity is an important data point in helping to frame a standard of cybersecurity care for medical device firms.[218]

AdvaMed works with these groups on different policies and leads in particular on policy matters given its deep interaction on Capitol Hill and with the FDA. In particular, AdvaMed's Cybersecurity Foundational Principles have been influential, both in the U.S. and abroad. These Principles were developed in the aftermath of the Muddy Waters Report involving St. Jude pacemakers discussed above.[219] There was some haste in developing these principles, according to Rothstein, meaning that some important issues like supply chain cybersecurity did not necessarily get the attention they deserved; in fact, "supply chain" is not even mentioned in the Principles. But these foundational principles, which are in turn based on the NIST CSF, will, in time, be expanded. "I would anticipate supply chain being within the next two issues that we tackle as an industry," said Rothstein.[220]

Best practices like the AdvaMed Principles can be spread more quickly by the advent of new information-sharing organizations, like the new Healthcare Coordinating Council under NH-ISAC.[221] The Council is intended, according to

---

218. *Manufacturer Disclosure Statement for Medical Device Security (MDS2)*, HEALTHCARE INFO. & MGMT. SYS. SOC'Y, http://www.himss.org/resourcelibrary/MDS2 (last visited Jan. 24, 2018); *see generally* Shackelford et al., *supra* note 12.

219. *See MW Is Short St. Jude Medical (STJ:US)*, MUDDY WATERS RES., http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/ (last visited Jan. 27, 2018).

220. Interview with Zach Rothstein, *supra* note 8.

221. NH-ISAC, *supra* note 204. For more on NH-ISAC, see *supra* Part IV(A).

Rothstein, to "coordinate all of the different players in the healthcare community in relation to cybersecurity."[222] This group is also likely to take on the issue of supply chain cybersecurity risk management in the medical device context, perhaps even more so than AdvaMed given that it is comprised of associations rather than individual members.[223] As Rothstein explains, "it can be tough to tackle cross-cutting issues like supply chain cybersecurity with diverse members like Intel and Medtronic playing in the same pool."[224]

Rothstein does not think that new legislation is needed in this space—at least on the security side.[225] Rothstein, however, has expressed one exception: "When it comes to cybersecurity, Congress could help with federal structure, particularly at establishing a more hierarchical structure at HHS."[226] Such a move would reportedly be well-received by AdvaMed members and the broader healthcare community, particularly in the confusion after Spectre and Meltdown, and earlier WannaCry, came to light.[227] According to Rothstein: "That's where Congress could really help out."[228] Rothstein further stated: "Two-factor authentication doesn't make sense across the board—yes for in the home, not necessarily in operating rooms where seconds matter—but I think we need to establish an appropriate, clear federal structure to meet these threats."[229] Even though this is unlikely in the near term, AdvaMed reports that the group is just as busy in 2018 as they were during the Obama Administration's second term, with new substantive rules coming from the FDA, including an update on premarket

---

222. Interview with Zach Rothstein, *supra* note 8.

223. *Id.*

224. *Id.*

225. *Id.*

226. *Id.*

227. *Id.*; Simon, *supra* note 33. Spectre and Meltdown are the names given to different variants of the same fundamental underlying vulnerability that affects nearly every computer chip manufactured in the last 20 years and could, if exploited, allow attackers to get access to data previously considered completely protected. Simon, *supra* note 33. The flaw was discovered in late 2017. *Id.* There are three variations on the vulnerability; two of the variants are grouped together as Spectre and the third is deemed Meltdown. *Id.*

228. Interview with Zach Rothstein, *supra* note 8.

229. *Id.*

cybersecurity activities to reflect current best practices for designers that currently dates to 2014.[230]

