Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 30 | Issue 2 Article 1

January 2013

Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions

Katherine Booth Wellington

CYBERATTACKS ON MEDICAL DEVICES AND HOSPITAL NETWORKS: LEGAL GAPS AND REGULATORY SOLUTIONS

Katherine Booth Wellington†

> America must also face the rapidly growing threat from cyber-attacks. . . . We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.
>
> —Barack Obama[1]

Abstract

Cyberattacks on medical devices and hospital networks are a real and growing threat. Malicious actors have the capability to hack pacemakers and insulin pumps, shut down hospital networks, and steal personal health information. This Article analyzes the laws and regulations that apply to cyberattacks on medical devices and hospital networks and argues that the existing legal structure is insufficient to prevent these attacks. While the Computer Fraud and Abuse Act and the Federal Anti-Tampering Act impose stiff penalties for cyberattacks, it is often impossible to identify the actor behind a cyberattack—greatly decreasing the deterrent power of these laws. Few laws address the role of medical device manufacturers and healthcare providers in protecting against cyberattacks. While HIPAA incentivizes covered entities to protect personal health information, HIPAA does not apply to most medical device manufacturers or cover situations where malicious actors cause harm without accessing personal health information. Recent FDA draft

---

† J.D., Harvard Law School (2013); B.A., Yale University (2008). The author is an Associate at Ropes & Gray LLP, with a focus on healthcare and life sciences law. This paper was written as part of the Petrie-Flom Health Law Policy, Biotechnology, and Bioethics Student Fellowship. The author thanks Professor Benjamin Roin and Professor I. Glenn Cohen for helpful comments and advice. The author also thanks Mikaela Ray and the rest of the editorial staff of the journal. The statements and views expressed in this Article are those of the author, do not reflect those of Ropes & Gray, and do not constitute legal advice or legal opinion.

1. Barack Obama, President of the United States of America, State of the Union Address (Feb. 12, 2013) (transcript *available at* http://www.foxnews.com/politics/2013/02/12/transcript-obama-state-union-speech).

guidance suggests that the agency has begun to impose cybersecurity requirements on medical device manufacturers. However, this guidance does not provide a detailed roadmap for medical device cybersecurity and does not apply to healthcare providers. Tort law may fill in the gaps, although it is unclear if traditional tort principles apply to cyberattacks. New legal and regulatory approaches are needed. One approach is industry self-regulation, which could lead to the adoption of industry-wide cybersecurity standards and lay the groundwork for future legal and regulatory reform. A second approach is to develop a more forward-looking and flexible FDA focus on evolving cybersecurity threats. A third approach is a legislative solution. Expanding HIPAA to apply to medical device manufacturers and to any cyberattack that causes patient harm is one way to incentivize medical device manufactures and healthcare providers to adopt cybersecurity measures. All three approaches provide a starting point for considering solutions to twenty-first century cybersecurity threats.

TABLE OF CONTENTS

INTRODUCTION

Cyberattacks against medical devices and hospital networks[2] are a real and growing threat. Iran's nuclear facilities,[3] Google's servers,[4] U.S. banks,[5] and Persian Gulf oil and gas companies[6] have all been recent victims of cyberattacks. As described in Part I, medical devices and hospital networks are just as vulnerable. Researchers have demonstrated that it is possible to remotely hack implanted insulin pumps and pacemakers—flooding the body with a deadly dose of insulin or releasing a heart-stopping electric charge.[7] Hospital network security breaches have "disrupted glucose monitors, canceled patient appointments and shut down sleep labs" in hospitals.[8] Several hospitals have experienced multi-day network outages due to malware attacks.[9] Medical identity theft—one goal of cyberattacks—is an increasing problem faced by millions of patients each year.[10]

The existing legal structure is insufficient to address these

---

2. This Article focuses on the problem of cyberattacks on both medical devices and hospital networks. It is unclear if a hospital network is a medical device. Commentators have suggested that the FDA could regulate hospital networks as medical devices under the broad definition of "devices" in the Food, Drug, and Cosmetics Act. The FDA may be moving in this direction. *See, e.g.*, Lucas Mearian, *FDA Eyes Regulation of Wireless Networks at Clinics, Hospitals*, COMPUTERWORLD (Jan. 10, 2011, 6:01 AM), http://www.computerworld.com/s/article/9203761/FDA_eyes_regulation_of_wireless_networks_at_clinics_hospitals?taxonomyId=132&pageNumber=1.

3. *Iran Nuclear Facilities Hit by Cyber Attack that Plays AC/DC's Thunderstruck at Full Volume*, MAIL ONLINE (July 25, 2012, 8:43 AM), http://www.dailymail.co.uk/news/article-2178781/Iran-nuclear-facilities-hit-cyber-attack-plays-AC-DCs-Thunderstruck-volume.html.

4. Nicole Perlroth, *Google Warns of New State-Sponsored Cyberattack Targets*, N.Y. TIMES (Oct. 2, 2012, 6:44 PM), http://bits.blogs.nytimes.com/2012/10/02/google-warns-new-state-sponsored-cyberattack-targets.

5. Lee Ferran, *Iran Denies Cyber Attacks on US Banks*, ABC NEWS (Jan. 11, 2013), http://abcnews.go.com/Blotter/iran-denies-cyber-attacks-us-banks/story?id=18191088.

6. Lolita C. Baldor, *US: Hackers in Iran Responsible for Cyberattacks*, NBC NEWS (Oct. 12, 2012, 2:30 PM), http://www.nbcnews.com/technology/technolog/us-hackers-iran-responsible-cyberattacks-1C6423908.

7. Christine Hsu, *Many Popular Medical Devices May Be Vulnerable to Cyber Attacks*, MEDICAL DAILY (Apr. 10, 2012, 1:34 PM), http://www.medicaldaily.com/news/20120410/9486/medical-implants-pacemaker-hackers-cyber-attack-fda.htm.

8. Susan D. Hall, *Hospital Medical Devices Riddled with Malware*, FIERCEHEALTHIT (Oct. 18, 2012), http://www.fiercehealthit.com/story/hospital-medical-devices-riddled-malware/2012-10-18.

9. *Bat Blue KOs Malware in the First Round!*, BAT BLUE NETWORKS, http://www.batblue.com/page.php?55 (last visited Feb. 9, 2014).

10. Taylor Armerding, *Ransom, Implant Attack Highlight Need for Healthcare Security*, CSO (Jan. 8, 2013), http://www.csoonline.com/article/725880/ransom-implant-attack-highlight-need-for-healthcare-security.

threats. As described in Parts II and III, federal and state legal regimes focus primarily on punishing the malicious actors behind cyberattacks. However, these actors are extremely hard to identify and often difficult to prosecute, undercutting the deterrence effects of these regimes. While the Food and Drug Administration (FDA) has the power to regulate the cybersecurity of medical devices and hospital networks, it has only begun to do so through non-binding draft guidance issued in 2013.[11] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) comes the closest to addressing the problem of cyberattacks by requiring healthcare providers to protect patient health information (PHI) on hospital networks.[12] However, HIPAA does not apply to most medical device manufacturers or address scenarios where a cyberattack does not breach PHI.

Given the difficulty of identifying and deterring the malicious actors behind cyberattacks, new approaches are needed to address the threat of these attacks. Part IV describes three potential approaches. The first approach is industry self-regulation, which could lead to the adoption of industrywide cybersecurity standards and lay the groundwork for future legal and regulatory reform. The second approach is to shift the FDA's focus from backward-looking adverse event reporting to forward-looking identification of cybersecurity risks. The regulation of aircraft safety by the Federal Aviation Administration (FAA) provides a model for a flexible approach to addressing and mitigating new threats. The third approach is to adopt a legislative solution to incentivize medical device manufacturers and healthcare providers to adopt security features. Expanding HIPAA to apply to medical device manufacturers and to any type of cyberattack is one potential legislative solution.

This Article makes three contributions. First, it analyzes the current legal framework that applies to cyberattacks on medical devices and hospital networks. To date, there has not been an overarching survey of this kind in the academic literature. Second, it identifies gaps in the statutory and regulatory framework that make

---

11. U.S. DEP'T OF HEALTH & HUMAN SERVS., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2013) [hereinafter CONTENT OF PREMARKET SUBMISSIONS], *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

12. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).

this framework insufficient to address the growing threat of cyberattacks. Finally, it presents three different approaches to addressing the threat of cyberattacks on medical devices and hospital networks.

I. OVERVIEW OF THE THREAT

Cyberattacks may impact individual medical devices or entire hospital networks. Security flaws may permit cyberattacks against individual medical devices, potentially harming the patient relying on the medical device. This could be the result of a malicious attack against an individual patient or simply a computer virus that happens to infiltrate the medical device. Security flaws may also lead to cyberattacks against entire hospital networks, resulting in widespread network outages and "impacting a hospital's ability to treat patients or relay critical information."[13] Security flaws may also permit the theft of patient medical data contained either on medical devices or hospital networks, "lead[ing] to fraudulent claims by the criminal entity to the patient's insurance company or . . . involv[ing] dishonest pharmacists that wire fraudulent prescriptions that are eventually sold on the black market."[14] All of these are serious threats to patient safety and privacy.

There are three primary types of cyberattacks: unauthorized access, malware, and a denial-of-service or distributed-denial-of-service (DDoS) attack.[15] Unauthorized access to a medical device involves "a malicious actor intercepting and altering signals sent wirelessly to the medical device."[16] Medical devices such as pacemakers, neurostimulators, defibrillators, and drug pumps "use embedded computers and radios to monitor chronic disorders and

13. U.S. DEP'T OF HOMELAND SEC., NAT'L CYBERSECURITY & COMMC'NS INTEGRATION CTR., ATTACK SURFACE: HEALTHCARE AND PUBLIC HEALTH SECTOR 3 (2012) [hereinafter ATTACK SURFACE], *available at* http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf.

14. *Id*. at 5.

15. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-816, MEDICAL DEVICES: FDA SHOULD EXPAND ITS CONSIDERATION OF INFORMATION SECURITY FOR CERTAIN TYPES OF DEVICES 15 (2012), *available at* http://www.gao.gov/assets/650/647767.pdf. "A 'denial-of-service' attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include attempts to 'flood' a network, thereby preventing legitimate network traffic; attempts to disrupt connections between two machines, thereby preventing access to service; attempts to prevent a particular individual from accessing a service; [or] attempts to disrupt service to a specific system or person." *Denial of Service Attacks*, CARNEGIE MELLON SOFTWARE ENGINEERING INSTITUTE, http://www.cert.org/tech_tips/denial_of_service.html (last updated June 4, 2001).

16. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 15.

treat patients with automatic therapies."[17] These computers and radios use electronic signals to communicate with devices outside of the body, creating an opportunity for a malicious actor to intercept the signals and disrupt the functioning of the medical device.[18]

Malware "is a malicious software program designed to carry out annoying or harmful actions."[19] The susceptibility of a medical device or hospital network to malware depends on the software involved; some types of software are susceptible to malware, while others are not.[20] As medical device manufacturers and hospital networks increasingly rely on off-the-shelf software, the threat of malware increases.[21] A DDoS attack often involves a computer worm or virus that "overwhelm[s] a device by excessive communication attempts, making the device unusable by either slowing or blocking functionality or draining the device's battery."[22] DDoS attacks may also occur against hospital networks. All three types of attacks may disrupt the functioning of the medical device or network, potentially harming patients.

A. Cyberattacks on Individual Medical Devices

The *Homeland* episode aside,[23] there have been no documented incidents of a patient suffering harm from an attack on a medical device. As one government panel discussion revealed, however, medical devices in hospitals are "riddled" with malware, which can "clog patient-monitoring equipment and other software systems, at times rendering the devices temporarily inoperable."[24] According to McAfee, a security company, "[m]edical devices, such as diagnostic

17. Daniel Halperin et al., *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, 2008 IEEE SYMPOSIUM ON SEC. & PRIVACY 129.

18. *Id.*

19. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 15.

20. *See id.*

21. *See* Martha Vockley, *Safe and Secure? Healthcare in the Cyberworld*, BIOMEDICAL INSTRUMENTATION & TECH., May-June 2012, at 165-66, *available at* http://www.aami.org/publications/bit/2012/Healthcare_Cybersecurity_BIT_MayJune2012.pdf.

22. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 15.

23. Tarun Wadhwa, *Yes, You Can Hack a Pacemaker (and Other Medical Devices Too)*, FORBES (Dec. 6, 2012, 8:31 AM), http://www.forbes.com/sites/singularity/2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too ("On Sunday's episode of the Emmy award-winning show *Homeland*, the Vice President of the United States is assassinated by a group of terrorists that have hacked into the pacemaker controlling his heart.").

24. David Talbot, *Computer Viruses are "Rampant" on Medical Devices in Hospitals*, MIT TECHNOLOGY REVIEW (Oct. 17, 2012), http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals.

tablet computers, heart rate monitors, and MRI scanners, are just as susceptible to malware as standard laptop computers."[25] At Boston's Beth Israel Deaconess Medical Center, one study showed that 664 medical devices ran on outdated software.[26] The hospital reported taking one or two medical devices offline each week to remove malware.[27] While software updates are available to combat malware, manufacturers may not permit hospitals to update the software on a medical device because the manufacturer fears that doing so will cause the device to lose FDA approval[28]—even though, according to the FDA, this is not the case.[29] Hospitals have described the regulatory process to update software as "onerous."[30]

While there are no reports of injuries to patients due to malware on medical devices, there have been close calls. In one hospital, "malware at one point slowed down fetal monitors used on women with high-risk pregnancies being treated in intensive-care wards."[31] In another instance, the Conficker worm,[32] a type of computer virus, "caused problems with a Philips obstetrical care workstation, a GE radiology workstation, and nuclear medical applications," although no one was apparently injured.[33] It is likely only a matter of time before malware causes harm to a patient in a critical situation.

Through several controlled experiments, researchers have shown that unauthorized access and DDoS attacks against medical devices are possible. In 2008, researchers gained remote access to one type of defibrillator.[34] The researchers conducted a "reprogramming attack," which "changes the operation of (and the information contained in)

---

25. *Medical Device Security*, MCAFEE, http://www.mcafee.com/us/industry/healthcare/medical-device-security.aspx (last visited Feb. 9, 2014).

26. *See* Talbot, *supra* note 24.

27. *See id.*

28. *See id.*

29. U.S. Food & Drug Admin., *Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility*, FDA (Nov. 4, 2009), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm189111.htm [hereinafter *Reminder from FDA*].

30. Talbot, *supra* note 24 (internal quotation marks omitted).

31. *See id.*

32. The Conficker worm can disable Windows security features and download arbitrary files. *Help Protect Yourself from the Conficker Worm*, MICROSOFT SAFETY AND SECURITY CENTER, http://www.microsoft.com/security/pc-security/conficker.aspx#EWC (last visited Feb. 9, 2014).

