South Carolina Law Review

Volume 71 | Issue 1 Article 4

Fall 2019

When "Things" Go Wrong: Redefining Liability for the Internet of Medical Things

Bethany A. Corbin
Wake Forest University School of Law

WHEN "THINGS" GO WRONG: REDEFINING LIABILITY FOR THE INTERNET OF MEDICAL THINGS

Bethany A. Corbin*

---

* Certified Information Privacy Professional (CIPP/US), Certified in Healthcare Compliance (CHC), and Certified in Healthcare Privacy Compliance (CHPC); Director, Wake Forest University School of Law, Master of Studies in Law Program; Health Care LL.M., 2018, Loyola University Chicago School of Law; J.D., 2013, Wake Forest University School of Law.

I. INTRODUCTION

The technological landscape of the healthcare industry is evolving at a rapid and unprecedented pace.[1] Increasingly dominated by connected medical devices, the healthcare sector is in the midst of a massive transformation to its approach to patient outcomes and value-based care.[2] Medical technology (MedTech), situated at the heart of this revolution, has the potential to significantly improve healthcare efficiency, convenience, and patient comfort, while also positively impacting quality of life.[3] However, MedTech is not without its vulnerabilities, and as connected medical devices become the norm in patient care settings, the risks for hacking and malicious attacks on these devices increase exponentially.[4]

As the new frontiers of MedTech continue to expand, one particular sector of the digital health industry has garnered significant attention: The Internet of Medical Things (IoMT). At its most basic, IoMT refers to the ability of healthcare devices to communicate, gather, and exchange data across WiFi and Internet platforms.[5] These devices can provide up-to-date patient information, enhance patient self-sufficiency, and decrease the cost of care.[6] WiFi-connected pacemakers, insulin pumps, and pill-shaped cameras are only the most recent examples of what this technology is projected to accomplish.[7] By 2025, experts estimate the impact of IoMT on the healthcare industry will

---

1. *How Technology is Changing Healthcare*, TEX. HEALTHCARE (Aug. 1, 2016), http://www.txhealthcare.com/health-news/how-technology-is-changing-healthcare/58/ [https://perma.cc/CTC7-MLB6].

2. *See* KAREN TAYLOR, DELOITTE CENTRE FOR HEALTH SOLS., CONNECTED HEALTH: HOW DIGITAL TECHNOLOGY IS TRANSFORMING HEALTH AND SOCIAL CARE 4–11 (2015).

3. *See* MARIE-VALENTINE FLORIN, GOVERNING CYBER SECURITY RISKS AND BENEFITS OF THE INTERNET OF THINGS: APPLICATION TO CONNECTED VEHICLES AND MEDICAL DEVICES 5, 7 (Maya Bundt et al. eds., 2016).

4. Alaap Shah, *Death by a Thousand Cuts: Cybersecurity Risk in the Health Care Internet of Things*, AM. HEALTH LAWS. ASS'N WKLY. (May 18, 2018), https://www.ebglaw.com/content/uploads/2018/05/AHLA-Weekly-Cybersecurity-IOT-Alaap-Shah-May-2018.pdf [https://perma .cc/UGN5-W9TQ]; *Untangling the Web of Liability in the Internet of Things*, MASON HAYES & CURRAN: TECH L. BLOG (May 19, 2016) [hereinafter *Untangling the Web*], https://www.mhc.ie/latest/blog/untangling-the-web-of-liability-in-the-internet-of-things [https://perma.cc/XWB3-6ED9].

5. Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 33 (2016).

6. *Id.* at 32–33; *see also* Bernard Marr, *Why The Internet of Medical Things (IoMT) Will Start to Transform Healthcare in 2018*, FORBES (Jan. 25, 2018), https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#1d1f6e3d4a3c [https://perma.cc/Y4VQ-F222].

7. Paez & La Marca, *supra* note 5, at 32.

range from $1.1 trillion to $2.5 trillion per year, mostly stemming from improved efficiency in treating chronically ill patients.[8]

As a subset of the Internet of Things (IoT), the IoMT ecosystem is unique from prior technology in that it "hinges on the interconnectivity of countless devices and participants," which requires the legal framework governing IoMT to account for the rights, responsibilities, and obligations of numerous stakeholders.[9] Given the nascent stage of IoMT, however, a comprehensive legal and liability structure does not yet exist for hacks, breaches, and hijacks of IoMT devices that cause harm to patients.[10] Privacy and security regulations in the United States are sectoral and patchwork in nature, and those applicable to the healthcare sector have not been regularly updated to reflect the technological innovation associated with digital health.[11] As a result, significant gaps exist in healthcare regulations for IoMT devices, with some aspects of the industry completely unregulated.[12]

Compounding this issue of non-regulation is the lack of a comprehensive liability framework for patients to follow if their IoMT device is hacked or malfunctions.[13] With numerous developers, suppliers, and manufacturers involved in the IoMT supply chain, it can be difficult for patients to identify the culpable party and apply existing liability standards to innovative technology.[14] While products liability currently serves as the primary vehicle for restitution if a device malfunctions, its application to IoMT is imperfect at best.[15] Apportioning liability between software and device manufacturers in an IoMT product can be difficult, and there are no clear boundaries to establish

---

8. *Id.* at 33.

9. *Id.* at 30.

10. *Id.* at 29; *see also* H. Michael O'Brien, *The Internet of Things and the Inevitable Collision with Product Liability PART 4: Government Oversight*, PROD. LIAB. ADVOC. (Oct. 16, 2015), https://www.productliabilityadvocate.com/2015/10/the-internet-of-things-and-the-inevitable-collision-with-product-liability-part-4-government-oversight/ [https://perma.cc/R9YR-P5W5].

