# Networked Medical Devices: Finding a Legislative Solution to Guide Healthcare into the Future

*Louiza Dudin*

## CONTENTS



## INTRODUCTION

As the healthcare industry adjusts to the electronic era, medical devices increasingly boast wireless abilities for efficient data collection and transmission, representing a means for more efficient healthcare. However, medical devices, much like other computer systems, are subject to cybersecurity issues ranging from malware infection to data breaches caused by hackers.[1] In October of 2016, a cyberattack on Dyn, an Internet

1. *See* Russell L. Jones & Sheryl Coughlin, *Networked Medical Device Cybersecurity and Patient Safety: Perspectives of Health Care Information Cybersecurity Executives*, DELOITTE (2013),

infrastructure management company, shut down sites such as Netflix, CNN, the Guardian, and Twitter after malware caused Dyn's server to collapse.[2] Although the attack on Dyn did not involve medical devices, it provides a prime example of the "catastrophic risks" to which networked devices, including medical devices, are vulnerable.[3] Thus, with wireless capabilities comes the threat of cyberattacks that compromise not only the patient information collected by these devices but also the health and safety of patients using the devices.[4]

Recently, the Commission on Enhancing National Cybersecurity released a report recommending that healthcare organizations invest in information technology (IT) infrastructure testing to avoid compromising patients' health information and safety.[5] Some institutions, including government agencies, have used so-called white hat hackers—individuals hired to hack into the institutions' own computer systems to test cybersecurity—to test their security systems to discover and fix vulnerabilities.[6] For instance, in 2013, the Mayo Clinic employed a team of white hat hackers to spend a full week hacking into forty different medical devices presented to them, and the team succeeded in compromising each device.[7] As recently as November 2016, patients using wireless insulin pumps were notified of a security flaw in their devices

---

http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf [https://perma.cc/FTG3-Y9ZL].

2. Mike Orcutt, *Security Experts Warn Congress That the Internet of Things Could Kill People*, MIT TECH. REV. (Dec. 5, 2016), https://www.technologyreview.com/s/603015/security-experts-warn-congress-that-the-internet-of-things-could-kill-people/ [https://perma.cc/H5BS-WCPJ]; *see also* Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say*, GUARDIAN (Oct. 26, 2016), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [https://perma.cc/K28M-YLEM] (stating that the cyberattack, "likely the largest of its kind in history," on Dyn's servers used special "botnet" malware to infect computers and overwhelm servers with traffic).

3. *See* Orcutt, *supra* note 2.

4. *See* Jim Finkle, *U.S. Government Probes Medical Devices for Possible Cyber Flaws*, REUTERS (Oct. 22, 2014), http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022#vxsirEiPIC8ghM5U.97 [https://perma.cc/5XYN-PQP7] (stating that a cybersecurity researcher, Billy Rios, wrote a program that could remotely force multiple pumps to dose patients with potentially lethal amounts of drugs).

5. *See* Elizabeth Snell, *How Healthcare Cybersecurity Ties into Larger National Plan*, HEALTHIT SECURITY (Dec. 6, 2016), http://healthitsecurity.com/news/how-healthcare-cybersecurity-ties-into-larger-national-plan [https://perma.cc/T34H-JKS8]; *see also* COMISSIONN ON ENHANCING NAT'L CYBERSECURITY, REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY (2016).

6. *See* Jason Miller, *IRS Hires 'White-Hat' Hackers to Help Protect IT Systems*, FED. NEWS RADIO (Nov. 28, 2016), http://federalnewsradio.com/cybersecurity/2016/11/irs-hires-white-hat-hackers-help-protect-systems/ [https://perma.cc/K6B9-8FDV].

7. *See* Monte Reel & Jordan Robertson, *It's Way Too Easy to Hack the Hospital: Firewalls and Medical Devices Are Extremely Vulnerable, and Everyone's Pointing Fingers*, BLOOMBERG BUSINESSWEEK (Nov. 16, 2015), http://www.bloomberg.com/features/2015-hospital-hack/ [https://perma.cc/L2SD-FNUM].

which "could permit hackers to take control, alter dosage levels and disable the device altogether."[8] These cybersecurity flaws present a legitimate concern about cyberattacks on medical devices and a consequent need for more effective cybersecurity measures.[9]

The U.S. Department of Homeland Security (DHS) noted that there are approximately 300 types of medical devices affected by the threat of cyberattacks, including drug infusion pumps, ventilators, and external defibrillators.[10] This risk is compounded by the fact that electronic Protected Health Information (ePHI)—the information contained in electronic patient medical records and often gathered via medical devices—is increasing in value on the black market.[11] Personal health information is now more valuable than credit card data. A 2012 report by the Healthcare Information and Management Systems Society stated "a patient health record is valued at $50, compared to $3 for a social security number and $1.50 for a credit card number."[12]

Reflecting the value of ePHI, the media is increasingly focusing its attention on the threat of cyberattacks on medical devices. Fictional television shows have broadcast episodes in which public figures, such as the Vice President of the United States, were victims of cyberattacks on their medical devices.[13] In reality, former Vice President Dick Cheney was so disturbed by the potential for cyberattacks on his own cardiac defibrillator that he asked his doctor to disable the device's wireless function.[14] More recently, pharmaceutical and medical device

---

8. Jon Markman, *Connected Medical Devices Cause Cybersecurity Blues*, FORBES (Nov. 29, 2016), http://www.forbes.com/sites/jonmarkman/2016/11/29/connected-medical-devices-cause-cybersecurity-blues/#624f5d831dc8.

9. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (2014), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf [https://perma.cc/V6AM-S9UA] [hereinafter HHS PREMARKET GUIDANCE]; *see also* Suzanne B. Schwartz, *National Cyber Security Awareness Month: Understanding the Interdependencies of Medical Devices and Cybersecurity*, U.S. FOOD & DRUG ADMIN. BLOG (Oct. 27, 2016), http://blogs.fda.gov/fdavoice/index.php/2016/10/national-cyber-security-awareness-month-understanding-the-interdependencies-of-medical-devices-and-cybersecurity/ [https://perma.cc/VF3M-3QQ3].

10. *See* Dina Fine Maron, *A New Cyber Concern: Hack Attacks on Medical Devices*, SCI. AM. (June 25, 2013), http://www.scientificamerican.com/article/a-new-cyber-concern-hack/ [https://perma.cc/7R3T-NZDR].