33. Talbot, *supra* note 24.

34. Halperin, *supra* note 17, at 1.

the defibrillator."[35] The researchers then altered when the device administered electric shocks, gaining the ability to administer a shock on command.[36] The researchers also demonstrated that DDoS attacks against the device were possible: "[A]n attacker can keep a [defibrillator] in a state of elevated energy consumption" by making the battery-operated defibrillator communicate indefinitely with an outside device.[37] Because DDoS attacks deplete battery life, this type of attack could prevent a defibrillator from functioning when a patient needs it.[38]

In 2010, another set of researchers demonstrated that they could gain unauthorized remote access to an insulin pump from 100 feet away.[39] The researchers "(1) chang[ed] already-issued wireless pump commands; (2) generat[ed] unauthorized wireless pump commands; (3) remotely chang[ed] the software or setting on the device; and (4) den[ied] communication with the pump device."[40] In other words, the researchers gained the ability to instruct the insulin pump to flood the body with insulin, potentially killing a person. The researchers also found that a malicious actor could interrupt the communication between the insulin pump and the patient's insulin control unit, preventing the patient from adding insulin to her bloodstream when needed. The researchers noted similar security flaws with wireless blood glucose monitors.[41] Many insulin pump systems also use a mobile phone to help patients monitor their glucose levels.[42] A malicious actor who breached the security of the mobile phone may be able to use the phone to change the insulin pump's settings.[43]

More recently, security researchers have demonstrated that it is possible to hack an insulin pump from as far away as 300 feet away.[44] Although previous experiments had required researchers to know the pump ID of an insulin pump in order to hack it, the security researcher Barnaby Jack created a device that could scan a room

35. *Id.*

36. *Id.* at 2.

37. *Id.*

38. *Id.*

39. *See* Nathanael Paul et al., *A Review of the Security of Insulin Pump Infusion Systems*, 5 J. OF DIABETES SCI. & TECH. 1557 (2011), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3262727.

40. *Id.* at 1559.

41. *Id.* at 1559-60.

42. *Id.* at 1560.

43. *Id.*

44. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 19.

looking for insulin pump IDs.[45] Using this device, Jack was able to identify the insulin pump ID of a volunteer and then cause the insulin pump to dispense insulin—up to a deadly dose.[46]

It is difficult to know when—and if—a malicious actor will exploit these vulnerabilities. According to security researcher David Harley, "there are easier ways of committing mass murder than death by pacemaker hacking, and there are certainly easier ways of harvesting patient data than by hacking individual devices for the meagre [sic] Patient Identifiable Data (PID) that may be embedded there."[47] In contrast, security researcher Alexandru Balan notes that "'[a]n unspoken law of IT security is that any vulnerability will eventually be exploited. . . . The scenarios that derive from this may very well look like crime movies. Hackers can perform attempts at patients' lives, steal information about high profile public figures . . . .'"[48] Considering the rise in malware and DDoS attacks against hospitals and the recent publicity over the relative ease of hacking medical devices, it is likely only a matter of time before a malicious actor conducts an attack against a personal medical device like a pacemaker or insulin pump. New approaches are needed to guard against these types of attacks.

B. Cyberattacks on Hospital Networks

In addition to disrupting the functioning of individual medical devices, malware infections may impact an entire hospital network.[49] Any network outage at a hospital can cause "chaos."[50] Malware can shut down some or all of the computer systems in a hospital. According to one security firm, "a multi-day malware outbreak" at a

45. *Researcher Ups Ante on Hacking Medical Devices*, INFOSEC ISLAND (Oct. 31, 2011), http://isa.infosecisland.com/blogview/17785-Researcher-Ups-Ante-on-Hacking-Medical-Devices.html.

46. *Id.*

47. David Harley, *Malware and Medical Devices: Hospitals Really Are Unhealthy Places*, WELIVESECURITY (Oct. 18, 2012, 3:19 AM), http://blog.eset.com/2012/10/18/malware-and-medical-devices-hospitals-really-are-unhealthy-places.

48. Bianca Stanescu, *Heart Patients, Diabetics at Increasing Risk from Medical Device Malware*, HOTFORSECURITY (Nov. 1, 2012), http://www.hotforsecurity.com/blog/heart-patients-diabetics-at-increasing-risk-from-medical-device-malware-4226.html.

49. ATTACK SURFACE, *supra* note 13, at 6.

50. Siobhan Chapman, *Computer Outage Leaves Hospital in Chaos*, COMPUTERWORLD UK (Nov. 28, 2008, 12:05 PM), http://www.computerworlduk.com/news/it-business/12162/computer-outage-leaves-hospital-in-chaos; Bob Brewin, *August VA Systems Outage Crippled Western Hospitals, Clinics*, GOVERNMENT EXECUTIVE (Oct. 5, 2007), http://www.govexec.com/defense/2007/10/august-va-systems-outage-crippled-western-hospitals-clinics/25469.

New York City hospital shut down all of the hospital's applications, with "over 3 million malware compromise attempts per hour."[51] While the security firm was able to fix the problem within a day, a day is a long time for a hospital to function without its computer systems. Other hospitals have also suffered malware outbreaks. According to a Veterans Administration report, "173 incidents of security breaches of medical devices from 2009-2011 . . . disrupted glucose monitors, canceled patient appointments and shut down sleep labs."[52]

DDoS attacks can also affect hospital networks. In 2002, the Beth Israel Deaconess Medical Center's entire computer system was shut down by a "napster-like application that began exchanging hundreds of gigabytes of data via multicast to multiple collaborators."[53] It took the hospital two days to bring its computer systems back online.[54] In 2009, the FBI foiled the plans of twenty-six-year-old hacker Jesse McGraw to use a hospital's computer network to launch a DDoS attack on a rival hacker group.[55] Prior to his arrest, McGraw had already "install[ed] malicious botnet code" on hospital computers, "allowing him to remotely access the systems, in preparation for launching . . . DDoS[] attacks."[56] McGraw had also "impaired the integrity of some of the computer systems by removing security features, e.g., uninstalling anti-virus programs, which made the computer systems and related networks more vulnerable to attack."[57] By gaining access to a computer controlling the heating and ventilation for the hospital, McGraw "could have affected the treatment and recovery of patients who were vulnerable to changes in the environment. In addition, he could have affected treatment regimes, including the efficacy of all temperature-sensitive drugs and

51. *See Bat Blue KOs Malware in the First Round!*, *supra* note 9.

52. Hall, *supra* note 8.

53. John D. Halamka, *The CareGroup Network Outage*, LIFE AS A HEALTHCARE CIO (Mar. 4, 2008, 5:44 PM), http://geekdoctor.blogspot.com/2008/03/caregroup-network-outage.html.

54. *Id.*

55. Mathew J. Schwartz, *Hospital Hacker 'GhostExodus' Sentenced to 9 Years*, INFORMATIONWEEK (Mar. 22, 2011, 11:27 AM), http://www.informationweek.com/security/attacks/hospital-hacker-ghostexodus-sentenced-to/229400039.

56. *Id.*

57. Press Release, U.S. Attorney's Office, N. Dist. of Tex., Former Security Guard Who Hacked Into Hospital's Computer System Sentenced to 110 Months in Federal Prison (Mar. 18, 2011), *available at* http://www.fbi.gov/dallas/press-releases/2011/dl031811.htm.

supplies."[58]

Hospital network and medical device security are interrelated. Medical devices with poor information security features can act as a vector through which malware or DDoS attacks enter hospital networks. According to the National Cybersecurity and Communications Integration Center, "[s]ince wireless [medical devices] are now connected to Medical information technology (IT) networks, IT networks are now remotely accessible through the [medical device]. . . . [T]he communications security of [medical devices] is now becoming a major concern."[59] Medical devices must therefore have sufficient security features to prevent both tampering with the medical device itself and using the medical device as an entry point to spread malware or conduct a DDoS attack against a hospital network.

C. Cyberattacks Leading to Theft of Medical Information

The theft of medical information contained on medical devices and networks is a growing threat. Malware can steal medical information from both medical devices and hospital networks.[60] Because some medical devices such as insulin pumps wirelessly broadcast patient information, malicious actors using specialized equipment can access patient medical information from as far as 300 feet away.[61] For example, an implanted defibrillator may broadcast the patient's name and diagnosis, in addition to the patient's vital signs.[62] Malicious actors may also steal patient information directly from hospitals. Ninety-four percent of healthcare providers experienced at least one data breach in 2011 or 2012.[63] According to a 2013 Ponemon Institute study, over 1.8 million Americans have been affected by medical identity theft, costing on average $18,660 per victim.[64] The total out-of-pocket cost of medical identity theft in

58. *Id.*

59. ATTACK SURFACE, *supra* note 13, at 2.

60. *Id.* at 5.

61. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 19.

62. Halperin, *supra* note 17, at 2.

63. PONEMON INSTITUTE, THIRD ANNUAL BENCHMARK STUDY ON PATIENT PRIVACY & DATA SECURITY 1 (2012), *available at* http://www2.idexpertscorp.com/assets/uploads/ponemon2012/Third_Annual_Study_on_Patient_Privacy_FINAL.pdf.

64. PONEMON INSTITUTE, 2013 SURVEY ON MEDICAL IDENTITY THEFT 4-5 (2013), *available at* http://clearwatercompliance.com/wp-content/uploads/2013/10/2013-Medical-Identity-Theft-Report-FINAL.pdf.

the United States is over $12 billion.[65] Breaches of PHI almost doubled from 2010 to 2011, and "525 breaches . . . involving 21.4 million individuals" occurred over a three-year period between 2009 and 2012.[66]

Medical identity theft can "lead[] to fraudulent claims by the criminal entity to the patient's insurance company or may even involve dishonest pharmacists that wire fraudulent prescriptions that are eventually sold on the black market."[67] One scheme involved stealing the medical information of 7000 patients, encrypting it, and then demanding a ransom to unencrypt the information so that patients and doctors could access it.[68] Missing or incorrect patient health information can lead to an "improper diagnosis or therapy," which may result in harm or death due to "delayed or inappropriate treatment."[69]

Researchers have recently demonstrated that they could hack two widely used medical management platforms that operate medical devices. From these platforms, researchers accessed patient information in connected databases.[70] By gaining access to the medical management platform, researchers were also able to theoretically operate any medical devices connected to the platform—such as an X-ray machine.[71] Given the growing threat of cyberattacks against medical devices and hospital networks, new approaches are needed to protect patients against attacks that could result in patient harm or medical identity theft.

II. CURRENT LEGAL STRUCTURE

There are three legal regimes governing cyberattacks on medical devices and hospital networks. First, federal statutes such as the Computer Fraud and Abuse Act (CFAA) and the Federal Anti-

65. *Id.*

66. Armerding, *supra* note 10.

67. ATTACK SURFACE, *supra* note 13, at 5.

68. Armerding, *supra* note 10.

69. Stephen L. Grimes, Chairman, Medical Device Security Workgroup, Overview of Medical Devices and HIPAA Security Compliance 9 (March 9, 2005), *available at* http://www.shcta.com/ftp/Presentations/Overview%20of%20Medical%20Device%20Security%20and%20HIPAA%20Compliance%20050228.pdf.

70. Darren Pauli, *Patient Data Revealed in Medical Device Hack*, SC MAGAZINE AUSTRALIA (Jan. 17, 2013, 6:30 PM), http://www.scmagazine.com/patient-data-revealed-in-medical-device-hack/article/276568.

71. John Leyden, *Paging Dr. Evil: Philips Medical Device Control Kit 'Easily Hacked,'* THE REGISTER (Jan. 18, 2013, 5:03 PM), http://www.theregister.co.uk/2013/01/18/medical_device_control_kit_security.

Tampering Act impose criminal liability on the malicious actors behind cyberattacks. Second, federal regulatory regimes including the Federal Food, Drug, and Cosmetic Act (FDCA) and HIPAA govern medical device manufacturers and healthcare providers. HIPAA provides some protection against cyberattacks by creating a regulatory framework to safeguard PHI. Under FDCA, the FDA has begun to evaluate cybersecurity as a part of the medical device approval process. However, the FDA has only recently issued draft guidance in this area and has yet to develop a regulatory approach designed to address rapidly evolving security threats. Finally, civil common law and state criminal law impose liability on the malicious actors behind cyberattacks and may also impose negligence liability on medical device manufacturers and healthcare providers. As discussed in Part III, these legal regimes are insufficient to address the threat of cyberattacks because they focus on deterring the malicious actors behind cyberattacks rather than on encouraging medical device manufacturers and hospitals to improve medical device and hospital network security.

A. Computer Fraud and Abuse Act

The CFAA[72] punishes malicious actors who transmit code or access protected computers, causing harm. This Act applies to malicious actors who conduct cyberattacks against medical devices and hospital networks.[73] Despite its expansive reach, however, the Act only criminalizes knowing and intentional acts.[74] It does not impose negligence liability on the developers or users of medical devices or hospital networks with poor security features.[75] Nevertheless, it is a powerful statute for prosecuting the malicious actors behind cyberattacks.

The CFAA's broad language criminalizes almost any knowing or intentional cyberattack. Under the CFAA, "[w]hoever . . . *knowingly*

72. 18 U.S.C. § 1030 (2012).

73. *Id.*

74. *Id.* §§ 1030(a)(5)(A)-(B).

75. *See* United States v. Mitra, 405 F.3d 492, 495-96 (7th Cir. 2005) ("What protects people who accidently erase songs on an iPod, trip over . . . a wireless base station, or rear-end a car and set off a computerized airbag, is not judicial creativity but the requirements of the statute itself: the damage must be intentional); Doe v. Dartmouth-Hitchcock Med. Ctr., No. CIV. 00-100-M, 2001 WL 873063 (D.N.H. July 19, 2001) (noting that a plaintiff could only recover under the CFAA against a defendant who violated the statute by accessing the plaintiff's "medical records without authority," not against the hospital system whose records were allegedly violated).

causes the transmission of a program, information, code, or command, and as a result of such conduct, *intentionally* causes damage without authorization, to a protected computer"[76] is punishable by "a fine under this title, imprisonment for not more than 10 years, or both"[77] for the first offense. If the actor "*intentionally* accesses a protected computer without authorization, and as a result of such conduct, *recklessly* causes damage,"[78] the actor faces "a fine . . . or imprisonment for not more than 5 years, or both" for a first offense involving:

> (I) [L]oss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value, (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals, (III) physical injury to any person; [or] (IV) a threat to public health or safety.[79]

This statutory language criminalizes cyberattacks that cause at least $5,000 in harm, physically harm a patient, potentially modify or impair patient diagnosis or treatment, or pose a threat to public health or safety. As a result, even if a cyberattack on a medical device or hospital network causes no physical harm or property damage, a prosecutor may bring charges for "potential" impairment of patient care or for posing a "threat" to public health or safety. Although scholars have criticized the CFAA's sweeping language under the "void for vagueness" doctrine,[80] most courts apply the statute.[81]

The CFAA only applies to acts involving "computers."[82] Under the CFAA, "the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions."[83] Recent case law makes clear that almost anything with a computer chip—such as a digital medical device or hospital network—is a "computer." In *United States v. Kramer*, the Eighth Circuit stated that the definition

---

76. 18 U.S.C. § 1030(a)(5)(A) (emphasis added).

77. *Id.* § 1030(c)(4)(B).

78. *Id.* § 1030(a)(5)(B) (emphasis added).

79. *Id.* § 1030(c)(4)(A)(i).

80. *See, e.g.*, Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1581 (2010).

81. *See, e.g.*, United States v. Kramer, 631 F.3d 900 (8th Cir. 2011); United States v. Mitra, 405 F.3d 492 (7th Cir. 2005). *But see* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

82. 18 U.S.C. § 1030.