11. Paez & La Marca, *supra* note 5, at 40.

12. PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., NSTAC REPORT TO THE PRESIDENT ON THE INTERNET OF THINGS 6 (Nov. 19, 2014); Nikole Davenport, *Smart Washers May Clean Your Clothes, But Hacks Can Clean Out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 260 (2016).

13. SALEN CHURI ET AL., UNIV. CHI. L. SCH., INTERNET OF THINGS (IOT) RISK MANAGER CHECKLIST, U.S. 4 (2017).

14. *See* BENJAMIN C. DEAN, AN EXPLORATION OF STRICT PRODUCTS LIABILITY AND THE INTERNET OF THINGS 12–13, 21 (2018). *See generally Untangling the Web*, *supra* note 4 ("Lawmakers and regulators will need to consider either new forms of liability, or new ways to manage and apply existing laws to different entities in the IoT supply chain.").

15. *See* DEAN, *supra* note 14, at 16; Paez & La Marca, *supra* note 5, at 58.

which party is at fault for a hack or breach.[16] Moreover, defect-free software does not exist, which complicates the application of strict products liability to software companies (assuming embedded software can even be considered its own separate product to trigger application of products liability standards).[17]

Further, the prevalence of end-user licensing agreements operates as a contractual tool to limit manufacturer liability for unsecure devices.[18] These agreements, which appear in many IoMT products and disclaim all liability for software failures, shift the risk of harm almost exclusively to consumers, and eliminate the burden for manufacturers to comply with industry best practices for cybersecurity and privacy.[19] The presence of these agreements hinders consumers' ability to bring product liability or breach of warranty actions, making restitution and recovery all but moot points.[20] Combined with the restrictions of the economic loss doctrine, which precludes tort recovery for purely financial harm, products liability (in its current form) is an almost unworkable liability structure for IoMT devices.[21] Not to mention, the products liability model risks exposing healthcare providers and IoMT device manufacturers to unbounded liability despite the lack of mandatory federal cybersecurity guidance and adherence to industry cybersecurity frameworks.[22]

Given the projected growth in the IoMT market over the coming years, new or revised liability models will undoubtedly develop as cases make their

---

16. *See Untangling the Web*, *supra* note 4.

17. *See* DEAN, *supra* note 14, at 17, 19; Paez & La Marca, *supra* note 5, at 59; Jon Evans, *Should Software Companies Be Legally Liable for Security Breaches?*, TECH CRUNCH (Aug. 6, 2015), https://techcrunch.com/2015/08/06/should-software-companies-be-legally-liable-for-security-breaches/ [https://perma.cc/FV86-2HY3].

18. *See* Robert Lemos, *Security Liability is Coming for Software: Is Your Engineering Team Ready?*, TECH BEACON, https://techbeacon.com/software-security-liability-coming-are-your-engineers-ready [https://perma.cc/G22R-XA2C].

19. Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 427 (2008); Paul Rosenzweig, *The Evolving Landscape of Cybersecurity Liability*, CHERTOFF GROUP (June 29, 2017), https://www.chertoffgroup.com/blog/the-evolving-landscape-of-cybersecurity-liability [https://perma.cc/TXE6-JV3Y].

20. Dawn Beery & Kevin Burns, *The Application of Traditional Product Liability Law to Emerging Technologies*, DEFENSE, Apr. 2018, at 58.

21. *Id.* at 55; *see also* Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J.L. REFORM 913, 915, 926–27 (2017).

22. *See generally* Jack Detsch, *Should Companies Be Held Liable for Software Flaws?*, CHRISTIAN SCI. MONITOR (Dec. 2, 2016), https://www.csmonitor.com/World/Passcode/2016/1202/Should-companies-be-held-liable-for-software-flaws [https://perma.cc/8HGP-CW3K] (discussing the benefits and drawbacks of holding companies liable for software flaws).

way through the court system.[23] As liability standards evolve, there must be an increased recognition that healthcare organizations and IoMT manufacturers are victims of cyberattacks and heightened emphasis should be placed on the proactive adoption of cybersecurity best practices.[24] That said, there is also a need to counterbalance these considerations against the requirements of patient safety and secure medical devices.[25] The existing regulatory gaps and liability frameworks have resulted in insufficient incentives to ensure adequate security measures are implemented into IoMT software to protect patients from hacks, hijacks, and breaches.[26] In a climate where a breach or hack can produce life or death consequences, it is imperative to develop well-defined security standards and liability expectations.[27]

Although it is impossible to predict at this stage the form of any new IoMT liability structure, two proposals merit consideration as incremental steps towards the new liability framework. First, end-user agreements that limit a software manufacturer's liability for vulnerable code should be prohibited in the IoMT context.[28] The unique risk of bodily harm posed by certain IoMT devices requires a corresponding liability system that will hold software manufacturers accountable for their failure to implement security best practices.[29] End-user agreements operate as an impediment to this goal

---

23. *See generally* Mildred Segura et al., *The Internet of Medical Things Raises Novel Compliance Challenges*, MED. DEVICE ONLINE (Jan. 3, 2018), https://www.meddeviceonline.com/doc/the-internet-of-medical-things-raises-novel-compliance-challenges-0001 [https://perma.cc/D7TV-NX3W] (acknowledging with the growth of IoMT manufacturers should "keep abreast of current minimum-security standards" to avoid lawsuits); *Untangling the Web*, *supra* note 4.

24. *See* MEGAN BROWN ET AL., CYBER IMPERATIVE: PRESERVE AND STRENGTHEN PUBLIC-PRIVATE PARTNERSHIPS 12 (2018).