11. *See* Dan Stoker, *Medical Devices: Safe, But Are They Secure?*, HIPPA CENT. (2014), http://docplayer.net/15746703-Medical-devices-safe-but-are-they-secure-dan-stoker-consultant-professional-services-coalfire.html [https://perma.cc/XX3Y-ULK3].

12. *Id.* at 2–3.

13. *See Homeland: Broken Hearts* (Showtime Networks, Inc. broadcast Dec. 2, 2012).

14. *See* Bob Fredericks, *Cheney Feared Terrorists Would 'Hack' Pacemaker*, N.Y. POST (Oct. 19, 2013, 4:11 AM), http://nypost.com/2013/10/19/cheney-feared-heart-gizmo-hack-attack/ [https://perma.cc/J574-6TC5].

manufacturer Johnson & Johnson issued a warning to patients using its insulin pumps that hackers could exploit a security flaw in the pumps "to overdose diabetic patients with insulin."[15] The Food and Drug Administration (FDA) echoed the concern about cyberattacks on medical devices when it issued guidance regarding networked medical devices, stating that vulnerable off-the-shelf software "can allow an attacker to get unauthorized access to a network or medical device[.]"[16] The media and the FDA's attention reflects the reality that cybersecurity is an "indispensable part of medical device design and implementation."[17]

The FDA has the authority to regulate medical devices premarket as well as those in the market.[18] Congress granted this broad regulatory authority to the FDA through the Food, Drug, and Cosmetic Act of 1938 and its subsequent amendments to include medical devices.[19] It is the FDA's responsibility to safeguard medical devices in the United States before and after they enter the market.[20] In response to growing concern over cyberattacks on medical devices, the FDA issued nonbinding guidelines on evaluating cybersecurity for device manufacturers.[21] More specifically, the draft guidance recommends that medical device manufacturers justify the security functions they have chosen for their medical devices during the premarket submission process for approval by the FDA.[22] In addition, the guidance document suggests a framework for manufacturers to implement cybersecurity functions and maintain the integrity of their medical devices.[23] The guidance suggested cybersecurity strategies that include limiting access to networked devices based on the type of device, its use and potential vulnerabilities, and the risk of harm in the event of a cybersecurity breach.[24] Further, the FDA noted that "it is

15. *Yes, Pacemakers Can Get Hacked*, N.Y. POST (Dec. 29, 2016), http://nypost.com/2016/12/29/yes-pacemakers-can-get-hacked/ [https://perma.cc/Q5A4-G3CR].

16. U.S. FOOD & DRUG ADMIN., GUIDANCE FOR INDUSTRY: CYBERSECURITY FOR NETWORKED MEDICAL DEVICES CONTAINING OFF-THE-SHELF (OTS) SOFTWARE, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf [https://perma.cc/8GJB-WFK8] [hereinafter FDA GUIDANCE ON OTS SOFTWARE DEVICES].

17. *See* Stoker, *supra* note 11, at 3.

18. *What Does FDA Regulate?*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194879.htm [https://perma.cc/KC95-C3SY]; *see also Does FDA Regulate Medical Devices?*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194413.htm [https://perma.cc/WH8H-C4X6].

19. 21 U.S.C. § 301 (1938). For pending legislation that addresses direct-to-consumer drug advertising, and investigational drugs and devices for terminally ill, respectively, see H.R. 4565, 114th Cong. (2015); H.R. 790, 114th Cong. (2015).

20. *See* Ann Mileur Boeckman, *An Exercise in Administrative Creativity: The FDA's Assertion of Jurisdiction over Tobacco*, 45 CATH. U. L. REV. 991, 991–92 (1996).

21. *See* HHS PREMARKET GUIDANCE, *supra* note 9, at 4.

22. *Id.*

23. *Id.* at 3–4.

24. *Id.* at 4–5.

rare for healthcare organizations to have enough technical resources and information on the design of medical devices to independently maintain medical device software. Thus, most healthcare organizations need to rely on the advice of medical device manufacturers."[25] As a result, there is a certain amount of reliance by healthcare providers on the information and guidelines medical device manufacturers provide about their networked devices.

As of December 2016, the FDA issued an additional nonbinding guidance document, this time addressing the post-market management of networked medical devices.[26] Particularly, the new guidance emphasizes that manufacturers should monitor the cybersecurity vulnerabilities of their devices after they enter the market.[27] In addition, the FDA sets up "a risk-based framework for assessing when changes to medical devices for cybersecurity vulnerabilities require reporting to the Agency" and when reporting is not required.[28] Medical device manufacturers are encouraged to gather cybersecurity information by means such as "independent security researchers, in-house testing, suppliers of software or hardware technology, health care facilities, and information sharing and analysis organizations."[29] This monitoring is in line with a Presidential Executive Order issued in 2013, which recognized information sharing as an essential component needed to "better protect and defend" against cyberattacks.[30] Finally, the post-market guidance provides that risk-assessment should focus on the risk of harm to a patient—ranging from temporary discomfort to death—if a networked device is vulnerable to attack.[31] Where a medical device's vulnerability to cyberattacks poses a risk of "serious adverse events or death" to patients, the patient harm is deemed "uncontrolled" under the FDA's proposed risk assessment, and manufacturers are urged to notify customers and the community, implement temporary controls, develop a plan to remedy the device's vulnerability, and for some devices,

---

25. *Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software"*, U.S. FOOD & DRUG ADMIN. (2015), http://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm [https://perma.cc/XQ6H-A79J] (responding to when healthcare organizations may apply software patches to medical devices that do not come from the medical device manufacturer).

26. *See generally* U.S. DEP'T OF HEALTH & HUMAN SERVS., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFf (2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf [https://perma.cc/8PUL-VL3P] [hereinafter HHS POSTMARKET GUIDANCE].

27. *See id.* at 4.

28. *Id.*

29. *Id.* at 14.

30. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

31. *See* HHS POSTMARKET GUIDANCE, *supra* note 26, at 15–17.

submit a remediation report to the FDA.[32] Both FDA guidance documents stress the importance of cybersecurity in developing and marketing medical devices, but both are nevertheless nonbinding.