83. *Id.* § 1030(e)(1).

of a computer in the CFAA "is exceedingly broad. . . . This definition captures any device that makes use of a electronic data processor."[84] Applying this definition, the court found that a cell phone was a computer.[85] In *United States v. Mitra*, the Seventh Circuit noted that "[s]ection 1030 is general. Exclusions show just *how* general. Subsection (e)(1) carves out automatic typewriters, typesetters, and handheld calculators; this shows that other devices with embedded processors and software are covered. As more devices come to have built-in intelligence, the effective scope of the statute grows."[86] Applying the *expressio unius* principle, the *Mitra* court held that a radio is a "computer" because it contained a "computer chip."[87]

Based on this case law, hospital networks are covered under the CFAA because they utilize "electronic data processor[s]" and "computer chips." The Department of Justice (DOJ) manual on computer crime supports this view. According to this manual, the CFAA:

> [P]rovides strong protection to the computer networks of hospitals, clinics, and other medical facilities because of the importance of those systems and the sensitivity of the data that they contain. . . . The evidence only has to show that at least one patient's medical care was at least *potentially* affected as a consequence of the intrusion.[88]

The hacker Jesse McGraw was convicted under CFAA Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i)(II) for accessing a hospital network and "downloading a malicious code into a protected computer without authorization" and was sentenced to nine years in prison,[89] similarly supporting an interpretation of "computer" that applies to hospital networks.

Under this case law, many medical devices also fall under the definition of "computer." As long as a medical device has a computer

---

84. *Kramer*, 631 F.3d at 902-04.

85. *Id.* (finding that a cell phone was a computer under the broad definition of "computer" under the CFAA even though "a 'basic' cell phone might not easily fit within the colloquial definition of 'computer').

86. See United States v. Mitra, 405 F.3d at 495.

87. *See id.* at 493-94.

88. OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS, COMPUTER CRIME AND INTELLECTUAL PROP. SECTION CRIMINAL DIV., PROSECUTING COMPUTER CRIMES 45 (2d ed. 2010), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

89. United States v. McGraw, No. 3:09-CR-0210-B, 2012 WL 6004208 (N.D. Tex. Nov. 5, 2012); United States v. McGraw, No. 3:09-CR-0210-B, 2012 WL 6013258 (N.D. Tex. Dec. 3, 2012).

chip or performs basic data processing functions, the CFAA applies. Wireless or networked medical devices, for example, are "computers" because they must perform data processing functions in order to transmit electronic information.

Given the broad definition of "computer" under the CFAA, supported by case law in the Seventh and Eighth Circuits, there is little question that a malicious actor would violate the CFAA by conducting a cyberattack on a medical device or hospital network. If the government can identify the malicious actor behind a cyberattack, the CFAA's expansive language and hefty penalties provide the government with a powerful prosecutorial tool. However, as discussed in Part III, it is very difficult to identify the malicious actors behind cyberattacks. Thus while the CFAA may prescribe steep penalties for conducting a cyberattack, it may not serve as a sufficient deterrent against these attacks. For this reason, new approaches to preventing cyberattacks are needed.

B. Federal Anti-Tampering Act

The Federal Anti-Tampering Act[90] (Anti-Tampering Act) criminalizes "tampering" with consumer products, including medical devices. Similar to the CFAA, the Anti-Tampering Act's steep penalties make it a powerful tool for prosecutors. However, while the Anti-Tampering Act likely applies to malicious actors who conduct cyberattacks, it does not apply to medical device manufacturers or hospitals that negligently fail to secure their devices or networks. In addition, it is an open question whether the Anti-Tampering Act applies to a cyberattack on a hospital network or to a cyberattack that causes patient harm but does not itself affect the operation of a medical device.

Because there have been no reported cyberattacks on medical devices leading to patient harm, the Anti-Tampering Act has not received much attention by courts or scholars in the context of cyberattacks on medical devices or hospital networks. The government has prosecuted cyberattacks on hospital networks under the CFAA, which provides for five- or ten-year sentences, depending on whether the actor intentionally or recklessly caused damage.[91] The Anti-Tampering Act penalties are harsher, but they require tampering

90. 18 U.S.C. § 1365 (2012).

91. *See infra* Part II.A.

with a "consumer product."[92] A "consumer product" is defined as "any 'food,' 'drug,' 'device,' or 'cosmetic,'"[93] which includes medical devices[94] but may not include hospital networks.

The Anti-Tampering Act does not define "tampering," leaving this term open to interpretation by the courts.[95] While it is unclear how courts will rule on this issue, it is likely that a cyberattack on a medical device is "tampering." In *United States v. Garnett*, the Eleventh Circuit upheld the conviction of a defendant under the Anti-Tampering Act for removing hydrocodone tablets from pill bottles and "introducing other drugs into the bottles after scratching off their identifying marks."[96] Even though "Garnett did not alter the hydrocodone tablets themselves, his actions constitute tampering" because "Garnett increased the risk that injury from incorrectly dispensed drugs would occur."[97] The court relied on "§1365's purpose—increasing the penalty for willful wrongful conduct" in reaching its conclusion.[98] In *United States v. Walton*, the Seventh Circuit upheld the conviction of a pacemaker vendor under the Anti-Tampering Act for changing the use-by dates of pacemakers and then selling the out-of-date pacemakers to hospitals.[99] The court found that Walton's conduct "falls quite clearly within the statutory prohibitions."[100]

Although most cases prosecuted under the Anti-Tampering Act have involved defendants tampering with controlled substances in

---

92. Under the Federal Anti-Tampering Act,

> Whoever, with reckless disregard for the risk that another person will be placed in danger of death or bodily injury and under circumstances manifesting extreme indifference to such risk, tampers with any consumer product that affects interstate or foreign commerce, or the labeling of, or container for, any such product, or attempts to do so, shall—in the case of attempt, be fined under this title or imprisoned not more than ten years, or both; if death of an individual results, be fined under this title or imprisoned for any term of years or for life, or both; if serious bodily injury to any individual results, be fined under this title or imprisoned not more than twenty years, or both; and in any other case, be fined under this title or imprisoned not more than ten years, or both.

18 U.S.C. § 1365(a) (2012).

93. *Id*. § 1365(h)(1)(A).

94. *See* 21 U.S.C. § 321(h) (2012).

95. *See* United States v. Garnett, 122 F.3d 1016, 1018 (11th Cir. 1997).

96. *Id*.

97. *Id*.

98. *Id*.

99. United States v. Walton, 36 F.3d 32, 33 (7th Cir. 1994).

100. *Id*. at 35.

medical syringes or pill bottles,[101] the Anti-Tampering Act should also apply to defendants who electronically tamper with medical devices. A cyberattack against a medical device may include turning off the device or altering the device's function. Both actions would risk injury to the patient by disrupting the treatment regime, which under *Garnett* should constitute tampering. A malicious actor who hacks into a patient's medical device and then uses that device as a way to access a hospital network (perhaps to conduct a DDoS attack or to steal patient health information) could disrupt the device's function, slowing down its processing speed or affecting the ability of the medical device to interface with the network. This conduct should also constitute "tampering."

Even if a malicious actor does not alter the medical device itself—just as the defendant did not alter the hydrocodone tablets in *Garnett*—a cyberattack may fall under the Anti-Tampering Act if the defendant's access to the medical device could potentially harm patients. For example, a malicious actor could use a medical device as an access point to disrupt a hospital network, leaving the medical device intact but potentially harming other hospital patients relying on the hospital network. Under *Garnett*, this could fall under the Anti-Tampering Act's purpose to penalize "willful wrongful conduct." It is unclear how a court would come out on this issue.

It is similarly unclear whether the Anti-Tampering Act criminalizes the disruption of a hospital network rather than the disruption of a medical device. The Anti-Tampering Act defines "consumer products" broadly to include "devices," and thus if a hospital network is a device, it likely qualifies. However, it is unclear if a hospital network is a medical device.[102] Even if a hospital network is not itself a "device," hospitals routinely connect medical devices to their networks. If a malicious code shuts down a hospital network, and therefore prevents a connected medical device from functioning properly, it is possible that the Anti-Tampering Act applies. A court looking to the purpose of this Act under *Garnett* might find liability, whereas a court more strictly construing "tampering" might not find liability where the effect on a medical device is one step removed from the defendant's actions. A court could look to the foreseeability of the harm to a medical device to

101. *See, e.g.*, United States v. Gonsalves, 435 F.3d 64 (1st Cir. 2006); Jane W. v. President & Directors of Georgetown College, 863 A.2d 821 (D.C. 2004); United States v. Garnett, 122 F.3d 1016 (11th Cir. 1997).

102. *See* Mearian, *supra* note 2.

help determine liability under this Act.

While the Anti-Tampering Act may be somewhat redundant with the CFAA, and prosecutors may be more comfortable prosecuting malicious actors for computer-related crimes under the CFAA, the Anti-Tampering Act may serve as an additional source of criminal liability for cyberattacks. The harsher penalties of the Anti-Tampering Act may appeal to prosecutors, especially in cases where actors have directly hacked medical devices rather than hospital networks and the provisions of the Anti-Tampering Act more clearly apply. However, this Act does not impose penalties on medical device manufacturers or hospitals that do not adopt measures to prevent "tampering" with these devices or networks. For this reason, the Act may ultimately do little to deter cyberattacks.

C. Health Insurance Portability and Accountability Act of 1996

HIPAA regulates the privacy and security of PHI such as patient names, diagnoses, and the serial numbers of medical devices.[103] Accordingly, HIPAA plays a central role in medical device cybersecurity. HIPAA does not, however, address some of the central issues posed by the threat of cyberattacks on medical devices and hospital networks. Because HIPAA focuses on the security of PHI, it does not address cyberattacks that disrupt devices or networks but do not involve a breach of PHI. HIPAA also does not apply to most medical device manufacturers. As a result, HIPAA incentivizes hospitals to adopt more secure networks—at least where PHI is involved—but does little to incentivize medical device manufacturers to adopt security features. Despite its underinclusiveness, HIPAA's strict liability scheme provides an example of one approach to protecting against cyberattacks.

HIPAA imposes significant responsibilities on healthcare providers to protect against unauthorized disclosure of PHI, levying large fines on providers who suffer breaches of PHI as a result of theft or accident. HIPAA has two main parts: the Privacy Rule and the Security Rule. The Privacy Rule "establishes national standards to protect individuals' medical records and other personal health information" and "requires appropriate safeguards to protect the privacy of personal health information."[104] The Security Rule

103. *Id.*

104. *The Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (last visited Feb. 9, 2014).

"requires appropriate administrative, physician and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[105]

HIPAA only applies to "covered entities." These include hospitals and other healthcare providers, but do not include medical device manufacturers unless they "sell to patients and bill Medicare."[106] Some medical device manufacturers, such as insulin pump manufacturers, are covered entities because they sell directly to Medicare patients.[107] Most, however, are not. HIPAA's criminal provisions apply to covered entities and certain employees of covered entities, but not to individuals unassociated with the covered entity.[108]

Regulations promulgated under the Health Information Technology for Economic and Clinical Health Act[109] (HITECH Act) impose harsh penalties for HIPAA violations and require covered entities to notify patients of a PHI breach. The HITECH Act enforcement rule provides penalties for four different violation categories: "Did Not Know," "Reasonable Cause," "Willful Neglect—Corrected," and "Willful Neglect—Not Corrected." The penalties range from $100 to $50,000 for each violation in the first category and are $50,000 for each violation in the fourth category. "Violations of an identical provision in a calendar year" are capped at $1.5 million.[110] The HITECH Act requires covered entities to "promptly notify affected individuals of a breach, as well as the U.S. Health and Human Services (HHS) Secretary and the media in cases

105. *The Security Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS,, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html (last visited Feb. 9, 2014).

106. *Privacy Basics: A Quick HIPAA Check for Medical Device Companies*, MEDICAL DEVICE & DIAGNOSTIC INDUSTRY (Aug. 1, 2009), http://www.mddionline.com/article/privacy-basics-quick-hipaa-check-medical-device-companies.

107. *See id.*

108. *But see Alabama Woman Sentenced to Prison for Patient Identifications at Hospital*, PRIVATE OFFICER NEWS NETWORK (Feb. 3, 2012), http://privateofficernews.wordpress.com/tag/chelsea-catherine-stewart (noting that a woman unassociated with a hospital was sentenced to three years in prison under a HIPAA criminal provision for "stealing identifying information on more than 4,000 patients from a Birmingham hospital"); Press Release, U.S. Attorney's Office, N. Dist. of Ala., Alabaster Woman Indicted for Stealing Hospital Patient Information (June 28, 2011), *available at* http://www.justice.gov/usao/aln/News/June%202011/June%2028,%202011%20Alabaster%20Woman.html.

109. 42 U.S.C.A. §§ 300jj, 17931-40 (2013).

110. HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56127 (proposed Oct. 30, 2009) (to be codified at 45 C.F.R. pt. 160), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf.

where a breach affects more than 500 individuals."[111] The DOJ has the power to bring criminal cases against covered entities that "knowingly" violate HIPAA,[112] although it rarely does so.[113] A criminal conviction could result in steep fines[114] and exclusion from Medicare, a serious penalty.[115]

The consequences of a HIPAA breach are severe, even when the breach is accidental or the result of theft. For example, the Alaska Department of Health and Social Services (DHSS) paid $1.7 million in a settlement with HHS after a USB drive containing the health information of 2000 patients was stolen.[116] A HHS investigation determined that "DHSS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule."[117] Phoenix Cardiac Surgery, a physician practice, paid $100,000 in a settlement with HHS after an Office of Civil Rights investigation determined "that the physician

111. *HITECH Breach Notification Interim Final Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html (last visited Feb. 9, 2014); *see also* Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740 (Aug. 24, 2009) (to be codified at 45 C.F.R. pts. 160, 164), *available at* http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf.

112. Under Section 1320d-6, HIPAA criminalizes "knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or discloses individually identifiable health information to another person." 42 U.S.C. § 1320d-6(a) (2012).

113. *See DOJ Steps Up Enforcement with Indictment of 'Loose Lips' Doctor, Hospital Visitor*, HEALTH BUSINESS DAILY (July 15, 2011), http://aishealth.com/archive/hipaa0711-01 (noting that DOJ "had prosecuted only a dozen or so criminal HIPAA violations in eight years" and describing two additional cases); *The HIPAA Medical Privacy Law: The Current State of Criminal Enforcement*, KAISER LAW FIRM, PLLC (May 23, 2012), http://kaiserfirm.com/lawyer/2012/05/23/Health_Care_Fraud/The_HIPAA_Medical_Privacy_Law__The_Current_State_of_Criminal_Enforcement_bl4229.htm.

114. The penalty for violation is a fine of up to $50,000, a one-year term of imprisonment or both. 42 U.S.C. § 1320d-6(b)(1). "[I]f the offense is committed under false pretenses," the fine is "not more than $100,000," imprisonment for up to 5 years, or both. *Id*. § 1320d-6(b)(2). "[I]f the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm," the violator may "be fined not more than $250,000, imprisoned not more than 10 years, or both." *Id*. § 1320d-6(b)(3).

115. *Id.* § 1320d-6(b)(3).

116. Press Release, Dep't of Health & Human Servs., Alaska Settles HIPAA Security Case for $1,700,000 (June 26, 2012), *available at* http://www.hhs.gov/news/press/2012pres/06/20120626a.html.

117. *Id.*

practice was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publically accessible."[118] Massachusetts Eye & Ear Infirmary (MEEI) agreed to a $1.5 million settlement with HHS after "an unencrypted personal laptop containing the electronic protected health information (ePHI) of MEEI patients and research subjects was reported stolen."[119]

HHS has begun prosecuting small-scale breaches of PHI. In June of 2010, a laptop containing the PHI of fewer than 500 patients was stolen from the Hospice of North Idaho (HONI).[120] HONI "had not conducted a risk analysis to safeguard []PHI" and "did not have in place policies or procedures to address mobile security as required by the HIPAA Security Rule."[121] In January of 2013, the hospice agreed to a $50,000 settlement with HHS.[122] The HONI case demonstrates that covered entities must protect against even small-scale loss or theft of PHI.