25. *See* Detsch, *supra* note 22.

26. *See generally* Charlie Mitchell, *Mark Warner Eyes Liability for Software Developers as Key Way to Shore up Cybersecurity*, WASH. EXAMINER (Apr. 10, 2018), https://www.washingtonexaminer.com/policy/technology/mark-warner-eyes-liability-for-software-developers-as-key-way-to-shore-up-cybersecurity [https://perma.cc/LAT8-DBY2].

27. *See Untangling the Web*, *supra* note 4.

28. *See* Lemos, *supra* note 18; *see also* Matthew Ashton, Note, *Debugging the Real World: Robust Criminal Prosecution in the Internet of Things*, 59 ARIZ. L. REV. 805, 834 (2017); Mitchell, *supra* note 26.

29. *See generally* Mitchell, *supra* note 26 (suggesting a cybersecurity doctrine should be implemented to include software liability); Detsch, *supra* note 22 ("[L]eading digital security experts are calling on US policymakers to hold manufacturers liable for software vulnerabilities in their products in an effort to prevent the bugs commonly found in smartphones and desktops from pervading the emerging IoT space.").

and shield software developers from accountability.[30] Software companies would almost certainly resist this course of action with a stringent warning that such liability would open the floodgates for judicial lawsuits and stifle innovation in a developing industry.[31] Thus, a second proposal should be simultaneously implemented that guards against unfettered liability for IoMT device manufacturers that adopt cybersecurity best practices.[32] Specifically, a "safe harbor" statute should be adopted that limits civil liability if IoMT manufacturers and software companies comply with voluntary, industry-approved cybersecurity frameworks.[33] These proposals help balance incentives with punishment and can result in safer IoMT products for patients.[34]

Further, by implementing small changes to the IoMT liability structure at this stage—without waiting for a liability scheme to be developed exclusively by the federal or state legislatures or the courts—IoMT companies and healthcare organizations can contribute to the dialogue on what an end-stage liability framework should entail.[35] Removing the protection afforded through end-user agreements can incentivize IoMT manufacturers to help form liability standards and best practice expectations that will continue to govern this evolving industry through public-private stakeholder participation.[36] These companies may additionally be motivated to adopt and adhere to existing cybersecurity frameworks, which may reduce the companies' compliance burden when new IoMT-specific standards are eventually promulgated.

---

30. *See* Mitchell, *supra* note 26.

31. *See id.*; John Daley, Note, *Insecure Software is Eating the World: Promoting Cybersecurity in an Age of Ubiquitous Software-Embedded Systems*, 19 STAN. TECH. L. REV. 533, 542 (2016) ("Critics will contend that any liability borne by software vendors will extinguish the vibrant startup ecosystem.").

32. *See* Daley, *supra* note 31, at 541.

33. *See generally id.* (describing an alternate safe harbor model); Mauricio Paez & Kerianne Tobitsch, *The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues*, 62 N.Y.L. SCH. L. REV. 217, 228 (2018); Scott Wenzel, *Not Even Remotely Liable: Smart Car Hacking Liability*, 2017 U. ILL. J.L. TECH. & POL'Y 49, 69.

34. *See generally* Daley, *supra* note 31, at 541 (discussing the need to incentivize cybersecurity practices and proposing a separate safe-harbor liability structure).

35. *See generally* Mitchell, *supra* note 26 (explaining that a dialogue must be started on incentivizing software companies to develop secure code, and liability may contribute to this incentive model); Paul Merrion, *Litigation Key to Securing Internet of Things, Capitol Hill Staffers Told*, CQ ROLL CALL, June 8, 2017, 2017 WL 2470487.

36. *See generally* Mitchell, *supra* note 26 (relying on software maker's user license agreements, courts have found in favor of software developers in civil suits); Merrion, *supra* note 35.

To support this two-pronged proposal, this Article proceeds in four parts. Part II offers a succinct introduction to IoMT, including the mechanics of how IoMT works and the benefits and vulnerabilities associated with these devices. Part III then explains the need to incentivize safer coding in these devices, focusing particularly on regulatory gaps for IoMT accountability and liability. This part highlights the strengths and weaknesses of regulations promulgated by the Department of Health and Human Services (HHS) and the Food and Drug Administration (FDA), along with the development and role of voluntary, industry-developed cybersecurity frameworks. Part IV discusses the need for a comprehensive liability framework to incentivize safer coding, describing why current liability structures are insufficient to govern and mitigate the risks posed by these digital health devices. This part presents the benefits and drawbacks of implementing the two-pronged liability model and articulates why such revisions are urgently needed in the IoMT industry. Finally, Part V concludes the Article.

II. UNDERSTANDING IOMT: BACKGROUND, BENEFITS, AND VULNERABILITIES

The technological revolution has taken the healthcare sector by storm.[37] Once perceived as mere science fiction, digital health has transformed imagination into reality with the advent of implantable, Internet-connected medical devices that not only monitor patient health, but also gather and exchange data across wireless networks with little human involvement.[38] Revolutionizing both patient behavior and the practice of medicine, the "smart" medical device industry is projected to be worth over $66 billion by 2024.[39] Indeed, experts anticipate that by 2026, approximately one-third of Americans will have either temporary or permanent healthcare devices in their bodies.[40] As the human body becomes increasingly connected to the Internet—a phenomenon that some deem the "next logical frontier" of digital health—it is crucial to understand the benefits and vulnerabilities of this

37. *Untangling the Web*, *supra* note 4; *see* Paez & Tobitsch, *supra* note 33, at 238; *see also*; Davenport, *supra* note 12, at 260; Shah, *supra* note 4 (explaining that "[h]ealth care continues to undergo lightning-fast transformation," particularly as it "enter[s] the brave new world of the Internet of Things").

38. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 92 (2014).

39. Tarifa B. Laddon & Blake A. Angelino, *Medical Device Litigation: The "Internet of Things is Coming,"* IN-HOUSE DEF. Q., Summer 2017, at 26, 26.

40. Amelia R. Montgomery, Note, *Just What the Doctor Ordered: Protecting Privacy Without Impeding Development of Digital Pills*, 19 VAND. J. ENT. & TECH. L. 147, 148 (2016).

technology.[41] This part discusses the advancement of the MedTech industry, including the evolution of IoMT, and explores the drivers and risks associated with using connected medical devices.

A. What's in a Name?: Understanding and Defining the Internet of Medical Things

In the past five years, the MedTech industry has experienced exponential growth, fueled primarily by a corresponding advancement in the Internet of Things.[42] As the name suggests, IoT represents a network of smart devices that collect and exchange personal data over the Internet.[43] While no universally accepted definition for IoT exists, the term refers to the general interaction between computers, sensors, and objects to collect and transfer information through a wireless data infrastructure.[44] These devices "operate on embedded sensors that automatically measure and transfer data (i.e., environmental and activity information) over a network to data stores without human interaction."[45] Breaking this down, IoT devices function in three stages.[46]

First, IoT devices are embedded with radio-frequency identification (RFID) sensors, which use radio waves to identify people and objects.[47] These embedded sensors enable IoT devices to detect and gather data from their hosts and surrounding environment, including the individuals who operate the devices.[48] Next, the IoT device transmits this data through WiFi, Bluetooth, mobile phone networks, or the Internet, where the data is stored using cloud-based applications.[49] Finally, end-users sift through the "massive troves of

---

41. *Id.*

42. Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 ANNALS HEALTH L., Winter 2017, at 1, 1.

43. Leta E. Gorman, *The Era of the Internet of Things: Can Product Liability Laws Keep Up?*, 84 DEF. COUNS. J. 1, 1 (2017).

44. *See id.* at 1–2; Davenport, *supra* note 12, at 261; *see also* Alan M. Winchester & Jaime L. Regan, *Attacking Justiciability of Cybersecurity Claims in the Product Liability Context*, DEFENSE, Nov. 2015, at 84, 87 (2015) (discussing the definition of IoT).

45. Gorman, *supra* note 43, at 1–2; *see also* Dalmacio V. Posadas, Jr., *After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 75 (2017) (explaining the collection of data).

46. *See* Paez & La Marca, *supra* note 5, at 31; Posadas, *supra* note 45, at 76–77.

47. *See* Posadas, *supra* note 45, at 76–77; *Frequently Asked Questions*, RFID J., http://www.rfidjournal.com/site/faqs#Anchor-What-363 [https://perma.cc/T4J2-TSYG].

48. Paez & La Marca, *supra* note 5, at 31; Posadas, *supra* note 45, at 76–77.

49. Paez & La Marca, *supra* note 5, at 31; Posadas, *supra* note 45, at 76.

data" collected from these devices.[50] This data is analyzed for insights, trends, and intelligence that can guide future decision-making and increase productivity, safety, and efficiency.[51]

In the healthcare industry, IoT operates by creating a network of medical devices that connect to healthcare information technology (IT) systems.[52] Known as IoMT, this network uses technology to enhance information and data flow between patients and physicians.[53] The most obvious examples of IoMT involve connected medical devices that are used to track patient progress and manage chronic illness.[54] These well-known devices include pacemakers, blood pressure monitors, intravenous fluid pumps, defibrillators, ingestible pill cameras, blood glucose monitors, imaging and scanning equipment, and electrocardiogram devices.[55] While IoT is relatively new to the healthcare context, it has been described recently as "permeat[ing] nearly every sector of the healthcare industry."[56]

B. Encouraging Innovation: IoMT Benefits

The benefits of IoMT in the healthcare sector are promising and are a major factor driving increased adoption of connected medical technology.[57] These benefits fall into three broad categories: (1) remote monitoring and telehealth; (2) behavioral modification and patient outcomes; and (3) administrative efficiency.[58] First, IoMT benefits patients and providers by transforming the landscape of telemedicine and enabling remote monitoring.[59] Remote monitoring allows providers to establish a constant connection with patients anywhere in the world, which assists with monitoring acute and

---

50. Paez & La Marca, *supra* note 5, at 31.

51. *Id.*

52. *See* FLORIN, *supra* note 3, at 8; Segura et al., *supra* note 23; Shah, *supra* note 4.

53. *See* Segura et al., *supra* note 23.

54. *See id.*

55. *Id.*; *see* Paez & La Marca, *supra* note 5, at 31–33; Gorman, *supra* note 43, at 7; Sarah Knapton, *Terrorists Could Hack Pacemakers Like In Homeland, Say Security Experts*, TELEGRAPH (Nov. 6, 2014), https://www.telegraph.co.uk/news/science/science-news/11212777/Terrorists-could-hack-pacemakers-like-in-Homeland-say-security-experts.html [https://perma.cc/N4JY-LL76].

56. Segura et al., *supra* note 23; *see also* Paez & La Marca, *supra* note 5, at 29 (supporting the emergence of IoT).

57. *See* Segura et al., *supra* note 23.