The Office of Inspector General (OIG) with the Department of Health and Human Services (DHHS) announced in the 2016 Work Plan that they intends to focus more intensively on the security of medical devices with wireless network capabilities.[33] Specifically, the OIG announced that it would "examine whether [the] FDA's oversight of hospitals' networked medical devices is sufficient to effectively protect associated electronic protected health information (ePHI)."[34] The OIG noted that medical devices integrated with electronic medical records (EMRs) were included in the threat to personal health information privacy and security.[35] Finally, the OIG remarked that device manufacturers must provide Manufacturer Disclosure Statements for Medical Device Security (MDS2) that assess the "vulnerability and risks associated with ePHI that is transmitted or maintained" by a particular medical device to health care providers purchasing the devices.[36] In contrast to the OIG's 2016 Work Plan, the Plan for 2017 appears to focus on the FDA's activity in addressing cybersecurity issues after devices have entered the market in addition to the FDA's regular premarket approval processes.[37] The 2017 Work Plan announces that OIG "will examine the FDA's plans and processes for timely communicating and addressing a networked medical device cybersecurity compromise" and specifically points out concern for patient safety.[38]

It is clear that government entities, such as the FDA, OIG, and DHHS, acknowledge the urgent need to mitigate the threat of cyberattacks

---

32. *See id.* at 17 (stating that if a manufacturer participates in information sharing, the FDA will not enforce compliance with reporting requirements under 21 C.F.R. § 806, but that class III device remediation must be reported annually). Class III medical devices are the most stringently regulated types of medical devices, such as heart valves, because they pose the highest risk to the patient. *See Overview of Medical Device Classification and Reclassification*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/aboutfda/centersoffices/officeofmedicalproductsandtobacco/cdrh/cdrhtransparency/ucm378714.htm [https://perma.cc/KFB2-6W4P].

33. *See* OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., WORK PLAN: FISCAL YEAR 2016, at 53, http://oig.hhs.gov/reports-and-publications/archives/workplan/2016/oig-work-plan-2016.pdf [https://perma.cc/NMY8-H57U] [hereinafter 2016 OIG WORK PLAN].

34. *Id.*

35. *Id.*

36. *Id.*

37. Marianne Kolbasuk McGee, *What's on HHS OIG's Plan for Scrutinizing Security in 2017?*, GOV INFO SECURITY (Dec. 2, 2016), http://www.govinfosecurity.com/whats-on-hhs-oigs-plan-for-scrutinizing-security-in-2017-a-9571 [https://perma.cc/T7E5-3V78]; *see also* OFF. OF INSPECTOR GEN., DEP'T OF HEALTH & HUMAN SERVS., WORK PLAN: FISCAL YEAR 2017 (Nov. 15, 2016), https://oig.hhs.gov/reports-and-publications/archives/workplan/2017/HHS%20OIG%20Work%20Plan%202017.pdf [https://perma.cc/NMY8-H57U] [hereinafter 2017 OIG WORK PLAN].

38. 2017 OIG WORK PLAN, *supra* note 37, at 62.

on hospital networks and medical devices.[39] However, current avenues for preventing cybersecurity breaches and remedies available to victims of cyberattacks, as well as federal healthcare regulatory laws, do not fully address the problems surrounding networked medical devices. Because cybersecurity risk assessment is not required by law, patients who may be harmed by cyberattacks on medical devices may be barred from seeking redress from device manufacturers whose devices have been market-approved by the FDA.[40] Rather than the provision of nonbinding guidelines, the best means of addressing this issue is through changes in legislation and stringent regulation by the FDA.

This article discusses: (I) the current legal approaches to addressing cybersecurity in general, (II) the shortcomings of current legal approaches, (III) a proposal for legislation to narrow the scope of the Medical Device Amendments (MDA) preemption clause, and (IV) the benefits and shortcomings of the proposed legislation.

## I. CURRENT LEGAL APPROACHES TO PROSECUTING CYBERATTACKS

Currently, prosecutors may use several avenues to address cyberattacks on medical devices: (A) the Computer Fraud and Abuse Act (CFAA), (B) the Federal Anti-Tampering Act, (C) tort law, and (D) the Health Insurance Portability and Accountability Act (HIPAA).

### *A. The Computer Fraud and Abuse Act*

Under the CFAA, individuals who access a computer without authorization to either obtain information or transmit harmful information are subject to a fine, imprisonment for up to ten years, or both.[41] To recover under Section 1030(a)(2)(C), a plaintiff would have to show that an accused (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and (3) obtained information from any protected computer.[42] Alternatively, a plaintiff harmed by malicious software on a medical device may recover under Section 1030(a)(5) if they are able to show that the accused accessed a protected computer without authorization either knowingly or intentionally, and both (1) caused the transmission of a program, code, or command, and (2) as a result of such

39. *See, e.g.*, HHS PREMARKET GUIDANCE, *supra* note 9, at 1; *see also* 2017 OIG WORK PLAN, *supra* note 37, at 51, 61–62.

40. *See* Riegel v. Medtronic Inc., 552 U.S. 312 (2008).

41. 18 U.S.C. § 1030 (2011). Pending legislation to clarify the meaning of "access without authorization" and other purposes has been proposed but is projected not to pass. *See* Aaron's Law Act of 2015, S. 1030, 114th Cong. (2015).

42. 18 U.S.C. § 1030(a)(2) (2011).

conduct, caused damage.[43] Thus, the CFAA punishes intentional acts causing harm, but it is important to note that the CFAA does not impose any liability on the manufacturers of medical devices.[44]

### *B. The Federal Anti-Tampering Act*

Similar to the CFAA, the Federal Anti-Tampering Act also imposes criminal liability on intentional actors who tamper with consumer products.[45] To prevail under Section 1365(a) of the Act, a plaintiff must show that the accused acted (1) with reckless disregard for the risk that another person will be placed in danger of death or bodily injury and (2) with extreme indifference to such risk.[46] The Federal Anti-Tampering Act punishes malicious actors in accordance with the damage caused, with potential imprisonment ranging from ten years to life.[47] Much like the CFAA, the Federal Anti-Tampering Act punishes intentional or reckless actors whose actions cause harm but does not impose liability on medical device manufacturers unless the damage results from the manufacturers' actions.[48] However, unlike the CFAA, Section 1365(g) of the Federal Anti-Tampering Act gives the FDA and the Department of Agriculture authority to investigate violations involving a consumer product regulated by their respective agencies.[49]

### *C. Tort Law*

Tort law imposes liability on the malicious actors behind cyberattacks and may also impose liability on negligent medical device manufacturers. Actors causing harm by way of a cyberattack on a patient's medical device may be sued under the tort of battery.[50] To prevail under a theory of battery, the plaintiff would have to show (1) that the accused acted intending to cause harmful or offensive contact with the plaintiff, or an imminent apprehension of such contact, and (2) that such contact

---

43. 18 U.S.C. § 1030(a)(5); *see also* Michael S. Urcuyo, *From Internet Trolls to Seasoned Hackers: Protecting our Financial Interests from Distributed Denial-of-Service Attacks*, 42 RUTGERS COMPUTER & TECH. L.J. 299, 304 (2016).

44. Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139, 152 (2014).

45. 18 U.S.C. § 1365 (2012).

46. 18 U.S.C. § 1365(a).

47. *Id.*

48. *See* 18 U.S.C. § 1365(b) (stating "Whoever, with intent to cause serious injury to the business of any person, taints any consumer product or renders materially false or misleading the labeling of, or container for, a consumer product, if such consumer product affects interstate or foreign commerce, shall be fined under this title or imprisoned not more than three years, or both").

49. 18 U.S.C. § 1365(a).

50. Wellington, *supra* note 44, at 175–77.

directly or indirectly resulted.[51] Under the Restatement of Torts, "contact with another's person" includes contact with anything held or attached to the person harmed.[52] This inclusion stems from battery theory, where "the plaintiff's grievance consists in the offense to the dignity involved in the unpermitted and intentional invasion of the inviolability of his person."[53]

Medical device manufacturers are governed by federal regulations, such as the Federal Food, Drug, and Cosmetic Act of 1938 (FDCA). Medical devices that "support or sustain human life" or "present a potential unreasonable risk of illness or injury" are subject to a "complete and thorough review process with the FDA," known as premarket approval (PMA) before they may be marketed.[54] This process requires a medical device manufacturer to provide to the FDA "reasonable assurance that its device is both safe and effective."[55] Thus, an injured patient may have a cause of action against medical device manufacturers that "fail to adopt reasonable cybersecurity measures" for their medical devices.[56] The FDA has recently issued draft guidance for manufacturers of devices that "contain software (including firmware) or programmable logic as well as software that is a medical device."[57] This guidance recommends that "manufacturers should address cybersecurity during the design and development of the medical device."[58] However, the draft guidance is nonbinding.[59] Consequently, the draft guidance does not appear to provide a strong incentive for manufacturers to meet their duty of care in ensuring the cybersecurity of their devices, and those devices approved for market by the FDA are shielded from manufacturer liability claims.[60] As such, tort law provides avenues for injured patients to seek redress but poses difficulties in assigning liability and ability to sue.

### *D. The Health Information Portability and Accountability Act*

Not all medical device companies are required to comply with the Health Information Portability and Accountability Act (HIPAA), although those companies that do comply are often "business associates" of

51. RESTATEMENT (SECOND) OF TORTS § 18 (AM. LAW INST. 1965).
52. *Id.*
53. *Id.*
54. *In re* Medtronic Inc., 592 F. Supp. 2d 1147, 1150 (D. Minn. 2009).
55. 21 U.S.C. § 360d (2011).
56. *See* Wellington, *supra* note 44, at 178.
57. *See* HHS PREMARKET GUIDANCE, *supra* note 9, at 2.
58. *Id.* at 4.
59. *Id.* at 1.
60. *See* Wellington, *supra* note 44, at 178; *see also* Riegel v. Medtronic, Inc., 522 U.S. 312 (2008) (holding that plaintiffs cannot sue device manufacturers in tort under most circumstances once the FDA clears a device through the PMA process).

healthcare providers.[61] HIPAA provides some protection against cyberattacks by creating a regulatory framework to safeguard protected health information (PHI).[62] The Act specifically regulates both the privacy and security of PHI, as well as healthcare providers that electronically bill for services (hereinafter referred to as "covered entities").[63] Generally, medical device companies are not covered by HIPAA unless they sell equipment to patients and bill Medicare.[64] Two regulations within HIPAA apply to protection of PHI: the Privacy Rule and the Security Rule.[65]

The Privacy Rule applies to information that could reasonably be used to identify an individual, including name; address; and past, present, or future health conditions.[66] The rule further permits de-identification of health information, entailing the removal of "specified identifiers of the individual" or "a formal determination by a qualified statistician."[67] The latter involves "a person with appropriate knowledge of and experience with" statistics to use scientific and statistical methods to determine that there is a very small risk that the information, combined with publicly available information, could be used to identify a patient.[68] To be properly anonymized under the Privacy Rule, ePHI must meet an "actual knowledge" standard, in that the de-identification "is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual."[69] One goal of the Privacy Rule and its requirements is to limit use and disclosure of protected health information, the latter being subject to exceptions as permitted by the Privacy Rule or as authorized by the individual with whom the information is concerned.[70] Further, an entity's maintenance, use, or disclosure of PHI

---

61. *See When may a Covered Health Care Provider Disclose Protected Health Information, with an Authorization or Business Associate Agreement, to a Medical Device Company Representative*?, U.S. DEP'T OF HEALTH & HUMAN SERV., https://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html [https://perma.cc/RLH9-VQGW].

62. 45 C.F.R. § 164.312 (2010).

63. *Privacy Basics: A Quick HIPAA Check for Medical Device Companies*, MED. DEVICE & DIAGNOSTIC INDUSTRY (Aug. 1, 2009), http://www.mddionline.com/article/privacy-basics-quick-hipaa-check-medical-device-companies [https://perma.cc/PL9W-YA5J] [hereinafter *Privacy Basics*].

64. *Id.*

65. *Id.*

66. U.S. DEP'T OF HEALTH & HUMAN SERV., SUMMARY OF THE HIPAA PRIVACY RULE 3 (2003), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html?language=es [https://perma.cc/489Z-5PVU] [hereinafter HIPAA PRIVACY RULE SUMMARY].

67. *Id.* at 4 (noting that there are no restrictions on the use or disclosure of de-identified health information, because it does not provide a reasonable basis to identify an individual).

68. 45 C.F.R. § 164.514(b) (2011).

69. *See* HIPAA PRIVACY RULE SUMMARY, *supra* note 66, at 4.

70. *Id.* at 4.

is subject to compliance investigations by the DHHS, for which such information may be accessed.[71]

The Security Rule applies to health care providers who transmit health information in electronic form.[72] Further, the Health Information Technology for Economic and Clinical Health (HITECH) Act expanded the application of the Security Rule to covered entities' business associates, which are entities or persons that are involved in the "use or disclosure of protected health information" on behalf of a covered entity.[73] Business associates include entities providing legal, accounting, consulting, administrative, and data aggregation services, among others.[74] The main purpose of the Security Rule is to provide enough flexibility to allow the integration of technological advancements into the operation of healthcare, specifically the electronic transmission of protected health information, while mitigating the risks to consumers.[75]

Most medical device distributors are not considered "business associates" under HIPAA but could be classified as such if their involvement in health information gathering, billing, or furnishing of "health care" satisfied HIPAA's definition of "health care providers."[76] Medical device manufacturers that sell their products to other entities for medical use would be required to enter into a business associate agreement in order to access PHI for cost-savings estimates on the use of their devices.[77] As a result, the expansion of the HIPAA Privacy and Security Rules has resulted in some, but not all, medical device manufacturers being subject to HIPAA compliance.