While HIPAA provides for significant penalties for PHI breaches, HIPAA does not adequately address the threat of cyberattacks. HIPAA is focused on protecting patient health information—not patient health. HIPAA does not incentivize hospitals to adopt security measures to protect against cyberattacks that do not involve PHI. It is possible that a malicious actor could conduct a cyberattack against a medical device or hospital network without accessing PHI and thus never run afoul of HIPAA. HIPAA also does not apply to most medical device manufacturers. Increased HIPAA prosecution of medical device manufacturers' customers, such as hospitals, will likely put pressure on medical device manufacturers to take information security risks into account when designing devices. Nevertheless, HIPAA fails to create a direct incentive for medical device manufacturers to adopt improved security measures. While HIPAA is a step in the right direction, it does not provide sufficient protection against the threat of cyberattacks.

---

118. *Id.*

119. Erin McCann, *Massachusetts Group to Pay $1.5M HIPAA Settlement*, HEALTHCARE IT NEWS (Sept. 17, 2012), http://www.healthcareitnews.com/news/massachusetts-group-pay-15m-hipaa-settlement.

120. Press Release, Dep't of Health & Human Servs., HHS Announces First HIPAA Breach Settlement Involving Less than 500 Patients: Hospice of North Idaho Settles HIPAA Security Case for $50,000 (Jan. 2, 2013), *available at* http://www.hhs.gov/news/press/2013pres/01/20130102a.html.

121. *Id.*

122. *Id.*

Although HIPAA is not designed to address all types of cyberattacks, it provides a regulatory model for combatting cybercrime. HIPAA focuses on the entities subject to attack, not the attackers. Such an approach is needed in the realm of cybercrime, where the attacker may be difficult or impossible to identify.[123] HIPAA's sliding scale liability scheme—including strict liability for data breaches where the covered entity "Did Not Know" and was not at fault—incentivizes covered entities to determine the best way to protect PHI. This type of approach makes sense where government regulators may not be able to respond quickly to new security risks. HIPAA's strict liability scheme permits the government to prosecute (or negotiate settlements) with covered entities in an area where the common law negligence standard of care is unclear. Until courts grapple with more cyberattack cases, the standard of care for protecting medical device and hospital networks against cyberattacks will likely remain unclear—providing a rationale for adopting this type of approach. Although HIPAA has its flaws, the Act addresses some of the weaknesses of a traditional regulatory scheme that is unable to respond quickly and flexibly to changing threats. While HIPAA itself does not provide sufficient protection against cyberattacks, it does provide a model for regulating security risks in a digital world. As described in Part IV, Congress could expand HIPAA to more fully address the risk of cyberattacks against medical devices and hospital networks.

D. Food, Drug, and Cosmetics Act

Although the FDA issued draft guidance on medical device cybersecurity in June of 2013,[124] the agency has yet to develop a forward-looking regulatory approach that addresses new cyberattack threats. The FDA has many different regulatory tools—including the premarket notification and approval processes and the postmarket review process—that could help ensure that medical device manufacturers and hospitals take precautions against cyberattacks. The FDA has also asserted its authority over mobile medical applications (MMAs) and medical device data systems (MDDSs), allowing the FDA to regulate medical device software and information storage systems. Until recently, the FDA has not used these tools to ensure that medical devices protect patients from the

123. *See infra* Part III.A.

124. *See* CONTENT OF PREMARKET SUBMISSIONS, *supra* note 11.

threat of cyberattacks in part because the FDA "did not consider information security risks from intentional threats as a realistic possibility . . . ."[125] The FDA's challenge, as described in Parts III and IV, is to recalibrate its regulatory structure to address the rapidly evolving threat of cyberattacks.

1. Overview of FDA Regulation

a. Premarket Notification and Approval

While the Federal Communications Commission (FCC)[126] and the Centers for Medicare and Medicaid Services (CMS)[127] play a role in medical device regulation, the FDA is the primary regulator of medical devices. The FDA's power to regulate "medical devices" is very broad and includes regulation of medical devices, components and accessories of medical devices, MMAs, MDDSs, and likely hospital networks[128] that interface with medical devices.[129] Under this expansive definition of "medical devices," the FDA has extended its regulatory authority to new types of devices, from smartphones that

125. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 1.

126. The FCC has regulatory authority over "various media and communication technologies, including the allocation of frequencies and the specification of technical requirements to ensure the security and reliability of wirelines, broadband, and wireless communication devices." Vernessa T. Pollard & Chandra Branham, *FDA Medical Device Requirements: A Legal Framework for Regulating Health Information Technology, Software, and Mobile Apps*, RECENT DEV. IN FOOD & DRUG LAW 2011, 2011 WL 5833341, at *9. FCC has agreed to partner with FDA to "develop a coordinated regulatory approach for wireless-enabled medical devices, mobile apps, and other health IT." *Id.*; *see* Margaret A. Hamburg, Comm'r, Food & Drug Admin., Remarks at the FDA/FCC Public Workshop: Enabling the Convergence of Communications and Medical Systems (July 26, 2010), *available at* http://www.fda.gov/NewsEvents/Speeches/ucm220447.htm.

127. CMS is not "being as active from an enforcement standpoint with respect to health IT products." Vernessa T. Pollard & Chandra Branham, *FDA Medical Device Requirements: A Legal Framework for Regulating Health Information Technology, Software, and Mobile Apps*, RECENT DEV. IN FOOD & DRUG LAW 2011, 2011 WL 5833341, at *9. However, CMS could play a much greater role in determining which medical devices and mobile applications to reimburse under federal programs like Medicare. *Id*.

128. Mearian, *supra* note 2.

129. Under the FDCA,

> The term 'device' . . . means an instrument, apparatus, implement, machine, contrivance, implant in vitro reagent, or similar or related article, including any component, part, or accessory, which is . . . intended for the 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 other function of the body . . . and which does not achieve its primary intended purpose through [chemical or metabolic action].

21 U.S.C. § 321(h) (2012).

allow doctors to view ultrasound images[130] to software "intended for use in the diagnosis of disease or other conditions."[131]

Under the Medical Device Amendments Act of 1976 (MDAA), there are three regulatory classifications for medical devices.[132] "Class I devices are typically simple in design, manufacture and have a history of safe use," such as "tongue depressors, arm slings, and hand-held surgical instruments."[133] These devices are unlikely to have wireless connections or otherwise be subject to cyberattacks, although as discussed below, medical device data systems are now Class I devices. A device falls under Class II if there are more concerns about its "safety and effectiveness."[134] Examples of these types of devices are insulin pumps,[135] "physiologic monitors, x-ray systems, [and] gas analyzers."[136] The majority of wireless medial devices are Class II devices.[137] Class III medical devices are those devices that are "life-supporting or life-sustaining, or for a use which is of substantial importance in preventing impairment of human health, or if the device presents a potential unreasonable risk of illness or injury."[138] This includes devices like cardiac defibrillators.[139]

There are three different levels of regulatory review of medical

---

130. *See* Scott Jung, *Mobisante's MobiUS Smartphone Ultrasound Receives FDA 510(k) Clearance*, MEDGADGET (Feb. 7, 2011, 1:58 PM), http://www.medgadget.com/2011/02/mobisantes_mobius_smartphone_ultrasound_receives_fda_510k_clearance.html.

131. Scott D. Danzis & Christopher Pruitt, *Rethinking the FDA's Regulation of Mobile Medical Apps*, 9 THE SCITECH LAWYER, no. 3, 2013, *available at* http://www.cov.com/files/Publication/56c8d97e-4432-4623-b81c-1230545cc204/Presentation/PublicationAttachment/cb8b13fe-9b8f-4de4-b8d3-15096d3b25be/Rethinking_the_FDA's_Regulation_of_Mobile_Medical_Apps.pdf.

132. Medical Device Amendments Act of 1976, 21 U.S.C.A. § 360c (West 2014).

133. *2008-04 FDA Device Classification*, LEEDERGROUP [hereinafter *FDA Device Classification*], http://leedergroup.com/bulletins/fda-device-classification (last visited Feb. 9, 2014).

134. 21 C.F.R. § 860.3 (2012), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2012-title21-vol8/pdf/CFR-2012-title21-vol8-sec860-3.pdf.

135. *Id.* § 880.5725 (2014), *available at* http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?fr=880.5725.

136. *FDA Device Classification*, *supra* note 133.

137. *Wireless Medical Technologies: Navigating Government Regulation in the New Medical Age*, FISH & RICHARDSON, at 6, http://www.fr.com/files/uploads/attachments/FinalRegulatoryWhitePaperWirelessMedical Technologies.pdf (last updated Nov. 2013).

138. 21 C.F.R. § 860.3 (2012), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2012-title21-vol8/pdf/CFR-2012-title21-vol8-sec860-3.pdf.

139. 21 C.F.R. § 870.5310 (2013), *available at* http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=870.5310.

devices: Premarket approval (PMA), 510(k) premarket notification, and quality controls. The highest level of review is the lengthy and expensive PMA process, which "demands extensive and meticulous documentation to demonstrate safety and effectiveness."[140] If PMA is not required, all medical devices must undergo 510(k) review unless the device is exempt from premarket notification.[141] "A 510(k) is a premarket submission made to the FDA to demonstrate that the device to be marketed is at least as safe and effective, that is, substantially equivalent" to a device already on the market when the MDAA was passed in 1976.[142] The 510(k) process is roughly three times faster and fifty times cheaper than the PMA process.[143] Manufacturers of devices that are subject to FDA regulation but do not require PMA or 510(k) review still "need to adopt a quality system, register and list with the FDA, and report adverse events associated with their product."[144]

Some devices—primarily Class I devices—are only subject to quality controls.[145] Most Class II devices and three-fourths of Class III devices receive 510(k) treatment, while the remaining Class III devices undergo PMA review.[146] The MDAA originally envisioned that all new medical devices would undergo PMA review. However, because PMA review is so lengthy and expensive, manufacturers attempt to demonstrate that new Class III devices are "substantially equivalent" to devices that were on the market in 1976 and thus subject to only 510(k) review. The FDA clears 99% of devices subject to premarket approval or notification under the 510(k) process and only 1% under the PMA process.[147] The 510(k) premarket notification process is therefore the primary process through which medical devices with wireless or network capabilities reach the

140. Adam Lewin, *Medical Device Innovation in America: Tensions Between Food and Drug Law and Patent Law*, 26 HARV. J. LAW & TECH. 403, 408-09 (2012), *available at* http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech403.pdf.

141. *Premarket Notification (510k)*, FDA, http://www.fda.gov/medicaldevices/deviceregulationandguidance/howtomarketyourdevice/premarketsubmissions/premarketnotification510k/default.htm (last visited Feb. 9, 2014).

142. *Id.*; *see* Lewin, *supra* note 140, at 409.

143. Lewin, *supra* note 140, at 409.

144. Brian Dolan, *Understanding FDA's New MDDS Rule*, MOBIHEALTHNEWS (Feb. 15, 2011), http://mobihealthnews.com/10234/understanding-fdas-new-mdds-rule.

145. *See Overview of Medical Devices and Their Regulatory Pathways*, FDA, http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHTransparency/ucm203018.htm (last visited Feb. 9, 2014).

146. Lewin, *supra* note 140, at 409.

147. *Id.*

market.

Despite the extensive testing that goes into the PMA process, prior to 2013, the "FDA ha[d] not begun to consider risks resulting from intentional threats,"[148] such as cyberattacks. While manufacturers of Class II and Class III devices had to conduct "software validation and risk analysis" in order to receive FDA approval,[149] the FDA did not require analysis of vulnerability to cyberattacks. A U.S. Government Accountability Office (GAO) analysis of the 2001 and 2006 PMA supplements for two medical devices with known security risks noted that the "FDA did not demonstrate that it had considered the potential benefits of mitigation strategies to protect devices against information security risks from certain unintentional or intentional threats in light of the appropriate level of acceptable risk for medical devices with known vulnerabilities."[150] In the 2012 PMA for a defibrillator, the FDA did consider information security threats. However, it only considered unintentional threats.[151] Additionally, the FDA did not engage in extensive testing of devices against specific threats, such as "testing of attempts to enter incorrect or invalid data in the device or the use of fuzzing, an information security-related testing technique that uses random data to discover software errors and security flaws."[152]

Following the GAO report, the FDA released draft guidance on medical device and hospital network cybersecurity in June 2013.[153] Although the guidance applies to both PMA and 510(k) submissions,[154] it is not binding.[155] At five pages in length, the guidance document lays out basic principles rather than specific recommendations. Echoing HIPAA, the document states that "[m]anufacturers should develop a set of security controls to assure medical device cybersecurity to maintain information confidentiality, integrity, and availability."[156] The document advises manufacturers to

148. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 25.

149. 21 C.F.R. § 820.30(g) (West 2014), *available at* http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?fr=820.30.

150. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 24-25.

151. *Id*. at 25.

152. *Id*.

153. *See* CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124.

154. *See id*.

155. *See id*. at 2.

156. *Compare id*. at 2, *with* 45 C.F.R. § 164.308(a)(1)(ii)(A) (2013) ("*Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health

"consider cybersecurity during the design phase of the medical device."[157] The document also recommends basic security features, such as user authentication and restriction of updates to authenticated code.[158] Although these recommendations are important because they signal a new focus on cybersecurity by the agency, they provide only a basic overview of cybersecurity considerations.[159]

The draft guidance is not, however, without teeth. FDA regulations already require manufacturers to conduct a "risk analysis" of medical device software to obtain FDA approval. The draft guidance expands the meaning of "risk" to include both unintentional and intentional security threats: "Manufacturers should define and document . . . their cybersecurity risk analysis and management plan as part of the risk analysis required by 21 CFR 820.30(g)."[160] This statement suggests that the FDA may exercise its authority under existing regulations to reject devices that are vulnerable to intentional cyberattacks even before the agency promulgates new rules addressing intentional security threats.

The FDA has refused to accept a 510(k) application for review because the application failed to address the new draft guidance.[161] Although at least one commentator has suggested that it was unlawful for the FDA to act on the basis of draft guidance,[162] the FDA has a strong argument that the phrase "risk analysis" is broad enough to include analysis of both intentional and unintentional threats. Under this view, the "draft" guidance is in part a statement of how the FDA will interpret existing regulations rather than merely a set of recommendations for manufacturers. Device manufacturers will likely take the draft guidance seriously going forward, although the FDA may face an administrative law challenge to its authority to regulate under this guidance.

---

information . . . ."), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec164-308.pdf.

157. *See* CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124, at 3.

158. *See id.* at 4.

159. *See* Erik Vollebregt, *FDA's Draft Guidance on Cybersecurity: Nothing Exciting but Useful Examples*, MEDICALDEVICESLEGAL (June 17, 2013), http://medicaldeviceslegal.com/2013/06/17/fdas-draft-guidance-on-cybersecurity-nothing-exciting-but-useful-examples.

160. *Id.*

161. *See* Allyson B. Mullen, *Premature Enforcement of CDRH's Draft Cybersecurity Guidance*, FDA LAW BLOG (Sept. 12, 2013), http://www.fdalawblog.net/fda_law_blog_hyman_phelps/2013/09/premature-enforcement-of-cdrhs-draft-cybersecurity-guidance.html.