58. *See id.*

59. *See id.*; *see also* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 7–8 (2015).

chronic conditions.[60] Platforms such as e-mail, video conferencing, texting, and patient portals enable health care to transcend the physical bounds of the provider's office and provide care to patients when it is most convenient and necessary.[61]

Second, IoMT encourages behavioral modifications for patients, particularly those with chronic illnesses, and has the potential to improve patient outcomes.[62] With connected devices, patients can manage their medical conditions at home, and have data transmitted to their providers automatically.[63] This offers patients a sense of responsibility and accountability for their health, and provides an incentive to take medication and perform necessary testing.[64] For example, ingestible pill sensors are being developed that notify healthcare providers when medication is taken.[65] Given that more than 20% of prescriptions are never filled, a doctor may refuse to order medication refills or increase medication dosages if she learns that a patient is not taking her medication consistently.[66] Patients, therefore, have more motivation to follow their medical plans when their activities will be reported to their healthcare providers.[67]

Finally, IoMT enhances administrative efficiency and operations.[68] Numerous medical tasks may be automated, and patient data can be gathered from various sources, even when the patient is not present in the doctor's

60. *See* Segura et al., *supra* note 23; *see* FED. TRADE COMM'N, *supra* note 59, at 7.

61. *See* Gorman, *supra* note 43, at 2 (noting the decreased need of human interaction); Segura et al., *supra* note 23 ("As the IoMT streamlines telemedicine, the physical office is becoming less critical for routine appointments, because patients can now communicate with their doctors via phone and video conference, as well as get prescription orders re-filled—all without leaving their homes, and at reduced cost.").

62. *See* FED. TRADE COMM'N, *supra* note 59, at 2, 7–8.

63. *Id.* at 7 ("For example, insulin pumps and blood-pressure cuffs that connect to a mobile app can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office.").

64. *See, e.g.*, Hendrik Sybrandy, *Doctors Hope New Digital Pill Will Encourage Medication Adherence*, CGTN: AMERICA (Aug. 5, 2018), https://america.cgtn.com/2018/08/05/doctors-hope-new-digital-pill-will-encourage-medication-adherence [https://perma.cc/TT3N-3CYR].

65. *See id.*

66. *See id.*; Andrea B. Neiman et al., *CDC Grand Rounds: Improving Medication Adherence for Chronic Disease Management–Innovations and Opportunities*, 66 CDC MORBIDITY & MORTALITY WKLY. REP. 1241, 1248 (2017).

67. *See* Sybrandy, *supra* note 64.

68. *See* FLORIN, *supra* note 3, at 5 (explaining that IoT can "improve performance and reduce inefficiencies in numerous sectors").

office.[69] Connected medical devices may run more efficiently and offer increased reliability with the potential to identify errors and mistakes more quickly than human providers.[70] In some instances, connected medical devices may even be able to warn providers of potential failure indicators before they occur.[71] Moreover, IoMT can encourage the development of innovative services and more efficient use of organization infrastructure.[72] For example, a hospital in Orlando, Florida used IoMT to develop a real-time location system in which family members can track the progress of a loved one undergoing surgery.[73] Similarly, a separate hospital in Waterbury, Connecticut used IoMT to analyze workflow trends with the goal of identifying staffing needs for each shift.[74] Use of IoT data saved the hospital $650,000 in just six months by reducing unnecessary overtime.[75] Thus, IoMT may be used by patients and healthcare providers to streamline and enhance healthcare delivery.

C. The Flip Side of Progress: IoMT Vulnerabilities

While IoMT has the potential to revolutionize patient care, the heightened connectivity of medical devices raises questions regarding patient security, network and data privacy, long-term maintenance, and device resilience.[76] In its 2014 *NSTAC Report to the President on the Internet of Things*, the President's National Security Telecommunications Advisory Committee explained that the risks accompanying IoMT devices include "new attack vectors, new vulnerabilities, and perhaps most concerning of all, a vastly increased ability to use remote access to cause physical destruction."[77] Although this list is not exhaustive, it highlights three areas of vulnerability

---

69. *See* Paez & La Marca, *supra* note 5, at 34; FED. TRADE COMM'N, *supra* note 59, at 7–8.

70. PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 12, at 5.

71. *Id.*

72. *Id.* at ES-1; *see* Shah, *supra* note 4 ("Health care organizations often pursue IoT efforts to find novel ways to engage patients, monitor health status, derive insights from clinical data, and advance care management and population health.").

73. Segura et al., *supra* note 23.

74. *Id.*

75. *Id.*

76. *See* SANDRA BURMEIER ET AL., SWISS RE SONAR–NEW EMERGING RISK INSIGHTS 11 (Urs Leimbacher et al. eds., 2015); *see also* PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 12, at ES-1 (noting additional possible risks).

77. PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 12, at ES-1.

that warrant discussion: (1) personal privacy and security; (2) network privacy and security; and (3) safety risks.[78]

First, IoMT presents an inherent risk of data breach that can expose sensitive user information.[79] Of particular concern is that many IoMT devices connect over unsecure networks, or networks with weak password protections.[80] Wireless transmission of data through these channels creates access points for hackers to compromise device security and privacy.[81] When such a device is compromised, sensitive patient health data may be shared publicly, resulting in a violation of individual privacy.[82] Given that healthcare data is highly coveted on the black market—medical records alone are 20 to 50 times more valuable than financial data—there is no shortage of bad actors attempting to hack unsecure medical devices.[83] Further, as discussed in Part III, numerous IoMT device manufacturers may fall outside the confines of federal regulation, which can disincentivize adoption of secure technology.[84] Consumers may not recognize the inherent risks associated with IoMT device use, believing their health data to be secure in the cloud.[85]

Second, IoMT exponentially expands the attack surface from which unauthorized users can gain entry into broader medical networks.[86] Each IoMT device that a healthcare operator places on its IT network has the potential to serve as a backdoor entry point into the entire healthcare system.[87] The mere presence of IoMT devices in a healthcare setting weakens the overall security of the network and creates access points that must be monitored by IT professionals.[88] Any unlawful hack or breach of an IoMT

78. *See* FED. TRADE COMM'N, *supra* note 59, at 10.