## II. SHORTCOMINGS OF CURRENT LEGAL APPROACHES

Part I described the current legal approaches to prosecuting cyberattacks. These approaches do not sufficiently address the threat of cyberattacks partly because they focus on deterrence or require an identifiable malicious actor. In cyberspace, effective deterrence is difficult

71. *See* DEP'T OF HEALTH & HUMAN SERVS., RESTRICTIONS ON GOVERNMENT ACCESS TO HEALTH INFORMATION, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/govtaccess.html [https://perma.cc/67WV-VXTP].

72. *See* HIPAA PRIVACY RULE SUMMARY, *supra* note 66.

73. DEP'T OF HEALTH & HUMAN SERVS., HEALTH INFORMATION PRIVACY: UNDERSTANDING HIPAA PRIVACY: BUSINESS ASSOCIATES (2003), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [https://perma.cc/GUW7-XCHZ].

74. 45 C.F.R. § 160.103 (2015).

75. *See* HIPAA PRIVACY RULE SUMMARY, *supra* note 66.

76. Barbara Kramer & Mitchell A. Kramer, *The New HIPAA Rules and What They Mean for Medical Device Distributors*, KRAMER & KRAMER, LLP, http://www.kramerandkramer.com/wp-content/themes/kramerkramer/img/HIPAA_REVISED_RULES_2.pdf [https://perma.cc/7JES-U2F2].

77. *Id.*

to implement, and an identifiable actor may be difficult to pinpoint.[78] Without the ability to attribute cyberattacks to the actors who perpetrate them or incentivize these actors to cease their attacks, the current legal framework for prosecuting such attacks remains insufficient.[79]

The CFAA may not serve as a sufficient deterrent against these attacks because it requires the ability to identify the malicious actors responsible.[80] Further, case law provides that even if an actor is identified, the evidentiary standard of "beyond a reasonable doubt" must be met to convict for any alleged cyberattack.[81] Tracing a cyberattack back to an actor depends as much on the type of code in the malware used as it does on the investigative resources available and can often leave investigators chasing their own tails.[82] For example, the documents leaked by Edward Snowden in 2013 provided data on the malware used by government agencies to spy on their targets, yet the accused agencies denied ownership of the identified malware.[83] Most cyberattack cases are not accompanied by an information leak to help narrow down malware and individual culprits, and plaintiffs seeking to recover damages do not have the same resources as a government in tracing an actor through cyberspace.[84] Although pinpointing the actor behind a cyberattack may be possible in cases where the actor uses a company laptop and login credentials,[85] it is admittedly more burdensome when the actor is less readily identifiable.[86]

While the Federal Anti-Tampering Act imposes harsher penalties than the CFAA, it does not impose penalties on medical device manufacturers or hospitals that negligently fail to secure their devices or networks.[87] In order to allege a prima facie products liability claim under

---

78. *See* Wellington, *supra* note 44, at 184.

79. *See* Shane McGee, Randy V. Sabett & Anand Shah, *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1, 28–29 (2013) [hereinafter *Adequate Attribution*] (stating: "Our legal and policy frameworks for responding to cyberattacks cannot work unless we have adequate attribution; these frameworks remain incomplete because we lack the basis (sufficient attribution) to actually use them").

80. 18 U.S.C. § 1030 (2011).

81. *See* United States v. Shahulhameed, 629 F. App'x 685, 687 (6th Cir. 2015) (stating that, in reviewing the sufficiency of the evidence, we must affirm the conviction if "after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt" (quoting Jackson v. Virginia, 443 U.S. 307, 319 (1979))).

82. Larry Greenemeier, *CSI: Cyber-Attack Scene Investigation—A Malware Whodunit*, SCI. AM. (Jan. 28, 2016), https://www.scientificamerican.com/article/csi-cyber-attack-scene-investigation-a-malware-whodunit/ [https://perma.cc/NP5E-9TRP].

83. *Id.*

84. *Id.*

85. *Shahulhameed*, 629 F. App'x at 687.

86. *See* Wellington, *supra* note 44, at 184 (stating that "[a]s long as it remains difficult to identify and prosecute the actors behind cyberattacks, criminal law is an insufficient deterrent").

87. 18 U.S.C. § 1030 (2011); 18 U.S.C. § 1365 (2012).

the Federal Anti-Tampering Act, "a plaintiff must demonstrate that the product was in a defective condition that made it unreasonably dangerous, that the defective condition existed when the product left the defendant's control, and that the defective condition proximately caused the plaintiff's injuries."[88] This burden of proof may prove difficult for a plaintiff to overcome.

Tort law imposes similar burdens of proof on plaintiffs regarding the identity of malicious actors. Under the Restatement of Torts, a plaintiff must identify a malicious actor as the cause of harm.[89] As discussed previously, attribution of a cyberattack imposes a high investigative burden that may prove to be impossible,[90] and without the ability to attribute cyberattacks to the actors who perpetrate them, the current legal framework for prosecuting such attacks remains insufficient.[91]

HIPAA fails to create a direct incentive for medical device manufacturers to adopt improved security measures because it does not apply to medical device companies unless they directly deal with PHI.[92] HIPAA focuses on the security of ePHI and does not address some of the central issues posed by the threat of cyberattacks on medical devices, such as hackers causing serious injury or death by remotely commandeering implanted medical devices (such as pacemakers and drug pumps) of patients.[93] Additionally, HIPAA does not create a right to private action (such as tort claims) by itself, although its regulations do not preempt causes of action that arise from a breach of HIPAA regulations.[94] As a result, HIPAA requires hospitals to implement and maintain secure networks in order to protect patient information but fails to provide incentive for medical device manufacturers to implement security features in their devices.[95]

Finally, and perhaps most significantly, the FDA's broad jurisdiction over the regulation of medical devices, combined with the preemption clause contained in the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act, constitute a roadblock to common law claims

88. Ramirez v. Medtronic Inc., 961 F. Supp. 2d 977, 981 (D. Ariz. 2013).

89. RESTATEMENT (SECOND) OF TORTS § 18 (AM. LAW INST. 1965).

90. *See* Lieutenant Commander Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 7 (2009); Greenemeier, *supra* note 82.