C. ESKENAZI EXPERIENCE

When reviewing the role played by industry best practices in medical device cybersecurity, it is helpful to include the perspective of a leading hospital system. Eskenazi Health is based in Indianapolis, Indiana, has been in operation for nearly 160 years, and currently provides treatment to nearly one million outpatients annually.[231] The system opened a new 315-bed hospital in 2013,[232] which required a large amount of procurement. During that phase, "the focus was not cybersecurity of medical devices, it was on getting a hospital started," according to Benjamin G. Esslinger, Clinical Engineer Manager of Eskenazi.[233] To help allay any resulting cybersecurity concerns, Eskenazi has used a variety of tools to help secure its Internet of Medical Devices.[234] The hospital bifurcates the responsibility for security between the IT systems touching Eskenazi's networks and the biomedical engineering department that assesses the security of procurement.[235] In particular, the engineering department utilizes the Medical Device Risk Assessment Platform, which is also aligned with the NIST CSF, and takes the form of a pre-procurement questionnaire to ensure that new medical devices meet a minimum-security baseline.[236] According Esslinger, however, it is still necessary to prioritize mitigation strategies for the most vulnerable devices.[237]

One element that helps improve security across Eskenazi's networks is the fact that they do not have a test environment; instead, the hospital system relies on manufacturers obtaining

---

230. *See supra* note 149.

231. *See* ESKENAZI HEALTH, *About*, http://www.eskenazihealth.edu/about (last visited Jan. 24, 2018).

232. *See* ESKENAZI HEALTH, *History*, http://www.eskenazihealth.edu/about/history (last visited Jan. 24, 2018); *see also* ESKENAZI HEALTH, *About*, *supra* note 231.

233. Interview with Ben Esslinger, *supra* note 9.

234. *Id.*

235. *Id.*

236. *Id.*

237. *Id.*

an approved patch[238]—echoing concerns discussed in Part III about this aspect of medical device cybersecurity. And even though partitioning networks can help cordon off threats, there is also the concern of "death by segmentation" in which every network has to be on its own network. Replacing a whole network of devices is not an option given the large outlay that would take. And there are still larger industry problems to address. According to Esslinger: "Manufactures are still selling devices with unsupported operating systems. So, in that case, how do you mitigate the threat?"[239] The unspoken answer seems to be through best practices in procurement, and sharing information with peers. In fact, Eskenazi shares best practices, including with regards to procurement, through the MDISS (MDRAP) Community of Practice, and the Indiana Biomedical Society through educational workshops.[240] Yet information is not readily attainable by manufacturers, underscoring the need for healthy two-way communication to promote due diligence in the Internet of Healthcare.[241]

D. A GLOBAL NOTE

These are dynamic times when it comes to global cybersecurity policy with important new laws in the European Union and China unsettling the status quo. First, in the EU, the General Data Privacy Directive (GDPR) and the Network Information Security (NIS) Directive both have far-reaching implications for IoT regulation generally, and medical devices in particular.[242] Similarly, the new Chinese cybersecurity law will likely impact the medical device industry, but it is unclear as of

---

238. *Id.*

239. *Id.*

240. *Id.*

241. Similar critiques have been made about public-private information sharing schemes in other cybersecurity contexts. *See* Elaine Lammert, *The Public-Private Partnership: A Two-Way Street*, CIPHER BRIEF (Jan. 24, 2016), https://www.thecipherbrief.com/the-public-private-partnership-a-two-way-street.

242. For more on this topic, see Scott J. Shackelford et al., *When Toasters Attack: Enhancing the 'Security of Things' Through Polycentric Governance*, 2017 U. ILL. L. REV. 415 (2017); Philip Piletic, *EU's General Data Protection Regulation Set to Disrupt the Medical Industry*, HEALTH IT OUTCOMES (Aug. 29, 2017), https://www.healthitoutcomes.com/doc/eu-s-general-data-protection-regulation-set-disrupt-medical-industry-0001.

this writing to what extent that will be the case.[243] These disruptions will make it more difficult in the near term to make much progress on global harmonization of cybersecurity best practices as applied to the Internet of Healthcare generally, or medical devices in particular. From the perspective of AdvaMed's members, though, the U.S. has maintained the best regulatory regime, driven by the FDA.[244] According to Rothstein: "They've been really engaged with industry, but also with the broader ecosystem (including with hospitals, even though they don't regulate them)."[245]