79. Gorman, *supra* note 43, at 3; Paez & La Marca, *supra* note 5, at 37–40.

80. *See* O'Brien, *supra* note 10; Kathryn R. Coburn, *The Internet of Medical Things: Scientific and Technical Innovations Predict, Preempt, and Treat Disease*, SCITECH L., Spring 2016, at 18, 19 (2016) ("Data in the IoMT is not secure."); *see also* FED. TRADE COMM'N, *supra* note 59, at 12 (discussing the exploitation of vulnerabilities in devices).

81. Coburn, *supra* note 80, at 19; Paez & La Marca, *supra* note 5, at 46.

82. Gorman, *supra* note 43, at 3; Paez & La Marca, *supra* note 5, at 39.

83. Clemens Scott Kruse et al., *Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends*, TECH. & HEALTH CARE, Aug. 19, 2016, at 1, 6; Tschider, *supra* note 42, at 8.

84. *See* Ashton, *supra* note 28, at 834; Paez & Tobitsch, *supra* note 33, at 240.

85. *See* Ashton, *supra* note 28, at 834 ("[T]he average consumer tends to undervalue the security of Internet-based products.").

86. FLORIN, *supra* note 3, at 18; PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 12, at 6.

87. *Cf.* PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 12, at 1 (discussing the growing threat caused by the expansion of interconnected IoT devices).

88. *See id.* at 6, 12.

device has the potential to not only expose the sensitive health data of its user but also the data of other patients stored on the broader healthcare network.[89] Hackers can even negatively impact organizational operations by encrypting patient and administrative data and demanding a ransom for the encryption key.[90] Without access to its data, a healthcare organization cannot function efficiently, and cannot confirm patient treatment plans.[91]

Finally, because IoMT operates as a portal between cyberspace and humans, it has the potential to inflict bodily harm or death that may not be present with other IoT applications.[92] As showcased in a 2012 episode of *Homeland*, implantable IoMT devices may be hacked to cause the device to purposefully malfunction.[93] Former Vice President Dick Cheney had the remote capabilities for his pacemaker disabled after research identified vulnerabilities that could enable hackers to cause heart attacks remotely.[94] Similarly, researchers and white hat hackers have showcased their ability to hack insulin pumps from a remote location and alter the device's settings to either deny delivery of medicine completely, or provide excessive insulin.[95] In 2014, the Federal Bureau of Investigations even warned hospitals to discontinue using certain infusion pumps designed with a security flaw that could allow an unauthorized user to alter medication dosages remotely.[96] Therefore, unlike other technologies, IoMT creates the possibility for significant human harm if a device is hacked or malfunctions.[97] These risks cannot be ignored when evaluating device security.

---

89. *See* FLORIN, *supra* note 3, at 18.

90. Charlie Osborne, *U.S. Hospital Pays $55,000 to Hackers after Ransomware Attack*, ZDNET (Jan. 17, 2018), https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/ [https://perma.cc/KYN7-42FK].

91. *See id.*

92. FLORIN, *supra* note 3, at 5; *see* Gorman, *supra* note 43, at 3; Paez & La Marca, *supra* note 5, at 48 ("[A] breach of an IoT object can also result in significant bodily harm."); Peppet, *supra* note 38, at 134 ("[I]nsulin pumps have been shown to be vulnerable to hacking."). *See generally* Detsch, *supra* note 22 (referencing the risks of injury from IoT).

93. Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST: THE SWITCH (Oct. 21, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/?utm_term=.bf1506f843d8 [https://perma.cc/N59Z-96KB].

94. *Id.*; *see* Trevor Weyland, *Medical Device Cybersecurity*, GALLAGHER HEALTHCARE: INDUSTRY INSIGHTS BLOG (May 19, 2016), https://www.gallaghermalpractice.com/blog/post/medical-device-cybersecurity [https://perma.cc/B7VY-TUPV] ("In 2015, students at the University of Alabama hacked the pacemaker implanted in an iStan (a robotic dummy patient used to train medical students) and were able to speed up its heart rate.").

95. Paez & La Marca, *supra* note 5, at 48, *supra* note 59, at 12; Weyland, *supra* note 94.

96. Weyland, *supra* note 94.

97. *See* Paez & La Marca, *supra* note 5, at 48.

III. THE NEED TO INCENTIVIZE SAFER CODING FOR IOMT DEVICES

Despite the serious risks accompanying IoMT, the industry has experienced impressive and sustained growth that far outpaces the federal legislature's adoption of safety and security regulations.[98] Existing laws and regulations do not sufficiently capture and mitigate the risks associated with digital technology, and require substantial updates to eliminate gaps in their applicability and coverage.[99] Indeed, due to the healthcare industry's slow adoption of MedTech at the beginning,[100] cybersecurity infrastructure and corresponding regulatory frameworks for IoMT are only in the nascent stages.[101] Further, IoMT manufacturers are not emphasizing safe coding practices, focusing instead on a "race to market" strategy that may result in unsafe consumer products.[102] This part explains the need to incentivize safer coding in IoMT devices, with particular emphasis on: (1) the regulatory gaps that enable IoMT device manufacturers to operate outside the bounds of regulatory authority; and (2) the economic realities of device creation that prioritize the "race to the market." Specifically, Part III explains why existing privacy and security standards are insufficient to comprehensively regulate the IoMT sector and clarify liability structures. Although state regulations also exist on this topic, they are beyond the scope of this Article.