91. *See Adequate Attribution*, *supra* note 79, at 28–29.

92. *See* HIPAA BUSINESS ASSOCIATES, *supra* note 73.

93. Mayura Noordyke, *Medical Device Exemptions to the Prohibition on Circumvention*, BRANDS PROTECTION BLOG (Nov. 18, 2015), http://www.thebrandprotectionblog.com/medical-device-exemptions-to-the-prohibition-on-circumvention/ [https://perma.cc/V6BX-VE9L].

94. Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 46–47 (Conn. 2014).

95. *See* Wellington, *supra* note 44, at 158.

asserting that a medical device was defective.[96] As previously discussed, compliance with the FDA's draft guidance on cybersecurity is not mandatory for medical device manufacturers.[97] In light of its "exclusive jurisdiction on the regulation of medical devices," the FDA's reluctance to enforce compliance with its issued guidance is problematic for the security of patient information and patient safety[98] because the guidance does not establish any rights for patients or create liability for manufacturers or the FDA.[99] Further, the FDA relies on a system of adverse event reporting to monitor medical devices that are already on the market.[100] This reporting system lacks a prospective approach necessary to prevent patient data and safety from being harmed[101] because it only identifies flaws once harm has occurred, and threat reports come too late.[102] Because the manufacturers of medical devices are in the best position to identify and find solutions to threats, the FDA should leverage its ability to increase oversight under its regulatory authority in order to ensure that manufacturers comply with safety and security standards and address threats prospectively rather than reporting adverse events after the fact.

## III. PROPOSED LEGISLATIVE SOLUTION

Although government entities and media commentators increasingly acknowledge the threat of cyberattacks, and the former have suggested some guidelines, a federal regulatory approach is the best solution for addressing the issue of cyberattacks on medical devices.[103] As discussed above, the FDA's regulatory authority over medical devices, combined with the preemption clause of the MDA, constitutes a significant

96. 21 U.S.C. § 360k(a) (2015). Pending legislation, Ariel Grace's Law, which amends 21 U.S.C. 360k, states, "[n]othing in this section shall be construed to modify or otherwise affect any action for damages or the liability of any person under the law of any State." *See* H.R. 5403, 114th Cong. (2015).

97. *See* HHS PREMARKET GUIDANCE, *supra* note 9, at 3.

98. David Holtzman, *FDA Approach to Medical Device Security Is a Step Backward*, HEALTHCARE IT NEWS (Apr. 7, 2015), http://www.healthcareitnews.com/news/fda-approach-medical-device-security-step-backward [https://perma.cc/FS8J-BDG3].

99. *See* HHS POSTMARKET GUIDANCE, *supra* note 26, at 4.

100. *Mandatory Reporting Requirements: Manufacturers, Importers and Device User Facilities*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/ucm2005737.htm [https://perma.cc/V6N6-4BWX].

101. Dov Greenbaum, *Direct Digital Engagement of Patients and Democratizing Health Care*, 32 SANTA CLARA HIGH TECH. L.J. 93, 116 (2015).

102. *See Mandatory Reporting Requirements*, *supra* note 100 (stating that "manufacturers are required to report to the FDA when they learn that any of their devices may have caused or contributed to a death or serious injury").

103. *See* HHS PREMARKET GUIDANCE, *supra* note 9; 2016 OIG WORK PLAN, *supra* note 33, at 53; Maron, *supra* note 10.

roadblock to plaintiffs harmed by medical devices seeking private action.[104] Congress should amend the MDA to (1) exempt private action asserting medical device defect caused by intentional cyberattacks and (2) exempt networked medical devices that are not sufficiently regulated by the FDA's premarket approval process.

### *A. Exemption for Private Action Asserting Defect Caused by Cyberattacks*

Despite the lack of enforcement of the FDA's guidelines for medical device manufacturers, patients harmed after using medical devices approved for market may find their common law claims preempted under the MDA.[105] Common law claims under the MDA are preempted because market-approved devices have already passed the FDA's rigorous approval process, and the statute bars claims attempting to impose additional requirements on manufacturers.[106] However, the MDA also supplies exceptions to its bar on common law claims, such as claims alleging manufacturer defect.[107] These exceptions provide an avenue for patients harmed by defective devices to seek redress. Narrowing the scope of the MDA preemption clause and allowing for exceptions, such as manufacturer defect to take into account flaws such as network vulnerabilities would provide plaintiffs greater protections and incentivize manufacturers to adhere closely to FDA guidelines.[108]

The federal government's requirements for the FDA's premarket approval process for medical devices are consistent with the fact that common law claims are preempted by the MDA:

> [N]o State or political subdivision of a State may establish or continue in effect with respect to a device intended for human use any requirement (1) which is different from, or in addition to, any requirement applicable under this chapter to the device, and (2) which relates to the safety or effectiveness of the device or to any other matter included in a requirement applicable to the device under this chapter.[109]

---

104. 21 U.S.C. § 360k(a) (2015).

105. *Id.*

106. *Id.*

107. 21 U.S.C. § 360k (2015).

108. *See* Riegel v. Medtronic Inc., 552 U.S. 312, 328–31 (2008); *see also* FDA GUIDANCE ON OTS SOFTWARE DEVICES, *supra* note 16, at 3 ("You (the device manufacturer who uses OTS software in your medical device) bear the responsibility for the continued safe and effective performance of the medical device, including the performance of OTS software that is part of the device."); Stengel v. Medtronic Inc., 704 F.3d 1224, 1233 (9th Cir. 2013) (narrowing the scope of preemption as compared to *Riegel*).

109. 21 U.S.C. § 360k(a).