162. *See id.*

The FDA's refusal to accept a 510(k) application that does not comply with its draft guidance on cybersecurity demonstrates the need to recalibrate the device classification and approval process to better address cybersecurity concerns. Most new devices are cleared through the 510(k) process. The 510(k) process, however, is primarily concerned with demonstrating the substantial equivalence of a new device to an existing device—not with the inherent safety or effectiveness of the new device.[163] The 510(k) pathway appears especially ill-suited to evaluating medical devices with network capabilities. A medical device that was safe in 1976 may no longer be safe once it has the capability to connect to a hospital network or broadcast a wireless signal.

The FDA has addressed weaknesses in the 510(k) approval process through policy and guidance documents. One commentator notes that "as FDA issues more and more policies and guidance documents, the standard for 510(k) clearance seems to move further from being equivalent to a device currently on the market to meeting FDA's new heightened standards. . . ."[164] From a cybersecurity perspective, draft guidance from the FDA is better than no guidance. From an administrative law perspective, however, the FDA may be vulnerable to legal challenges if it tries to aggressively enforce its guidance documents. To stay within the bounds of its regulatory authority, the FDA may be forced to issue less aggressive guidance and policy documents and hope industry will comply.[165] This may prevent the FDA from taking a strong stance on cybersecurity.[166] It may also create uncertainty for medical device manufacturers.[167] Many commentators have suggested that the 510(k) process is

163. *See* INSTITUTE OF MEDICINE, MEDICAL DEVICES AND THE PUBLIC'S HEALTH: THE FDA 510(K) CLEARANCE PROCESS AT 35 YEARS 2 (2011), *available at* http://www.iom.edu/~/media/Files/Report%20Files/2011/Medical-Devices-and-the-Publics-Health-The-FDA-510k-Clearance-Process-at-35-Years/510k%20Clearance%20Process%202011%20Report%20Brief.pdf ("When the FDA assesses the substantial equivalence of a device, it generally does not require evidence of safety or effectiveness; and when a device is found to be substantially equivalent to a predicate device, the new device is assumed to be as safe and effective as the predicate because of its similarity.").

164. *See* Mullen, *supra* note 161.

165. *See generally* K.M. Lewis, *Informal Guidance and the FDA*, 66 FOOD & DRUG L.J. 507, 538 (2011) ("FDA currently produces roughly twice as many guidance documents per year as legislative rules, and statistics suggest its annual output of guidance has increased regularly.").

166. *See id*. ("[T]o the extent FDA relies on guidance as its primary mode of policymaking, it may find it increasingly difficult to win victories in court.").

167. *See id.* ("The Supreme Court has offered little further guidance regarding the level of deference that informal FDA documents warrant.").

flawed,[168] and the poor fit between the 510(k) process and cybersecurity concerns is one more reason for Congress to revisit the medical device approval process.

b. Post-Market Review

The FDA uses three primary methods of post-market regulation of medical devices: adverse event reporting, postapproval studies, and postapproval reports. The FDA uses the Manufacturer and User Facility Device Experience Database (MAUDE) to monitor adverse events involving medical devices once they are on the market.[169] As part of the PMA or 510(k) process, the FDA may require medical device manufacturers to conduct postapproval studies "to identify potential problems."[170] The FDA also requires medical device manufacturers to prepare annual postapproval reports.[171] As the GAO report revealed, the FDA could use post-market regulation more effectively to protect against information security threats.

MAUDE could help identify cybersecurity issues that impact patient care. The FDA uses codes to categorize different types of adverse events, and "although FDA does not categorize its codes as specifically related to information security problems, it has codes in place that could potentially identify information security problems resulting from . . . intentional threats."[172] Adverse events may include problems such as "(1) an application issue, (2) the unauthorized access to a computer system, or (3) a computer-security issue."[173] The Veteran's Administration (VA) Office of Information Security manages a robust reporting system for malware infections.[174] In its database, the VA identified over 142 incidents involving 207 devices between January 2009 and December 2011.[175] The FDA could

168. *See, e.g.*, INSTITUTE OF MEDICINE, *supra* note 163, at 3 ("[T]he FDA's finite resources would be better invested in developing an integrated premarket and postmarket regulatory framework that provides a reasonable assurance of safety and effectiveness throughout the device life cycle.").

169. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 9-10; *see* 21 C.F.R. pt. 803 (West 2014).

170. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 10; *see* 21 C.F.R. pt. 803 (West 2014). For devices cleared through the 510(k) process, postapproval studies are called "522 studies." U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 10 n.18.

171. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 30-31.

172. *Id.* at 29-30.

173. *Id.* at 29.

174. *See FDA Preparing for the Hacking of Medical Devices*, ORTHOSTREAMS (Aug. 27, 2013), http://orthostreams.com/2013/08/fda-preparing-for-the-hacking-of-medical-devices.

175. *See id.*

similarly use MAUDE to help flag cybersecurity flaws that lead to adverse events. Given the FDA's recent focus on cybersecurity issues, the agency may be moving in this direction. Better software is likely needed. As one researcher warns, in the MAUDE database "real problems may be obscured by hundreds, if not thousands, of unhelpful reports that are all lumped together."[176]

To complement its adverse event reporting system, the FDA could also require manufacturers to conduct postapproval studies of their devices. According to the 2012 GAO report, "FDA officials said that, while they could require manufacturers to conduct postmarket studies to focus on information security risks, they did not currently have plans to request that any manufacturers do so."[177] The 2013 FDA draft guidance on cybersecurity recommends that manufacturers submit a "systematic plan for providing validated updates and patches to operating systems or medical device software, as needed, to provide up-to-date protection and to address the product life-cycle."[178] Because the FDA has already requested that manufacturers create a plan to keep their devices up-to-date, the FDA could take this request one step further by requiring manufacturers to conduct postmarket studies of device cybersecurity and report their findings to the FDA. While it may be too costly to require all manufacturers to conduct such studies, requiring postapproval studies of high-risk devices could help ensure that manufacturers abide by the cybersecurity plans submitted during the approval process.

The FDA could also require manufacturer postapproval reports to include an analysis of cybersecurity concerns. Postapproval reports must include information about any changes the manufacturer made to the device during the preceding year, including software changes.[179] The reports must also detail any defects in the device identified in scientific literature.[180] The GAO report revealed, however, that these reports may not be comprehensive. GAO examined the annual postapproval reports of a defibrillator that researchers hacked in a 2008 study. The postapproval reports did not mention the study, even though it was published in scientific literature and demonstrated a significant security flaw in the device.[181]

176. *Id.* (describing presentation by Jay Radcliffe).
177. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 30.
178. CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124, at 4.
179. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15, at 30-31.
180. *Id.* at 31.
181. *Id.*

Similarly, the postapproval report of an insulin pump hacked by researchers in 2010 did not include any reference to information security issues.[182] The FDA could take a more active role in auditing these reports for accuracy and in emphasizing that these reports must include cybersecurity risks.

In addition to more comprehensive adverse event reporting, postapproval studies, and postapproval reports, the FDA should also consider more proactive approaches to identifying new cyberattack risks. The type of risk posed by an intentional cyberattack is different from the type of risk posed by software or hardware flaws that unintentionally cause injury. Intentional threats constantly evolve. A device that is safe when first put on the market may develop a security flaw as hackers develop new techniques or discover new software vulnerabilities. Instead of monitoring adverse events and manufacturer reports, the FDA should work with manufacturers to proactively identify software flaws before cyberattacks occur. Part IV describes some of the elements of a proactive and flexible regulatory approach to protecting against cyberattacks.

2. FDA Regulation of Mobile Medical Applications

Following the proliferation of medical devices with software components and the dramatic increase in health-related mobile applications (apps), the FDA has begun to regulate these devices and apps. The FDA has no "overarching software policy."[183] The text of the FDCA is broad, defining a medical device to include any "instrument," "apparatus," or "contrivance," and "any component, part, or accessory" that is used to diagnose or treat disease.[184] The FDA has reduced confusion over whom and what it will regulate by releasing its September 2013 final guidance on MMAs[185] and its Final Rule on MDDSs.[186] However, neither the MMA guidance nor the MDDS rule mentions cybersecurity concerns. The FDA may need to

182. *Id.*

183. FDA, DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF – MOBILE MEDICAL APPLICATIONS (2011) [hereinafter DRAFT GUIDANCE], *available at* http://www.genomicslawreport.com/wp-content/uploads/2013/03/FDA-mHealth-Draft-Guidance.pdf.

184. 21 U.S.C. § 321(h) (2010).

185. FDA, MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2013), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

186. *See infra* Part II.D.3.

revisit its MMA classification scheme to ensure that its regulation of MMAs takes into account the risk of cyberattacks.

The FDA defines MMAs broadly. An MMA is a device "used as an accessory to a regulated medical device; or to transform a mobile platform into a regulated medical device."[187] MMAs include apps that perform the following functions: (1) "[d]isplaying, storing, analyzing, or transmitting patient-specific medical device data" as an extension of a medical device; (2) "[t]ransform[ing] a mobile platform into a regulated medical device" by using "attachments, display screens, [or] sensors;" or (3) "performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations."[188] The FDA looks to an app's "intended use" to determine whether it is a regulated device, including its "labeling claims, advertising materials, or oral or written statements by manufacturers or their representatives."[189] If the app is used to diagnose or treat disease, the app is a "device." Almost any mobile app that is useful to doctors in a medical setting will constitute an MMA. According to FDA guidance, an app that controls a cell phone light becomes a regulated medical device if the manufacturer markets the app as a tool for examining patients.[190]

The FDA regulates MMAs based on the classification of the device associated with the MMA or whose function the MMA replaces. "[M]anufacturers must meet the requirements associated with the applicable device classification."[191] For example, "a mobile app that displays radiological images for diagnosis transforms the mobile platform into a class II" device.[192] An MMA manufacturer includes not only the company that creates the app software but also "anyone who initiates specifications, designs, [or] labels" the app.[193] For example, a hospital is a device manufacturer if it hires a software firm to design an MMA. This definition of "manufacturer" imposes FDA oversight on hospitals, which also face HHS regulation of information security under HIPAA. MMA distributors, such as iTunes, do not constitute MMA manufacturers.[194]

---

187. FDA, *supra* note 185, at 12.
188. *Id.* at 14-15.
189. *Id.* at 8.
190. *Id.*
191. *Id.* at 13.
192. *Id.* at 15.
193. FDA, *supra* note 185, at 9.
194. *Id.* at 11.

The FDA guidance on MMAs raises a number of important questions about medical device and hospital network cybersecurity. By expanding the definition of "device" to cover most medical-related mobile applications, the FDA opens the door to significant regulation of MMAs. As the FDA begins to regulate more comprehensively against cyberattacks, the FDA will be able to regulate the security features of wireless and networked devices in addition to mobile devices and even the software running mobile devices. Because all of these devices work together, it makes sense to develop an overarching regulatory approach to cybersecurity.

A device's classification determines how much regulatory oversight it receives. As a result, the classification of an MMA will determine how closely the FDA scrutinizes the app's information security features. One potential issue is that a medical device may be a Class I device—and thus subject to little or no regulation—which could mean that an MMA associated with the device similarly receives little or no scrutiny. While the MMA may not pose a health risk to the patient, it may nevertheless constitute a cybersecurity threat. MDDSs, for example, are Class I devices yet may still be vulnerable to cyberattack.[195] Similarly, Class II and a Class III MMAs may pose exactly the same cybersecurity risk—and even run on exactly the same software—but may receive different scrutiny under the 510(k) and PMA approval processes. While the FDA's draft guidance on cybersecurity may help alleviate this inconsistency, the FDA likely needs to develop a new classification scheme for cybersecurity threats.

3. FDA Regulation of Medical Device Data Systems

In addition to its guidance on MMAs, the FDA has issued a final rule governing MDDSs. These systems are "passive databases and communications software products"[196] that store information but do not actively interact with medical devices or provide decision support.[197] An example of an MDDS is software that stores blood pressure readings.[198]

Because of the lower risks associated with MDDSs, the FDA

195. *See infra* Part II.D.3.

196. Dolan, *supra* note 144.

197. *Id.*

198. *Medical Device Data Systems*, FDA, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/MedicalDeviceDataSystems/default.htm (last updated Apr. 19, 2011).

issued a final rule in 2011 that declassified MDDSs from Class III to Class I medical devices. This rule makes MDDSs "exempt from premarket review but still subject to quality standards."[199] The FDA's rationale for this rule is that quality controls are sufficient to ensure the safety and effectiveness of MDDSs.[200]

Although the final MDDS rule downgraded MDDSs to Class I devices, it also expanded FDA regulatory authority to include some types of previously unregulated software.[201] For example, the MDDS classification now includes "hospital-derived software" with an intended use in the medical field and "hardware, such as modems, that are expressly promoted as part of the system."[202] The FDA's exertion of broader regulatory power over medical software makes sense in part because this software could pose an information security risk to medical devices or hospital networks, although it is not clear that the FDA's decision to broaden its regulatory power was motivated by these concerns.

One potential danger in downgrading MDDSs to Class I devices is that they will receive little regulatory oversight beyond the specification of general controls. This is problematic if an MDDS contains a security flaw that permits a malicious actor to hack an entire hospital network. Because MDDSs are databases that store information, they are targets for cyberattacks seeking PHI for medical identity theft. MDDSs are also likely to be hooked up to hospital networks so that physicians can remotely access the information contained in the MDDS. A security flaw in an MDDS may allow a malicious actor or malware to infiltrate a hospital network. It makes little sense to impose the draft cybersecurity guidance on Class II and Class III medical devices[203] but not on Class I MDDSs. Accordingly, the FDA should reconsider its classification system when evaluating the cybersecurity risk posed by MDDSs that are connected to medical networks.

4. Food and Drug Administration Safety and Innovation Act

The FDASIA of 2012 established a new pathway for classifying medical devices. The FDASIA states that "[i]n lieu of submitting a

199. *Id.*

200. *Id.*

201. *See* Dolan, *supra* note 144.

202. *Id.*

203. CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124, at 2.

report under section [510](k) . . . if a person determines there is no legally marketed device upon which to base a determination of substantial equivalence . . . a person may submit a request under this clause for the Secretary to classify the device."[204] The FDASIA responds in part to criticism of the "substantial equivalence" framework of the 510(k) process. The FDA has not yet released guidance on how it will implement the FDASIA, so it is difficult to know how this law will change the regulatory process for medical devices. The FDASIA permits the FDA to rethink its medical device classification scheme, providing the FDA with an opportunity to adopt a regulatory structure that better addresses the risk of cyberattacks.

E. Tort Liability

Injured patients may have a civil cause of action against malicious actors, hospitals, or medical device manufacturers following a cyberattack against a medical device or hospital network. On one hand, it seems unlikely that a court would find a legal barrier to a civil suit against a malicious actor who conducts a cyberattack and physically harms a person. On the other hand, cyberattacks do not comfortably fit within the traditional framework of battery and trespass to chattels actions. Until a body of case law develops, it is unclear how these actions will play out in court. A patient injured by a cyberattack may also have a cause of action against medical device manufacturers and hospitals for negligence. The success of the suit will likely depend on how the court treats the superseding cause doctrine and on how the court views the defendant's standard of care. It is likely that state courts will ultimately develop doctrines that impose liability on medical device manufacturers and hospitals that negligently fail to take precautions against cyberattacks. Without more certainty, however, the threat of civil liability may not provide a sufficient incentive for medical device manufacturers and hospitals to adopt cybersecurity measures.