A. Regulatory Gaps: Evaluating the Roles of HHS and FDA

MedTech in the United States does not operate in a wholly unregulated environment.[103] Rather, the United States has implemented a patchwork and sector-based framework to govern privacy and security throughout the nation.[104] In the healthcare industry, this regulatory authority is vested primarily with two government agencies: Department of Health and Human Services and Food and Drug Administration.[105] HHS's Office for Civil Rights

---

98. *See* BROWN ET AL., *supra* note 24, at 10.

99. CHURI ET AL., *supra* note 13, at 4.

100. *See* HEALTH CARE INDUS. CYBERSECURITY TASK FORCE, REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY 9 (2017),

101. *See* DEAN, *supra* note 14, at 2–4; Dave Fornell, *Raising the Bar for Medical Device Cyber Security*, DAIC: CYBERSECURITY (Aug. 16, 2017), https://www.dicardiology.com/article/raising-bar-medical-device-cyber-security [https://perma.cc/NU2L-FAJY].

102. *See* DEAN, *supra* note 14, at 2–4.

103. *See* Paez & Tobitsch, *supra* note 33, at 240.

104. Paez & La Marca, *supra* note 5, at 40.

105. *See, e.g.*, Office for Civil Rights, *HIPAA for Professionals*, U.S. DEP'T HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/index.html

(OCR) is the primary regulator of privacy and security in the healthcare sector, while FDA's jurisdiction extends to the safety and efficacy of medical devices.[106] Although the reach of both government agencies may encompass certain IoMT devices and their developers, significant gaps exist in the established regulatory frameworks such that portions of the IoMT industry remain unregulated, with no mandatory privacy and security standards.[107]

1. *The Health Insurance Portability and Accountability Act: Applicability, Scope, and Gaps*

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 to ensure motility of health insurance coverage and reduce costs associated with healthcare delivery.[108] Although HIPAA's goals did not originally encompass privacy and security, such protections were later mandated as healthcare organizations transitioned to electronic health records and digital systems to reduce costs of care and administrative burdens.[109] As a result, the HIPAA Privacy and Security Rules govern the healthcare landscape for privacy and security issues.[110]

The scope of HIPAA, however, is intentionally limited. HIPAA applies only to "covered entities" and only protects a subset of health information

---

[https://perma.cc/KZF6-EE7T]; *Medical Devices*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/Medicaldevices/default.htm [https://perma.cc/F6TB-AFR5]. The Federal Trade Commission ("FTC") is another agency responsible for consumer protection and the elimination of anti-competitive behaviors. *See* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017 1 (2017). The FTC is not specific to health care, and its regulatory authority extends primarily to unfair and deceptive acts or practices. *See id.* FTC's authority is not directed to preventing or regulating privacy and security standards in the healthcare industry, and the FTC does not create cybersecurity standards. *See* Kirk J. Nahra & Bethany A. Corbin, *Digital Health Regulatory Gaps in the United States*, 4 COMPLIANCE ELLIANCE J. 21, 30 (2018). As a result, the FTC "does not address legislative gaps that may leave digital health technology unregulated." *Id.*

106. *See* Office for Civil Rights, *About Us (OCR)*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/ocr/about-us/index.html [https://perma.cc/F5CK-6U2Q]; *Consumers (Medical Devices)*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/resources-you-medical-devices/consumers-medical-devices [https://perma.cc/2E4U-R6HQ].

107. *See* Paez & Tobitsch, *supra* note 33, at 240.

108. *HIPAA Privacy and Security for Beginners*, WILEY REIN: NEWSLS. (July 2014), https://www.wileyrein.com/newsroom-newsletters-item-5029.html [https://perma.cc/8XBH-NZXC] [hereinafter *HIPAA for Beginners*].

109. *Id.*

110. *See id.*

known as "protected health information."[111] To qualify as a covered entity,[112] an organization must fall into one of three categories that are statutorily defined: (1) healthcare provider;[113] (2) health plan;[114] or (3) healthcare clearinghouse.[115] In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act expanded HIPAA's provisions to encompass "business associates," which include any person or organization that performs certain specified functions on behalf of a covered entity.[116] Regardless of the type of covered entity involved, HIPAA's coverage only extends to protected health information (PHI), which is individually identifiable health information transmitted in any form or medium.[117]

The HIPAA Privacy Rule works by setting limitations on a covered entity's or business associate's use or disclosure of PHI.[118] The basic principle, subject to certain exceptions, is that a covered entity may not use or disclose PHI except as the Privacy Rule permits or requires, or as the individual (whose PHI is at issue) authorizes in writing.[119] The HIPAA Security Rule, in turn, complements the HIPAA Privacy Rule by operationalizing the Privacy Rule's protections through implementation of administrative, technical, and physical safeguards for a subset of PHI—electronic PHI (ePHI).[120] The Security Rule focuses on guarding against unauthorized access to a patient's ePHI and represents the first set of widely accepted security standards for healthcare practitioners.[121]

While HIPAA appears to offer comprehensive privacy and security frameworks for the healthcare industry, significant gaps are revealed by applying these regulations to digital health technology.[122] First, as explained

---

111. Paez & Tobitsch, *supra* note 33, at 240.

112. *See id.*

113. A healthcare provider is any individual or organization that gets paid to provide health care and transmits health information in electronic form. 45 C.F.R. § 160.102 (2018).