The rationale is that if the FDA authorizes the commercial distribution of a medical device that has passed its premarket approval process, then common law actions alleging defect of the medical device should be barred.[110] Congress implemented this preemption clause under the policy that it "justifies the effective promotion and marketing of medical devices despite the potential cost to a few individuals who may lack redress for the occasional failure of [a] device."[111] For example, in *Riegel v. Medtronic*, the U.S. Supreme Court held that the MDA preempted the petitioner's state tort law claims.[112] In that case, the Court defined a two-pronged test for determining preemption of a common law claim.[113] According to this test, courts must determine whether the FDA's premarket approval process imposes device specific requirements on manufacturers, and if so, whether the asserted common law claims impose different or additional requirements to those set out by the FDA.[114] In *Marmol v. St. Jude Medical Center*, the court held that Florida's state law did not recognize the plaintiff's strict liability and negligence claims against a medical manufacturer based on violations of FDA regulations.[115] The federal claims were impliedly preempted because the state law did not recognize private actions to enforce FDA regulations and because state law lacked a parallel duty to file adverse reports with the FDA.[116] Thus, the general scheme of preemption revolves around whether or not a plaintiff's claim is attempting to impose additional legal requirements on a medical device manufacturer.[117]

However, certain exemptions apply to the statute. The statute describes two circumstances, one of which is relevant here, in which an exemption to the preemption clause may apply:

> Upon application of a State or a political subdivision thereof, the Secretary may, by regulation promulgated after notice and opportunity for an oral hearing, exempt from subsection (a) of this section, under such conditions as may be prescribed in such regulation, a requirement of such State or political subdivision applicable to a device intended for human use if (1) the requirement is more stringent than a requirement under this chapter which would be applicable to the device if an exemption were not in effect under this subsection or; (2) the requirement (A) is required by compelling

110. Marmol v. St. Jude Med. Ctr., 132 F. Supp. 3d 1359, 1363–64 (M.D. Fla. 2015).
111. Haidak v. Collagen Corp., 67 F. Supp. 2d 21, 30 (D. Mass. 1999).
112. *See Riegel*, 552 U.S. at 328–31.
113. *Id.* at 321–22.
114. *See id.*
115. *Marmol*, 132 F. Supp. at 1370.
116. *Id.*
117. *See* 21 U.S.C. § 360k(a) (2015).

> local conditions, and (B) compliance with the requirement would not cause the device to be in violation of any applicable requirement under this chapter.[118]

Some of these exemptions include claims alleging manufacturing defect, failure to warn, breach of express warranty, strict liability, negligence,[119] and "unreasonable danger per se."[120] For example, personal injury, product liability, and other state law claims against medical device manufacturers are not preempted, particularly where the requirements of these state law claims were either parallel to or not covered by the MDA.[121] As such, common law claims are preempted only where they might interfere with the specific federal requirements set out in the FDA's product approval process.[122]

In its nonbinding guidelines, the FDA does not enforce the requirement that medical device manufacturers assess cybersecurity risks to their devices. Refusal by the FDA to enforce its guidelines through the MDA premarket approval process—which would require manufacturers to implement the proposed cybersecurity measures if they want their medical devices to be marketed—combined with the MDA preemption clause could leave patients harmed by cyberattacks to their networked devices preempted in their claims. Specifically, because cybersecurity risk assessment is not a statutory requirement within the MDA, a court may hold that patients' claims that attempt to impose liability on a device manufacturer after a cyberattack are barred because the claims would impose legal requirements in addition to or different from current FDA approval standards.[123] The FDA's guidance document provides examples of "intentional" threats to networked medical devices.[124] These examples include hackers, disgruntled employees, and organized crime hackers who will use malware, viruses, or their administrative access to attempt to infiltrate ePHI or attack the personal medical devices of high-profile patients.[125] Consideration of this language when implementing an amendment to the MDA preemption clause may provide plaintiffs an avenue to assert common law claims that arise from cyberattacks on medical devices. By permitting claims that allege a defect in device

118. 21 U.S.C. § 360k(b) (2015).

119. 21 U.S.C. § 360k (2015).

120. *Id.*

121. *See In re* Medtronic, Inc., 592 F. Supp. 1147, 1150 (D. Minn. 2009).

122. *Id.*

123. *See* Riegel v. Medtronic Inc., 552 U.S. 312, 326 (2008) (stating that the preemption clause for medical devices removes all means of judicial recourse for consumers injured by FDA-approved devices).

124. *See* HHS PREMARKET GUIDANCE, *supra* note 9, at 3.

125. *See* Jones, *supra* note 1, at 6, 8.

software or network security, courts could open the door to investigation into the cause of such cyberattacks, incentivizing both sides—patients and manufacturers—to pinpoint cybersecurity vulnerabilities that may then be addressed.

Reducing the breadth of the MDA preemption clause is also expressly supported in *Riegel*, where the Court states:

> [Although] "§360k does not prevent a State from providing a damages remedy for claims premised on a violation of FDA regulations[,]" [t]hat remedy . . . does not help consumers injured by devices that receive FDA approval but nevertheless prove unsafe. The MDA's failure to create any federal compensatory remedy for such consumers further suggests that Congress did not intend broadly to preempt state common-law suits grounded on allegations independent of FDA requirements. It is "difficult to believe that Congress would, without comment, remove all means of judicial recourse" for large number of consumers injured by defective medical devices.[126]

Such a narrowing of the MDA preemption clause would incentivize medical device manufacturers to adhere to the FDA's guidelines more stringently until an appropriate regulatory scheme for networked medical devices is implemented. Providing an exemption to the MDA's preemption clause for private action resulting from an intentional cyberattack on medical devices presents one legal remedy for harm caused by cyberattacks on medical devices.

### *B. Exemption for Insufficient Regulation by the FDA's Premarket Approval Process*

Taking into account the difficulty in identifying who is responsible for cyberattacks on medical devices, it is important that strict regulation of networked medical devices be enforced either by FDA premarket approval and post-market monitoring requirements or by providing an exemption to the MDA's preemption when device regulation is insufficient. The emphasis should be on incentivizing the incorporation of stringent enforcement of cybersecurity standards in the regulation of medical device manufacture and sale, not merely shifting liability for cyberattacks from hackers to medical device manufacturers or hospitals.[127] HIPAA's Security Rule provides useful language for implementing exemptions for preempted plaintiffs harmed by cyberattacks on medical devices where

126. *Riegel*, 552 U.S. at 337 (quoting Silkwood v. Kerr-McGee Corp., 464 U.S. 238, 251 (1984)).

127. *See* Holtzman, *supra* note 98 (stating that more robust regulatory oversight of medical devices is needed in order to minimize cybersecurity risks).

network security was compromised.[128] The security standards provided under Section 164.306 state that

> [c]overed entities . . . must . . . (1) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits[,] (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information[,] [and] (3) [p]rotect against any reasonably anticipated uses or disclosures of such information that are not permitted or required . . . .[129]

While liability in such cases may shift to hospitals maintaining the medical devices' networks, providing legal avenues for plaintiffs may help create a culture of cybersecurity compliance—an industry-wide effort to follow network safety guidelines and address vulnerabilities.[130] Further, language requiring device manufacturers and hospitals to take "reasonable steps" to protect medical devices from security breaches would avoid strict liability, thereby barring imposition of damages on entities that followed prescribed standards.[131] Medical device manufacturers seeking to gain the trust of clients, such as hospitals, in order to sell medical devices, may enter into business associate agreements requiring the manufacturers to continuously monitor their devices in accordance with the FDA's guidelines. As a result, healthcare providers and device manufacturers collaborate to prevent rather than remedy vulnerabilities in their networked devices.