1. Malicious Actors

Plaintiffs harmed in a cyberattack may bring suit against the cyberattacker under tort theories including battery and trespass to

204. 21 U.S.C. § 360c(f)(2)(A)(ii) (2012), *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2012-title21/pdf/USCODE-2012-title21-chap9-subchapV-partA-sec360c.pdf.

chattels.[205] A battery theory is likely to succeed, although courts have yet to grapple with potentially thorny issues such as whether a cyberattack satisfies the "intent" and "offensive touching" elements of battery. Trespass to chattels, which is the intentional interference with personal property leading to injury, is another potential cause of action. Courts will likely need to reinterpret elements of both torts to address the issues raised by digital attacks that cause physical harm to patients.

a. Battery

Battery requires an intentional "offensive touching of the plaintiff's person, or something so closely associated with the plaintiff as to make the touching tantamount to a physical invasion of the plaintiff's person."[206] Courts are split on whether:

> [T]he Second Restatement's definition of intent is properly interpreted to require both intent to make bodily contact and, in addition, intent to harm or offend (dual intent), or whether it is sufficient that the defendant intends to make a bodily contact that turns out to be harmful or offensive (single intent).[207]

Plaintiffs may have difficulty proving the "intent" element of battery in some cyberattack cases. A malicious actor who intentionally conducts a cyberattack against a medical device likely meets the "intent" prong. A programmer who writes malware that happens to infect a medical device and harm a patient, however, may not have "intent" to commit battery. First, the programmer may not have intended the code to have any effect on physical reality, undermining the argument that the programmer intended a "touching of the plaintiff's person." Second, the programmer may not have intended harm. For example, the programmer may only have intended to steal a patient's medical identity, not cause physical injury. In cases where the plaintiff can only show intent to touch the plaintiff's person and not intent to cause harm, the definition of intent adopted by the court will likely govern the outcome of the case.

Satisfying the element of "offensive touching" may also be difficult. The success of the action may depend on how closely

---

205. Some commentators have suggested that a plaintiff may also have a nuisance claim against a cyberattacker. *See, e.g.*, Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53-54 (2000).

206. Neal Hoffman, *Battery 2.0: Upgrading Offensive Contact Battery to the Digital Age*, 1 CASE W. RES. J.L. TECH. & INTERNET 61, 68 (2010).

207. *See* Kerr, *supra* note 80, at 1597.

associated a medical device is with the plaintiff's body. The comments to the Second Restatement of Torts note that:

> Since the essence of the plaintiff's grievance consists in the offense to the dignity involved in the unpermitted and intentional invasion of the inviolability of his person and not in any physical harm done to his body, it is not necessary that the plaintiff's actual body be disturbed. Unpermitted and intentional contacts with anything so connected with the body as to be customarily regarded as part of the other person and therefore as partaking of its inviolability is actionable as an offensive contact with her person.[208]

There is a strong argument that at least some medical devices, such as pacemakers and insulin pumps, are "closely associated with the plaintiff." Other medical devices, however, may not be as closely integrated with the plaintiff's physical body. A heart rate monitor, for example, may play an important role in monitoring a patient's health. A cyberattack against a hospital network that shuts down the heart rate monitor, or that prevents the physician from accessing the heart rate monitor from a mobile device, may have no physical effect on the patient. However, without the ability to monitor the patient, the physician may not catch the warning signs of a heart attack. While it seems likely that a court would stretch the element of "offensive touching" to apply in this type of situation, it is also possible that some courts may decline to find this element of battery satisfied. Courts may also struggle with defining "touching" to include digital touching, although courts may overcome this hurdle by defining "touching" broadly or by focusing on the physical movement of electrons. While it seems likely that a court would hold a defendant liable for intentionally harming a patient through a cyberattack, courts may need to reinterpret traditional tort principles to address the issues raised by digital attacks that cause physical harm.

b. Trespass to Chattels

Trespass to chattels is a tort that some courts have applied in the context of unauthorized use of computer systems. "Trespass to chattels lies where an intentional interference with the possession of personal property has proximately cause[d] injury."[209] To establish a claim, the plaintiff must show that "(1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use

208. RESTATEMENT (SECOND) OF TORTS § 18 cmt. c (1965).

209. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069 (N.D. Cal. 2000).

proximately resulted in damage to the plaintiff."[210] In *eBay, Inc. v. Bidder's Edge, Inc.*, eBay alleged that another company's unauthorized access to its website had increased the load on its system, resulting in monetary damages.[211] The court found for eBay, holding that eBay had demonstrated a likelihood of success on the merits for a trespass to chattels claim because the defendant company had repeatedly accessed information on eBay's website without permission.[212]

When a malicious actor accesses a medical device or hospital network without permission, downloading data or interfering with the device, the owner of the medical device or network may have a claim for trespass to chattels if the court follows the reasoning of the *eBay* decision. The patient relying on the medical device or hospital network, however, may not have a claim under this tort theory unless she has a possessory interest in the device or network. The trespass to chattels doctrine may therefore allow a hospital to sue a malicious actor who attacks its network or device, but it may not provide a cause of action for an injured patient. Trespass to chattels is ultimately an old doctrine with uncertain application in the digital era. While some courts may allow a trespass to chattels claim, others may not. The legal uncertainty around the application of battery and trespass to chattels theories may reduce the deterrence effect of tort law on the malicious actors behind cyberattacks.

2. Medical Device Manufacturers and Hospitals

A hospital or medical device manufacturer may be negligent if it fails to adopt reasonable cybersecurity measures. It may be difficult, however, to define the duty of care in the context of cyberattacks. Experts have only recently identified cyberattacks as a realistic threat. Furthermore, cybersecurity standards will continue to evolve, making the identification of a standard of care difficult. In some states, the superseding cause doctrine blocks negligence liability where a malicious actor is the direct cause of a plaintiff's injuries. Additionally, *Riegel v. Medtronic* dictates that once the FDA clears a medical device through the PMA process, plaintiffs cannot sue the device manufacturer in tort under most circumstances.[213] Given these difficulties, the success of a negligence action against a medical

210. *Id.* at 1069-70.

211. *See id.* at 1061-63.

212. *See id.*

213. Riegel v. Medtronic, 552 U.S. 312 (2008).

device manufacturer or hospital is uncertain.

a. Duty of Care

At common law, a hospital or medical device manufacturer is negligent if it breaches a duty of care towards an injured individual. The duty of care to ensure that networks and devices are secure from outside intrusion is unclear. It is likely that a court would look to HIPAA standards to help define at least the lower limit of a hospital's duty of care. Other standards, such as those promulgated by the National Institute of Standards and Technology[214] or the International Organization for Standardization,[215] may also serve as a benchmark for the duty of care. HIPAA standards do not generally apply to medical device manufacturers, however, and thus a court may or may not hold a medical device manufacturer to relevant HIPAA standards. While the recent FDA draft guidance on cybersecurity may provide a benchmark for courts, the guidance is general and non-binding.[216] Until courts regularly grapple with negligence suits following cyberattacks, the duty of care is likely to remain uncertain.

The duty of care is also complicated by the fact that information security measures may detract from patient care. Installing encryption or security programs on implantable medical devices may require larger batteries, which in turn could require either larger devices—potentially decreasing the safety and efficacy of the medical device—or devices with a significantly shorter battery life. Battery life is especially important for implantable medical devices like pacemakers. A court may hesitate to impose such a duty of care on a medical device manufacturer. Network security features, such as complicated login systems, may make it more difficult for doctors to access patient information in emergency situations. Mobile device security requirements may also make it more difficult for doctors to check on patients remotely. The FDA's draft guidance on cybersecurity recognizes the tension between security and patient care.[217] These arguments could sway courts in at least some cases to

214. *See Computer Security Division*, NAT'L INST. OF STANDARDS & TECH., http://www.nist.gov/itl/csd/index.cfm (last updated Jan. 18, 2013).

215. *See* INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, http://www.iso.org/iso/home.htm (last visited Feb. 9, 2014).

216. *See* CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124.

217. *See* CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124, at 3 ("Manufacturers should also carefully consider the balance between cybersecurity safeguards and the usability of the device in its intended environment . . . . For example, security controls should not hinder access to the device during an emergency situation.").

find no duty of care to adopt certain security measures.

The class action plaintiffs' complaint in a data breach case against TJX Companies outlines some of the arguments a plaintiff might bring in a negligence case against a medical device manufacturer or hospital following a cyberattack. After a hacker stole the credit card information of thousands of TJX customers, affected customers brought a complaint alleging that TJX had a "special fiduciary relationship" with its customers because it stored customers' personal and financial information and that this relationship created a "duty of care to use reasonable means to keep nonpublic information of the Class private and secure."[218] Plaintiffs alleged that TJX was negligent because it failed to comply with industry standards and because the data breach was extremely large and took place over a 14-month period.[219] In a cyberattack case, plaintiffs might similarly argue that a medical device manufacturer, and especially a hospital, has a fiduciary relationship with its patients, creating a duty of care to protect against cyberattacks.[220] The level of compliance with industry standards and the magnitude of the attack may also factor into the duty of care.

Critics have noted that HIPAA standards do not go far enough in requiring security measures for mobile devices. For example, HIPAA does not require "the ability to remotely wipe sensitive patient data" on mobile devices.[221] If a hospital or medical device manufacturer meets HIPAA standards but does not go beyond them, a court may find that it has satisfied the duty of care—even if the HIPAA

---

218. Complaint at 38, *In re* TJX Companies Retail Security Breach Litigation, No. 07-10162-WGY (D. Mass. Dec. 20, 2007), *available at* http://sp09tcs401601pbj.pbworks.com/f/class+action+lawsuit.pdf.

219. *Id.*

220. The fiduciary duties of hospitals towards patients is unclear, but "[s]ome American courts have begun to assume a fiduciary obligation in the hospital setting." Barry R. Furrow, *Patient Safety and the Fiduciary Hospital: Sharpening Judicial Remedies*, 440 DREXEL L. REV. 439, 461 (2009), *available at* http://www.earlemacklaw.drexel.edu/~/media/Files/law/law%20review/furrow.ashx. In *Washington v. Washington Hosp. Ctr.*, for example, the D.C. Court of Appeals affirmed a lower court's finding that Washington Hospital was negligent for failing to adopt the latest carbon dioxide monitoring technology. *Washington v. Washington Hosp. Ctr.*, 579 A.2d 177, 183 (D.C. Cir. 1990). It is possible that a court would similarly find that a hospital was negligent for failing to adopt the latest cybersecurity standards, especially where other similar hospitals have done so.

221. Greg Slabodkin, *New HIPAA Rule Falls Short in Protecting Mobile Patient Information*, FIERCE MOBILE HEALTHCARE (Jan. 20, 2013), http://www.fiercemobilehealthcare.com/story/new-hipaa-rule-needed-expand-its-reach-protecting-mobile-patient-informatio/2013-01-20.

standards do not adequately protect medical device or hospital network information security. The fact that HIPAA does not apply to most medical device manufacturers, and that HIPAA addresses threats to protected health information rather than all types of cyberattacks, makes it difficult in many cases for courts to use HIPAA to determine the duty of care. While the FDA draft cybersecurity guidelines are applicable to medical device manufacturers, they are not applicable to hospital networks. These guidelines are also general and non-binding. Without a clear duty of care, a court may hesitate to impose liability for negligence. Given these potential obstacles to tort liability, Part IV outlines three potential approaches to addressing the threat of cyberattacks on medical devices and hospital networks.

b. Superseding Cause

Hospitals and medical device manufacturers may also avoid tort liability if a court finds that the malicious actor behind a cyberattack is the "superseding cause" of the attack. "A 'superseding cause' is an intervening act that operates to relieve the original actor of liability for the ultimate harm even though the original actor was a factual cause of that harm."[222] Courts generally adopt one of two approaches to superseding cause.[223] Under the first approach, the court will find a superseding cause only if the intervening act is unforeseeable. Foreseeability is a matter of fact for the jury to decide.[224] Under the second approach, adopted by the Third Restatement of Torts, the court focuses on proximate cause rather than the foreseeability of the intervening act.[225] The Third Restatement "focuses the inquiry on whether the type of harm suffered by the injured party was within the scope of the risk presented by the original actor's tortious conduct."[226] This proximate cause analysis looks at whether the "ultimate harm" is

222. Jim Gash, *At the Intersection of Proximate Cause and Terrorism: A Contextual Analysis of the (Proposed) Restatement Third of Torts' Approach to Intervening and Superseding Causes*, 91 KY. L.J. 523, 581 (2003).

223. *Id.*

224. *See, e.g.*, Duphily v. Delaware Elec. Co-op., Inc., 662 A.2d 821, 830-31 (Del. 1995) ("[A]n intervening negligent act will not relieve the original tortfeasor from liability if: the original tortfeasor at the time of his negligence *should have realized* (foreseen) that another's negligence might cause harm; or, if a *reasonable person* would not consider the occurrence of the intervening act as *highly extraordinary;* or, if the intervening act was not *extraordinarily negligent*.").

225. Jim Gash, *supra* note 222, at 595.

226. *Id.*

foreseeable, not whether the intervening act is foreseeable.[227]

These two different formulations of the superseding cause doctrine can lead to different outcomes. The first approach asks whether it is foreseeable that a malicious actor would conduct a cyberattack on a medical device or hospital network. Because there have been no reported cases of patient harm caused by cyberattacks on medical devices or networks, there is an argument that these attacks are not foreseeable. However, the GAO report and researcher experiments demonstrating that medical devices can be hacked provide a good argument that hospitals and medical device manufacturers should foresee cyberattacks.[228] Malware attacks on devices and hospital networks are much more common and thus are more foreseeable. The specific type of attack, however, may not be foreseeable. It is therefore difficult to know how a court would rule on the issue of foreseeability.

The second approach asks whether it is foreseeable that negligence by medical device manufacturers or hospitals would lead to harm from cyberattacks. This too is an open question. According to Professors Kesan and Hayes, "[b]ecause the connection between cybersecurity measures and cyberattacks is self-evident, and lax cybersecurity could foreseeably lead to negative consequences from cyberattacks, a court following the [second approach] would likely find that the causal relationship is preserved, and would thus be likely to conclude that proximate cause still exists."[229] However, there is also an argument that no matter how good the information security measures, a creative actor may find a way to breach them. The foreseeability issue may in part depend on the creativity of the attack. Again, it is difficult to know how courts will rule on the issue of foreseeability under the second approach, adding one more level of uncertainty to a negligence claim against hospitals and medical device manufacturers.

c. Riegel v. Medtronic

Under *Riegel v. Medtronic*,[230] manufacturers of medical devices cleared through the lengthy and expensive PMA process are generally

227. *Id.*

228. *See supra* Part I.A; *see also infra* Part II.D.

229. Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 487 (2012), *available at* http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech429.pdf.

230. 552 U.S. 312 (2008).

not subject to state tort suits.[231] In *Riegel*, the Supreme Court "held that because the FDA imposes rigorous design, manufacturing, and labeling requirements on Class III devices, tort claims that would impose requirements different from or additional to the FDA's requirements are preempted."[232] State tort law that is "'parallel'" to FDA requirements is not preempted.[233] Tort suits against the manufacturers of devices that have been approved under the 510(k) process, including many Class III devices cleared under 510(k), are also not preempted.[234] Because most wireless devices, such as insulin pumps, are Class II devices, the majority of tort suits are not preempted. However, some important medical devices—such as cardiac defibrillators—are Class III devices cleared under the PMA process.

Class III devices are "life-supporting or life-sustaining, or for a use which is of substantial importance in preventing impairment of human health, or if the device presents a potential unreasonable risk of illness or injury."[235] For this reason, malicious actors may target PMA-cleared Class III devices for cyberattacks. Because *Riegel* as a policy measure places its trust in the FDA to ensure the safety of PMA-cleared devices, it is especially important for the FDA to regulate the information security features of these PMA-cleared devices. While the FDA has released draft guidance on cybersecurity, this guidance is not mandatory. Part IV discusses potential reforms that could give the FDA a greater role in medical device cybersecurity.