But as for the potential of blockchain to enhance medical device cybersecurity, Rothstein, at least, is not yet convinced: "From what I've seen so far, I don't think that blockchain will be a game-changer for the healthcare system."[246] However, he hedged his conclusion a bit with the insight that healthcare organizations often follow the movements of major financial firms, saying: "So, if more financial firms start to incorporate blockchain, will likely see that flow into healthcare."[247] The rapid pace at which the financial industry is embracing blockchain, then, may push the healthcare sector to similarly explore its applications, including in the supply chain context.[248] More exciting at present, at least for Rothstein, are the prospects for machine learning and artificial intelligence, which are topics deserving of further research in the healthcare context.[249]

---

243. *See* Scott J. Shackelford & Frank W. Alexander, *China's Cyber Sovereignty: Paper Tiger or Rising Dragon?*, POL'Y F. (Jan. 12, 2018), https://www.policyforum.net/chinas-cyber-sovereignty/; Mini vandePol & Fun Hui, *New China Cybersecurity Guidelines for Registration of Networked Medical Devices*, BAKER MCKENZIE (Mar. 23, 2017), https://www.bakermckenzie.com /en/insight/publications/2017/03/new-china-cybersecurity-guidelines/.

244. Interview with Zach Rothstein, *supra* note 8.

245. *Id.*

246. *Id.*

247. *Id.*

248. *See, e.g.*, *5 Blockchain Technology Use Cases in Financial Services*, DELOITTE, https://www2.deloitte.com/nl/nl/pages/financial-services/articles/5-blockchain-use-cases-in-financial-services.html (last visited Feb. 22, 2018).

249. For more on how this movement could impact cybersecurity, see BEN BUCHANAN & TAYLOR MILLER, MACHINE LEARNING FOR POLICYMAKERS: WHAT IT IS AND WHY IT MATTERS (2017), https://www.belfercenter.org/sites/default /files/files/publication/MachineLearningforPolicymakers.pdf.

VI. CONCLUSION

This Article has explored cybersecurity vulnerabilities in the healthcare sector with a particular emphasis on the thorny problem of managing supply chains. As we have seen, new technologies like blockchain can help manufacturers and other healthcare stakeholders mitigate cyber risk, but only to a point. In the end, it is vital for these organizations to take lessons from other firms like J&J and invest in proactive cybersecurity best practices while taking cybersecurity seriously as part of its corporate social responsibility.[250] This is part and parcel of an ecosystem-based approach to security the Internet of Healthcare drawing from analogies such as sustainable development in an effort to promote cyber peace. As more organizations embrace such a proactive approach discussed in Part IV, they can become norm entrepreneurs, as Eskenazi Health and AdvaMed have done, establishing "new normative standards" for industry.[251] Eventually, after a tipping point is reached, such bottom-up efforts could catalyze positive network effects and even cause a "norm cascade" in which normative standards, in this context cybersecurity best practices related to supply chain management, become internalized and perhaps eventually codified in national and international laws benefiting global cybersecurity through polycentric action.[252]

In some respects, supply chains are like living organisms: externally, they look like self-contained entities, but internally, they are multifarious systems that depend upon the proper functioning of many invisible sub-systems. Vulnerabilities in these sub-systems don't tend to announce themselves. Disease can long lay dormant and then strike without warning. As a consequence, there is no quick or simple way to make medical device supply chains more robust and impervious to attack. But as challenging as it is, the problem's implications for public

---

250. *See* Shackelford, *supra* note 31.

251. ANNEGRET FLOHR & KLAUS DIETER WOLF, THE ROLE OF BUSINESS IN GLOBAL GOVERNANCE: CORPORATIONS AS NORM-ENTREPRENEURS 10 (2010).

252. *See* Neal K. Katyal, *The Dark Side of Private Ordering: The Network/Community Harm of Crime*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 193–94 (Mark F. Grady & Francesco Parisi eds., 2006) (exploring network effects and network externalities in cyberspace); Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998) (describing the three stages of "the norm 'life cycle,'" including "norm emergence," "norm cascade," and "norm internalization.").

health demand our attention, resources, and creativity. Blockchain is unlikely to be a panacea, but it seems worth exploring as part of a package of technological advancements and regulatory reforms aimed at securing the Internet of Healthcare.