## IV. CRITIQUE AND BENEFITS OF PROPOSED LEGISLATION

Current legal approaches to prosecuting cyberattacks, such as the CFAA,[132] Federal Anti-Tampering Act,[133] or tort law, impose significant burdens of proof on plaintiffs when it comes to attributing responsibility for their harm, which limit their efficacy. Although HIPAA addresses the need for securing ePHI,[134] it does not apply to medical device

128. 45 C.F.R. § 164.306 (2004).

129. *Id.*

130. FDA GUIDANCE ON OTS SOFTWARE DEVICES, *supra* note 16, at 3–5 (encouraging medical device manufacturers to engage in timely preventive actions regarding software vulnerabilities and work with third parties, including healthcare organizations, to perform software maintenance and address vulnerabilities).

131. *Privacy Basics: A Quick HIPAA Check for Medical Device Companies*, MED. DEVICE & DIAGNOSTIC INDUSTRY (Aug. 1, 2009), http://www.mddionline.com/article/privacy-basics-quick-hipaa-check-medical-device-companies [https://perma.cc/PL9W-YA5J].

132. 18 U.S.C. § 1030 (2011).

133. 18 U.S.C. § 1365 (2012).

134. 45 C.F.R. § 164.312 (2010).

manufacturers or all medical devices without an explicit agreement.[135] The FDA's current nonbinding guidelines for medical device manufacturers provide a strong regulatory framework but are expressly not enforced.[136] The FDA refraining from exercising its regulatory authority over medical devices could result in preemption of common law claims brought by persons injured by an attack that compromised the function of their medical device because of the precedent set by *Riegel*.[137]

Allowing injured plaintiffs to seek reasonable legal remedy via the MDA preemption exemption is the best way to address existing gaps within our legal framework until better avenues of tracing malicious actors and securing such devices are available. Technologies currently in development may render devices ranging from pacemakers to cars unhackable.[138] However, implementation of such technologies may be years away,[139] and our legal system must move with technology—especially in the field of healthcare and networked medical devices.[140]

It is undeniable that allowing damages claims by patients harmed as a result of cyberattacks on their medical devices would lead to an increase in litigation and a strain on judicial resources. For this reason, in addition to those discussed previously, an enforceable regulatory framework for networked medical devices would promote the proactive safety culture[141] sought by the FDA's guidance documents.[142] Therefore, while narrowing the MDA's preemption clause to provide legal means of addressing patient

---

135. *Privacy Basics*, *supra* note 131.

136. Holtzman, *supra* note 98.

137. *See* Riegel v. Medtronic, Inc., 552 U.S. 312, 330 (2008) (stating that the MDA preempts claims "'different from, or in addition to' the requirements imposed by federal law").

138. Michael Slezak, *Unhackable Kernel Could Keep All Computers Safe From Cyberattack*, NEW SCIENTIST (Sept. 16, 2016), https://www.newscientist.com/article/mg22730392-600-unhackable-kernel-could-keep-all-computers-safe-from-cyberattack-2/ [https://perma.cc/D3RK-A8W4] (discussing the seL4 kernel, which provides the ability to keep operating systems separate to prevent hackers from accessing critical parts of a computer's hardware).

139. *Id.* (citing a researcher's statement that "[m]y hope is that in 10 years' time, anything that is security critical is running on our system or some other one built on the principles we've established").

140. *See* Jof Enriquez, *Next Big Cybersecurity Threat to Medical Devices: Ransomware*, MED DEVICE ONLINE (Nov. 20, 2015), http://www.meddeviceonline.com/doc/next-big-cybersecurity-threat-to-medical-devices-ransomware-0001[https://perma.cc/8KDR-ZT9F] (stating that the healthcare industry is only in its initial stages of dealing with the implementation of cybersecurity measures that have been commonplace in cyberspace for over a decade).

141. *See* HHS POSTMARKET GUIDANCE, *supra* note 26, at 6 (noting that "a proactive and risk-based approach" to medical devices in the market should include cybersecurity data sharing and monitoring, routine network maintenance, and evaluating vulnerabilities so that risks that could impact patients can be mitigated).

142. *See generally* HHS PREMARKET GUIDANCE, *supra* note 9; HHS POSTMARKET GUIDANCE, *supra* note 26.

harms caused by cyberattacks is one solution to the problem of cyberattacks on medical devices, its retroactive nature presents the same flaw as the FDA's adverse event reporting scheme in that it will not deter cyberattacks, only seek to punish those after they have committed the offense.

## CONCLUSION

Even though cyberattacks on medical devices may currently seem like a fictive scheme meant to frighten the general public, the reality is that hackers were able to commandeer medical devices years ago,[143] and more cyberattacks could occur before any legal remedies have been established. As such, the need for more stringent FDA regulation and legal avenues for prosecuting cyberattacks is undeniably urgent.

Since the FDA regulates devices currently in the market mainly through adverse event reporting, networked devices that were subject to cyberattacks should be included in an exemption to the MDA preemption clause where unsecure networked medical devices are involved. Until better technological and legal avenues exist for attributing cyberattacks on medical devices to the actual attackers, our legal system must provide adequate remedies to persons who sustain loss of health or life as a result of such attacks, even if that means holding device manufacturers accountable to a high standard of care in maintaining cybersecurity. In addition, the potential liability of manufacturers and hospitals could promote information sharing within the healthcare and tech communities where network vulnerabilities and mitigation tactics are of concern. The FDA's guidelines point to the importance of employing cybersecurity experts to test network vulnerabilities and sharing the information gathered so that the safety of medical devices, and ultimately patients, may be efficiently promoted.[144] Therefore, a regulatory incentive for manufacturers and technology companies to collaborate in matters of cybersecurity could move the future of healthcare in a positive direction.

Cyberattacks in the healthcare field are no longer a fictive futuristic threat; they are a reality that can no longer be left to the technology industry. The time has come for our government and regulatory agencies to address this issue through legislation and enforcement.

---

143. *See* Reel, *supra* note 7.

144. *See generally* HHS PREMARKET GUIDANCE, *supra* note 9; *see also* HHS POSTMARKET GUIDANCE, *supra* note 26.