III. GAPS IN THE LEGAL FRAMEWORK

Three different legal structures govern cyberattacks against medical devices and hospital networks. Criminal law focuses primarily on deterring the malicious actors behind cyberattacks. Federal regulatory regimes such as the FDCA and HIPAA provide a framework for regulating medical device manufacturers and healthcare providers. Common law principles may impose liability

231. *See id.*

232. *See* Elliot Sheppard Tarloff, *Medical Devices and Preemption: A Defense of Parallel Claims Based on Violations of Non-Device Specific FDA Regulations*, 86 N.Y.U. L. REV. 1196, 1196 (2011).

233. *Riegel*, 552 U.S. at 330.

234. *See* Medtronic, Inc. v. Lohr, 518 U.S. 470 (1996).

235. 21 C.F.R. § 860.3 (2012), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2012-title21-vol8/pdf/CFR-2012-title21-vol8-sec860-3.pdf.

on medical device manufacturers and healthcare providers that negligently fail to protect against cyberattacks. As described in this Part, however, these legal structures do not fully address the threat of cyberattacks. As long as it remains difficult to identify and prosecute the actors behind cyberattacks, criminal law is an insufficient deterrent. FDCA and HIPAA were not designed to protect against cyberattacks against medical devices and do not provide sufficient regulatory safeguards in this area. The scope of negligence liability for medical device manufacturers and healthcare providers is untested and unclear. New approaches are needed to address the threat of cyberattacks.

A. Difficulty of Effective Prosecution of Malicious Actors Behind Cyberattacks

The malicious actors behind cyberattacks face criminal liability under several federal statutes in addition to common law civil liability and possible state criminal liability. However, the difficulty of identifying and prosecuting cyberattackers greatly undercuts the deterrence power of these laws.[236]

As many commentators have noted, it is often difficult or impossible to identify the actor behind a cyberattack.[237] "In cyberspace, attackers can hide their identity, cover their tracks. Worse, they may be able to mislead, placing blame on others by spoofing the source."[238] For example, the malicious actor behind a 2009 DDoS attack against U.S. and South Korean government and business websites remains unknown.[239] Because the attack was

236. Some academic literature questions whether our current legal regime ever achieves deterrence. *See, e.g.*, Raymond Paternoster, *How Much Do We Really Know About Criminal Deterrence?*, 100 J. CRIM. L. & CRIMINOLOGY 765, 818-23 (2010) ("Criminal deterrence may have its limits precisely because the legal costs are far removed in time and people find it difficult to feel the pain of the longer-term consequences of their actions.").

237. *See, e.g.*, Stephenie Gosnell Handler, *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, 48 STAN. J. INT'L L. 209, 213 (2012) ("[I]t is extremely difficult and sometimes impossible to definitely identify where a cybercrime or cyberattacks originates. And, even if the location is identified, the perpetrator . . . may even remain anonymous."); Kesan & Hayes, *supra* note 229, at 438 ("It is almost impossible to accurately and consistently identify attackers, which severely complicates any steps that might be taken to uncover those responsible and hold them accountable for their actions."). *See generally* Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397-404 (2011) (describing some of the many reasons why it is difficult to identify the actors behind a cyberattack).

238. Richard Clarke, *War from Cyberspace*, NAT'L INT., Nov.-Dec. 2009, *available at* http://nationalinterest.org/article/war-from-cyberspace-3278.

239. Hollis, *supra* note 237, at 397.

relatively unsophisticated, almost anyone could have orchestrated it.[240] Criminal law may attempt to deter crimes where few perpetrators are caught by making the penalties large. While penalties under the CFAA and the Anti-Tampering Act are large—ranging from five to twenty years in prison[241]—even large penalties may fail to deter where identification of the perpetrator is very difficult.[242] In the near term, it is unlikely that it will become any easier to identify the actors behind cyberattacks.[243]

Once identified, it may be difficult to prosecute cyberattackers. Selecting the appropriate venue may be challenging if the attack occurs across state or national lines.[244] For domestic defendants, "the complexity of Internet routing creates jurisdictional conflicts among the localities, states, and countries that wish to exercise jurisdiction over transient information packets."[245] Prosecution of foreign defendants is even more difficult. U.S. criminal statutes like the CFAA likely do not apply extraterritorially.[246] If the cyberattacker resides outside of the United States, she may succeed in dismissing a suit on *forum non conveniens* grounds.[247] While there are international regimes in place to address cyberattacks, foreign governments do not consistently enforce them.[248]

Although criminal liability for cyberattacks under statutes like the CFAA is relatively clear, civil liability is murkier due to unresolved questions about how torts like battery and trespass to chattels apply in cyberspace.[249] Plaintiffs may be unsure which tort theory to choose, and courts may differ on how broadly they interpret

240. *Id.*

241. *See supra* Part II.B.

242. *See* Steven Shavell, *Criminal Law and the Optimal Use of Nonmonetary Sanctions as a Deterrent*, 85 COLUM. L. REV. 1232, 1232 (1985) ("[I]t is emphasized that if the probability is too low, it will not be possible to deter certain parties even with the threat of the highest conceivable sanctions.").

243. *See* Hollis, *supra* note 237, at 402-03.

244. *Id.*

245. Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 873 (1999).

246. *See id.*; Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 874 & n.275 (2012) (noting that "[t]here is generally a presumption against extraterritorial application of federal law" under *United States v. Cotton* and discussing exceptions to this rule).

247. *Id.*

248. *See* Kesan & Hayes, *supra* note 229, at 496 ("Because there is significant uncertainty over how to address cyberattacks under international law, potential attackers are unlikely to be deterred by the threat of criminal charges in other countries . . . .").

249. *See supra* Part II.E.1.

common law principles to accommodate digital acts.[250]

The malicious actors behind cyberattacks may also be relatively judgment proof,[251] decreasing the deterrence effect of tort liability and increasing the risk that cyberattacks will lead to uncompensated harm. The actors behind recent cyberattacks against the Department of Defense have ranged from Chinese military agents to a sixteen-year-old Florida student.[252] Conducting a cyberattack may not require extensive investment[253] but may nevertheless lead to significant physical and monetary harm to patients and healthcare providers.

Together, the difficulty of identifying, prosecuting, and recovering damages from the malicious actors behind cyberattacks counsels against relying solely on criminal and civil penalties against these actors to deter attacks.

B. Poor Fit of Current FDA Device Classification Scheme to Cyberattack Threat

The current medical device classification system does not always reflect the cyberattack risk posed by a particular device. Traditional medical devices fall under one of three classifications, with Class I devices receiving little oversight and Class III devices often undergoing the extremely expensive PMA process.[254] MMAs receive the same classification as the device they are associated with.[255] The FDA regulates MDDSs as Class I medical devices.[256]

In the case of targeted attacks against an individual's wireless medical device, such as a pacemaker or insulin pump, the current classification scheme aligns with the threat posed by a cyberattack. The importance of the device to the patient's health will likely correlate with the potential harm to the patient if a malicious actor manipulates or disables the device.

In the case of cyberattacks against MDDSs or hospital networks, however, the medical device classification may bear little relation to the risk posed by a cyberattack. To the extent that a medical device

250. *See* Kesan & Hayes, *supra* note 229, at 496.

251. *See id.* at 438 ("Cyberattacks are not resource-intensive, which renders them even more dangerous because no practical requirement exists to limit the attackers to being members of organized and well-funded sources such as a nation's military.").

252. Handler, *supra* note 237, at 213-14.

253. *See* Kesan & Hayes, *supra* note 229, at 470.

254. *See supra* Part II.D.1.

255. *See supra* Part II.D.2.

256. *See supra* Part II.D.3.

of any classification is connected to a hospital network, it may be used as an entry point to disrupt the network or steal information from the network. Whether an MMA is a Class II device used as an insulin monitor or a Class I device used to create a meal plan for a diabetic, a flaw in the MMA software could pose a security risk to the entire hospital network. Class I MDDSs may be "passive" repositories of patient data and thus may pose little risk to patient health. However, repositories of patient data are a treasure trove for identity thieves. From an identity theft perspective, a Class III pacemaker containing the identifying information of one patient may be far less valuable than a Class I passive database containing thousands of patient records. The exact same type of device may run on off-the-shelf software that is more vulnerable to cyberattacks or on proprietary software that is less vulnerable to cyberattacks.[257] The current device classification system does not reflect these distinctions. Concerns over the fit of the medical device classification system to the threat posed by cyberattacks support the need for further regulatory reforms, such as those discussed in Part IV.

C. The Role of Medical Device Manufacturers and Large Healthcare Providers in Preventing Cyberattacks

Medical device manufacturers and large healthcare providers play an important role in preventing cyberattacks. The FDA recognizes this, stating in a 2009 "Reminder from the FDA" that "cybersecurity for medical devices and their assembled communication networks is a shared responsibility between medical device manufacturers and medical device user facilities."[258] One striking feature of the current regulatory regime, however, is that it does not harness the ability of industry to adopt cybersecurity measures. According to one commentator, the CFAA "does not provide an incentive for anyone to adopt adequate anti-hacking security measures. In fact, network security remains at a[] shockingly low level and is virtually nonexistent in many companies despite the severity of the hacking threat."[259] While medical device manufacturers may adopt the FDA draft guidance on cybersecurity, this guidance is not mandatory. New legal and regulatory frameworks are needed to ensure that medical device manufacturers and large healthcare providers protect against cyberattacks.

257. *See* ATTACK SURFACE, *supra* note 13, at 2.

258. *See Reminder from FDA*, *supra* note 29.

259. Lee et al., *supra* note 245, at 873 n.147.

IV. SOLUTIONS TO STATUTORY AND REGULATORY GAPS

Because the current statutory and regulatory framework is not adequate to address the threat of cyberattacks on medical devices and hospital networks, new approaches are needed. One potential approach is industry self-regulation. A second approach is to equip the FDA with expanded authority and resources to identify and address security risks before cyberattacks occur. This would likely require a new focus by the agency, which has previously relied on a backward-looking analysis of adverse events rather than a forward-looking analysis of emerging security threats. FAA regulation of airline safety could provide a model for this type of regulatory process. A third approach is to create a new legislative framework to address cyberattacks. Because HIPAA provides a preexisting model for addressing information security issues in the healthcare industry, an expansion of HIPAA to cover medical device manufacturers and to protect against the risk of all types of intentional cyberattacks—not just those involving PHI—is one potential legislative solution. All three approaches provide a starting point for considering solutions to twenty-first century cybersecurity threats.

A. Industry Self-Regulation

Industry self-regulation is common in the healthcare space and could play an important role in helping to design hospital networks and medical devices that are less vulnerable to cyberattacks. Two examples of industry self-regulation are The Joint Commission's healthcare provider accreditation process[260] and the Pharmaceutical Research and Manufacturers of America (PhRMA) Code[261] for pharmaceutical marketing activities. The Joint Commission is an independent non-profit that accredits and certifies over 20,000 healthcare programs and organizations in the United States.[262] As an independent organization, The Joint Commission mediates between private industry, state regulators, and patients without the strictures of the administrative rulemaking process.[263] The Joint Commission

260. *See About The Joint Commission*, THE JOINT COMMISSION, http://www.jointcommission.org/about_us/about_the_joint_commission_main.aspx (last visited Feb. 9, 2014).

261. *See Code on Interactions with Health Care Professionals*, PHRMA, http://www.phrma.org/code-on-interactions-with-healthcare-professionals (last visited Feb. 9, 2014).

262. *See About The Joint Commission*, *supra* note 260.

263. *See id.*

releases new standards annually and frequently posts policy revisions on its website,[264] leading to an adoption of new standards that is more rapid than a state or federal regulatory process. Compliance with these standards is often mandatory because states require many healthcare providers to receive accreditation from an organization such as The Joint Commission.[265] The Joint Commission accreditation process represents a successful approach to industry self-regulation that permits the ongoing creation of new standards in consultation with both private industry and public regulators to address new challenges in the healthcare industry.

The PhRMA Code is another example of industry self-regulation. To address concerns over pharmaceutical marketing practices, industry participants created the PhRMA Code's voluntary guidelines for marketing activities.[266] Shortly thereafter, the U.S. Office of Inspector General, which investigates healthcare fraud and abuse, designated the PhRMA Code as the minimum standard for marketing to healthcare professionals,[267] laying the groundwork for later legislation. The Physician Payment Sunshine Act of 2009, adopted as part of the Affordable Care Act (ACA), built on the PhRMA Code and FDA guidelines by requiring certain disclosures related to marketing practices.[268] By developing and voluntarily adopting the PhRMA Code, industry participants took the first steps towards addressing an important industry concern and also helped shape future legal and regulatory requirements.

The Joint Commission accreditation process and the PhRMA Code demonstrate that industry self-regulation can help address safety concerns and confront new industry challenges. In the highly regulated healthcare industry, self-regulation may play an important role in a larger government regulatory framework. As healthcare providers and medical device manufacturers begin to confront the challenges posed by cybersecurity, they could develop industry

---

264. *See, e.g.*, *Hospitals (CAMH)*, THE JOINT COMMISSION, http://www.jointcommission.org/standards_information/hap_requirements.aspx (last visited Feb. 9, 2014).

265. *See State Recognition*, THE JOINT COMMISSION, http://www.jointcommission.org/state_recognition/state_recognition.aspx (last visited Feb. 9, 2014).

266. *See* Howard L. Dorfman, *The 2009 Revision to the PhRMA Code on Interactions with Healthcare Professionals: Challenges and Opportunities for the Pharmaceutical Industry in the Age of Compliance*, 31 CAMPBELL L. REV. 361, 361 (2009).

267. *Id.* at 362.

268. *See* 42 U.S.C. § 1320a-7(h) (West 2014).

standards to guide the creation of new software and systems that help protect against cyberattacks. This type of approach could allow industry to more quickly and flexibly address emerging cybersecurity threats while potentially reducing the need for burdensome federal and state regulatory requirements. Because the FDA is likely to take an increasing role in cybersecurity regulation, an industry attempt to address these issues could also lead to a better dialogue between the agency and medical device manufacturers. The PhRMA Code provided an important starting place for later laws and regulations addressing pharmaceutical and medical device marketing, and medical device manufacturers and healthcare providers would be wise to similarly take a proactive stance towards developing new approaches to address the threat of cyberattacks.

B. Forward-Looking FDA Regulation to Address Rapidly Evolving Threats

A second approach to protecting against cyberattacks is to develop a FDA regulatory structure that proactively identifies and protects against evolving information security threats. This would represent a shift from existing agency practice. Currently, the FDA relies primarily on adverse event reporting and postmarket studies to monitor the continuing effectiveness of medical devices—techniques that may be ineffective at preventing cyberattacks before they occur. In conjunction with a more forward-looking approach, the FDA could develop a flexible regulatory process that permits the agency to work with medical device manufacturers and hospitals to address cyberattack threats in proportion to the risk posed.

The FDA's draft guidance on cybersecurity is a step in the right direction. The guidance adopts several of the information security recommendations listed in the GAO report, such as encryption software, frequent antivirus and anti-spyware updates, and authentication procedures.[269] The FDA has solicited comments on the guidance[270] and will likely use it as a starting point for developing more detailed cybersecurity standards. The FDA has also recently released twenty-five new standards for medical device interoperability and security.[271] In conjunction with industry and

269. *See* ATTACK SURFACE, *supra* note 13, at 2; CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124, at 3-4.

270. *See* CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124.

271. U.S. Food & Drug Admin., *FDA Recognizes Certain Standards for Interoperability and Cybersecurity of Medical Devices*, FDA,

cybersecurity experts, the FDA should continue to develop standards that help secure the thousands of different types of medical devices and networks against cyberattacks.

Building on these standards, the FDA should develop a strategy for identifying cybersecurity threats before they materialize, rather than after malicious actors exploit them. The FDA does not currently regulate hospital networks,[272] and the agency relies on a system of adverse event reporting, postapproval studies, and postapproval reports to monitor medical devices already on the market.[273] Adverse event reporting identifies medical device flaws only after patient harm (or a near miss) has occurred. Annual postapproval reports may come too late to alert the FDA of cyberattack threats. While postapproval studies could focus on information security risks, these studies generally focus on risks identified at the time the device was approved, not risks that emerge later.[274] The FDA's Sentinel System, a national electronic system that monitors the postmarket safety of medical products, represents an initiative to replace passive postmarket monitoring with more active surveillance.[275] However, even this initiative focuses on recognizing safety issues as they occur rather than on preventing them from occurring in the first place.[276]

Protecting against intentional cyberattacks requires a different approach than protecting against unintentional medical device defects. The FDA has announced that it will develop a cybersecurity laboratory to test medical devices for security flaws.[277] If the FDA uses this lab to continuously and proactively monitor the cybersecurity of medical devices currently on the market, this lab could be a valuable tool in protecting against cyberattacks. In order to use this lab effectively, however, the FDA will have to equip itself

---

http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm364035.htm (last updated Aug. 6, 2013).

272. *See* Mearian, *supra* note 2.

273. *See supra* Part II.B.

274. U.S. Food & Drug Admin., *Post-Approval Studies (PAS) – Frequently Asked Questions (FAQ)*, FDA, http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/PostApprovaStudies/ucm135263.htm (last visited Feb. 9, 2014).

275. U.S. FOOD & DRUG ADMIN., THE SENTINEL INITIATIVE: NATIONAL STRATEGY FOR MONITORING MEDICAL PRODUCT SAFETY 4 (2008), *available at* http://www.fda.gov/downloads/Safety/FDAsSentinelInitiative/UCM124701.pdf.

276. *See id.* at 8 (discussing how FDA will improve collection and analysis of data to identify existing safety issues).

277. *FDA to Develop Cybersecurity Laboratory*, AAMI NEWS (July 24, 2013), http://www.aami.org/news/2013/072413_FDA_Cybersecurity_Lab.html.

with the latest information about potential new medical device security flaws. In addition to hiring scientists, the FDA should hire hackers who can pinpoint new security vulnerabilities. The FDA should also develop a program to work with other government agencies, security companies, medical device manufacturers, and healthcare providers to identify and find solutions to new information security risks. The biggest challenge will be to identify and respond to new cyberattack threats quickly enough to flag these issues for manufacturers and healthcare providers before attacks materialize. The FDA may need to seek additional funding and potentially new regulatory authority from Congress to take on this type of role in identifying and protecting against cyberattacks.

In addition to conducting its own proactive monitoring of cybersecurity risks, the FDA should leverage industry compliance programs to ensure manufacturers similarly identify and protect against new threats. Medical device manufacturers are likely in the best position to know the weaknesses in their devices and to monitor their devices for new vulnerabilities. The FDA's draft guidance recommends that manufacturers create a systematic plan for updating device security.[278] If the FDA can require manufacturers to develop robust cybersecurity programs to gain approval for their devices, the FDA can then monitor manufacturers to ensure compliance with these programs. However, the FDA may need to issue new regulations or look to Congress for authority to penalize device manufacturers who do not adhere to their cybersecurity programs.

Once the FDA identifies a new risk through its own investigation or through industry reporting, it will have to develop a flexible and tailored approach to mitigating the risk. Unlike hardware flaws that are difficult to repair—such as faulty wiring in a pacemaker—software flaws may be easier to fix. Unlike hardware flaws, however, a mandatory software patch may quickly turn into a liability if it hinders future security patches or creates a new vulnerability. The FDA will have to tread carefully. If the FDA promulgates very specific cybersecurity standards and ties premarket review or approval to meeting these standards, there is a significant risk that such standards will quickly become outmoded. Out-of-date standards that do little to improve cybersecurity may impose unnecessary costs on companies. By requiring one method of addressing a security threat, out-of-date standards could hinder cybersecurity by preventing

278. CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124, at 5.

companies from adopting a new and better method of addressing a security flaw. Many medical device companies are unwilling to update outmoded software because of the fear that their products will lose FDA approval;[279] detailed FDA regulation of cybersecurity could further exacerbate this problem.

The FAA's airworthiness directive process serves as a model for a regulatory process where the agency takes an active role in identifying and remedying ongoing, and sometimes minor, safety risks. If the FAA finds that unsafe conditions exist, the FAA may issue an airworthiness directive that requires air carriers to correct the unsafe condition within a certain period of time.[280] The FAA may also approve an "alternative method of compliance," such as the use of different procedures or service instructions, as long as an "acceptable level of safety is maintained."[281] The FAA adopted the airworthiness directive process as a way to improve safety by increasing coordination between the agency and the airline industry.[282] A similar approach that is focused on communication between the FDA and medical device manufacturers and hospitals could improve safety while leaving room to flexibly address evolving cybersecurity threats.

Many different government agencies will need to rethink their regulatory processes to respond to rapidly evolving technology and the threat of intentional cyberattacks. Monitoring adverse events may be sufficient to detect and correct unintentional risks; fighting intentional attacks may require a more proactive and vigilant approach. Speed and flexibility will be important. While the Administrative Procedure Act's notice and comment process does not lend itself to these characteristics, the FDA could look to other regulatory agencies such as the FAA for examples of how to quickly and flexibly respond to new risks.

C. Expanding HIPAA to Address the Threat of Cyberattacks on Medical Devices and Hospital Networks

While FDA reforms will help, Congress must ultimately revisit

279. *See* Talbot, *supra* note 24.

280. FED. AVIATION ADMIN., AIRWORTHINESS DIRECTIVE 2006-15-15: PROCESS REVIEW TECHNICAL REPORT 4 (2009), *available at* http://www.faa.gov/aircraft/air_cert/continued_operation/media/AD%202006-15-15%20Report%206-3-09.pdf.

281. *Id.*

282. *Id.* at 5.

the question of how to protect medical devices and hospital networks against cyberattacks. HIPAA governs the information security of hospital networks, but it does not apply to cyberattacks that do not involve PHI. HIPAA also does not apply to most medical device manufacturers. FDCA regulates medical devices but not hospital networks. FDCA's current device classification scheme reflects the harm to patients posed by unintentional threats, but not by intentional cyberattacks. A Class I MDDS may provide a vehicle for a malicious actor to attack a hospital network, whereas a Class III pacemaker may not be hooked up to a hospital network at all. While the FDA's guidance on cybersecurity is a step in the right direction, it is not mandatory. Criminal law may eventually deter the malicious actors behind cyberattacks, and tort law may eventually incentivize manufacturers and providers to adopt cybersecurity measures. For the present, however, criminal and tort law are ineffective tools. What is needed is a regulatory scheme that applies to both medical devices and hospital networks, and that imposes sensible but mandatory requirements on manufacturers and hospitals.

HIPAA provides a starting point for a new regulatory scheme. Congress could expand HIPAA's information security requirements to apply to medical device manufacturers. Because HIPAA already applies to a small number of device manufacturers that sell directly to Medicare patients,[283] it is conceivable that Congress could expand HIPAA to apply to all device manufacturers. Congress could also expand HIPAA to apply to any type of cyberattack that harms patient health or privacy. Limiting HIPAA to attacks involving PHI makes little sense when cyberattacks could harm patient health without involving PHI.

Expanding HIPAA would force Congress to address the question of how HHS and the FDA should work together to regulate cyberattacks against medical devices and hospital networks. HHS oversees HIPAA, while the FDA oversees FDCA. In addition, many different agencies play some role in protecting against cyberattacks.[284] The federal Information Security and Privacy Board "finds that diffusion of responsibility when it comes to cybersecurity of medical

283. *See Privacy Basics*, *supra* note 106.

284. Alexander Gaffney, *Federal Board: Need for a Single Entity to Assess Cybersecurity Standards for Devices*, REGULATORY FOCUS (July 31, 2013), http://www.raps.org/focus-online/news/news-article-view/article/3871/federal-board-need-for-a-single-entity-to-assess-cybersecurity-standards-for-de.aspx.

devices raises growing concern."[285] Because medical devices are now an integral part of hospital networks, at the very least FDA and HHS should develop a joint regulatory scheme. FDA's draft guidance on cyberattacks adopts the same general principles as HIPAA—confidentiality, integrity, and availability[286]—suggesting that the two agencies may be able to find common ground. If Congress were to expand HIPAA or otherwise revisit the regulation of medical devices and hospital networks to protect against cyberattacks, it might consider whether one agency should take the lead in this area.

Expanding HIPAA would incentivize medical device manufacturers and hospitals to protect against cyberattacks. As described in Part II, the standard of care for cybersecurity is relatively unclear. Until courts have the opportunity to grapple with several cases involving cyberattacks, it is unlikely that courts will have the opportunity to flesh out a standard of care that will incentivize medical device manufacturers and hospitals to take additional cybersecurity precautions. In the interim, Congress could expand HIPAA to impose fines on medical device manufacturers and healthcare providers if a cyberattack occurs. This is one way to incentivize rapid and flexible response by industry even where the standard of care is unclear. This type of regulatory approach is consistent with that of the Obama administration, which has focused on setting "performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt."[287]

Under HIPAA, there are four tiers of culpability if a patient data breach occurs. The defendant's level of culpability determines the amount of damages. As described in Part II, the first tier covers violations where "the person did not know (and by exercising reasonable diligence would not have known) that such person violated such provision," with a minimum penalty of $100 per violation and an annual maximum penalty of $25,000 for repeat violations.[288] The second tier covers violations where "the violation was due to reasonable cause and not to willful neglect" with a minimum penalty of $1,000 per violation and an annual maximum penalty of $100,000

285. *Id.*

286. *See* CONTENT OF PREMARKET SUBMISSIONS, *supra* note 124.

287. Exec. Order No. 13563, 76 Fed. Reg. 3821 (Jan. 21, 2011).

288. HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56127 (Oct. 30, 2009) (to be codified at 45 C.F.R. pt. 160), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf.

for repeat violations.[289] The third tier covers violations "due to willful neglect" that are corrected within a certain period of time, with a minimum penalty of $10,000 per violation and an annual maximum penalty of $250,000 for repeat violations.[290] The fourth and final tier covers violations that are "due to willful neglect" but are not corrected in a timely manner, with a minimum penalty of $50,000 per violation and an annual maximum penalty of $1.5 million.[291]

Congress could use this sliding scale approach to incentivize medical device manufacturers and healthcare providers to adopt cybersecurity measures.[292] A sliding scale approach provides at least two benefits over a fine-grained regulatory approach. First, it forces medical device manufacturers and healthcare providers to forecast future threats rather than to rely on FDA or HHS standards that—due to the length and difficulty of the regulatory process—may only address current (or even past) threats. This approach incentivizes industry to rapidly adapt to changing threats or face liability. Second, a sliding scale approach to damages allows industry to develop the most cost-effective approach. While a particular regulatory standard may make sense when promulgated, it may not make sense even a few months later in the rapidly changing world of software. Forcing industry to adopt an obsolete standard may be costly and counterproductive.

Congress or the FDA would have to carefully define the types of violations that trigger liability for device manufacturers and hospitals. If every non-negligent software vulnerability led to a fine, the statute could over-incentivize investment in cybersecurity. It may make sense to apply the tier one through tier three penalties only in the case of a cyberattack that leads to large-scale disruption of a network or physical harm to a patient. Tier four penalties for willful neglect could apply to security flaws that are serious but remain uncorrected. The statute or accompanying regulations would have to define what constitutes a serious security flaw.

Congress would also have to carefully consider which entities would face penalties under this scheme. Medical device

289. *Id.*

290. *Id.*

291. *Id.*

292. It may also be possible to simply amend HIPAA to cover cyberattacks and to make medical device manufacturers liable. However, HIPAA represents a carefully constructed statutory framework that addresses both privacy and security, and it may be difficult to integrate liability for cyberattacks without disrupting this framework.

manufacturers have greater insight into the security flaws of their individual medical devices, whereas large healthcare providers such as hospitals have control over the security features of their networks. The security of individual devices and hospital networks both play an important role in cybersecurity, although applying the same penalty scheme to both types of entities may create different incentives for medical device manufacturers and hospitals. A security flaw in a medical device may result in a large number of violations for a single medical device manufacturer. Consequently, the "per violation" penalties may be too high—or conversely, the maximum annual penalties may be too low—to ensure the optimal amount of deterrence.

The same penalty scheme could affect healthcare providers differently. Penalizing hospitals with thin profit margins may be counterproductive in some cases, making it more difficult for the hospital to invest in security or other important aspects of patient care. Different types of healthcare providers have vastly different resources and use different types of devices and networks. Focusing on large providers such as hospitals may be sufficient to protect against cyberattacks as long as incentives for medical device manufacturers provide an extra layer of security for devices and networks used by small providers. Ultimately, calibrating the penalties may be difficult and would require research into the best way to incentivize industry without unduly increasing costs or sacrificing patient care.

While Congress has important details to work out before expanding HIPAA to addresses cyberattacks against both medical device manufacturers and healthcare providers, this approach could help protect against cyberattacks while leaving it up to industry to adopt the most cost-effective solution. Although it is unlikely that medical device manufacturers or hospitals would support an expanded HIPAA scheme, this approach could ultimately save manufacturers and hospitals compliance costs by reducing overlapping HHS and FDA regulation.

D. Other Approaches

There are other potential approaches to addressing the threat of cyberattacks on medical devices and hospital networks. One solution is to promote investment in technology to identify the malicious actors behind cyberattacks, improving the deterrent power of laws that impose liability on these actors. Tax credits for medical device manufacturers and hospitals that invest in cybersecurity measures are another approach. Negligence liability under the CFAA would also

create incentives for medical device manufacturers and hospitals, although the imposition of criminal liability for negligence is harsh. Other approaches may become viable in the future. As courts begin to grapple with some of the questions posed by negligence liability in the context of cyberattacks, courts may develop a common law framework that renders a statutory approach unnecessary. However, given the emerging nature of the threats described in this Article, waiting for the common law to catch up may waste valuable time that could be spent improving cybersecurity.

CONCLUSION

Congress, regulators, healthcare providers, and medical device manufacturers should address the growing threat of cyberattacks against medical devices and hospital networks. The current legal structure is insufficient to protect patients because it does not adequately deter the malicious actors behind cyberattacks and because it does not focus on the role of healthcare providers and medical device manufacturers in protecting against these attacks. One solution is industry self-regulation, which has been successful in addressing other types of challenges in the healthcare industry. Another solution is to create a more forward-looking FDA regulatory structure geared towards anticipating and preventing cyberattacks. A third option is to build on existing laws such as HIPAA to create a new legislative structure that incentivizes industry to invest in cybersecurity. As recent cyberattacks on military computers and financial institutions suggest, cyberattacks are a serious threat. It is only a matter of time before a malicious actor attacks a medical device or hospital network and harms patients. While networked hospitals and wireless medical devices bring new advances in patient care, they also bring new risks. New approaches are needed to address these risks.