114. A health plan is an individual or group that pays the cost of medical care. *Id.*

115. A healthcare clearinghouse consists of entities that process information so it can be transmitted in standard format between covered entities. *Id.*

116. *See id.* § 160.103; *HIPAA for Beginners*, *supra* note 108.

117. § 160.103; *HIPAA for Beginners*, *supra* note 108.

118. *HIPAA for Beginners*, *supra* note 108.

119. 45 C.F.R. § 164.502(a).

120. *Id.* § 164.302.

121. *Id.*

122. *See* DHHS, EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 20 (2016); Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 U. ILL. L. REV. 415, 448–49; Kirk Nahra, *What Closing the HIPAA Gaps Means for the Future of Healthcare Privacy*, HITECH ANSWERS (Nov. 9, 2015),

above, HIPAA's protections and requirements extend only to digital health actors that are covered entities or business associates.[123] This means that if an organization does not qualify as a covered entity or business associate, it has no obligation to comply with HIPAA's privacy and security requirements.[124] For instance, companies that manufacture fitness trackers that collect basic health data, such as weight, heart rate, and height are not subject to HIPAA's regulations because they do not qualify as a healthcare provider, healthcare plan, or healthcare clearinghouse.[125] Rather, the company provides this product directly to consumers without involving providers or insurers.[126] Numerous MedTech companies, therefore, exist outside the bounds of the HIPAA Privacy and Security Rules because they are not covered entities or business associates.[127]

Second, HIPAA's applicability is limited by the type of information it protects.[128] Extending only to PHI, HIPAA excludes categories of health information that may be sensitive but not individually identifiable or directly related to a person's physical or mental health.[129] Healthcare data that does not satisfy the definition of PHI may be collected, used, and disclosed by any company without violating federal healthcare regulations.[130] For example, the Ohio Supreme Court held that lead-contamination notices issued by the Cincinnati Health Department could be disclosed even though they contained blood test results because the child's name was not included in the document.[131] MedTech companies that gather or aggregate data that is not personally identifiable are within their rights to sell or disclose such data under

---

https://www.hitechanswers.net/what-closing-the-hipaa-gaps-means-for-the-future-of-healthcare-privacy-2/ [https://perma.cc/PJ56-JW5E].

123. Paez & Tobitsch, *supra* note 33, at 240; Montgomery, *supra* note 40, at 170 (examining the application of HIPAA to the Proteus digital pill and noting relevant statutory gaps).

124. *See* Elizabeth Snell, *How Do HIPAA Regulations Apply to Wearable Devices?*, HEALTHIT SECURITY (Mar. 23, 2017), https://healthitsecurity.com/news/how-do-hipaa-regulations-apply-to-wearable-devices [https://perma.cc/6LEH-3QEQ].

125. *See* Nicolas P. Terry, *Will the Internet of Things Transform Healthcare?*, 19 VAND. J. ENT. & TECH. L. 327, 342 (2016) ("HIPAA data protection seldom will apply to data generated or stored on a mobile device, wearable, or IoT node.").

126. *See* Snell, *supra* note 124.

127. Paez & Tobitsch, *supra* note 33, at 240.

128. *See* 45 C.F.R. § 164.502(a).

129. *See id.* § 164.502(a), (d).

130. *See generally* Terry, *supra* note 125, at 338, 342 (discussing coverage of electronic medical apps under HIPAA).

131. State *ex rel.* Cincinnati Enquirer v. Daniels, 844 N.E.2d 1181, 1185 ¶ 11 (Ohio 2006).

HIPAA.[132] Similarly, if the data MedTech companies collect does not directly relate to a person's physical or mental health, and does not concern the provision of healthcare services or payment for such services, then individually identifiable health data may be disclosed, used, and sold.[133]

As a result, HIPAA is limited in its applicability and contains regulatory gaps that cause MedTech actors to fall outside its scope.[134] With minor exceptions, most digital health companies today will not qualify as covered entities or will collect data outside the scope of PHI, allowing them to remain unregulated by federal privacy and security frameworks.[135] When this occurs, MedTech companies may operate with little to no federal oversight, and can lack incentives to ensure adequate privacy and security standards are upheld.[136] Moreover, there is nothing in HIPAA that addresses liability for the malfunctioning, hijacking, or hacking of a healthcare device. HIPAA even precludes a private right of action for violations of its own provisions.[137] HIPAA's focus is thus purely on establishing federal standards of care that covered entities must satisfy, not remedying harm to consumers from device vulnerabilities.[138] Accordingly, HIPAA does not sufficiently regulate the MedTech industry.

2. FDA: Device and Cybersecurity Guidance

In contrast to the limited oversight of MedTech companies by HHS, FDA plays a central role in the regulation of medical devices generally. FDA is responsible for ensuring the safety and efficacy of certain classifications of devices, though not all MedTech products will trigger FDA scrutiny.[139] The type of oversight and pre-market approval that medical devices must

---

132. *See* 45 C.F.R. § 164.502(a), (d).

133. *See id.*

134. PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 12, at 6; Davenport, *supra* note 12, at 260.

135. *See* Terry, *supra* note 125, at 338–39, 342.

136. *See id.* at 343; DEAN, *supra* note 14, at 3–4; PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 12, at 6.

137. *See* 42 U.S.C. § 1320d-6 (2009); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462-01, 82601 (Dec. 28, 2000); Acara v. Banks, 470 F.3d 569, 571–72 (5th Cir. 2006); Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 45 (Conn. 2014).

138. *See generally HIPAA for Beginners*, *supra* note 108.

139. *See New York Attorney General Addresses Key Health Care Privacy Gaps*, WILEY REIN: NEWSLS. (Apr. 2017), https://www.wileyrein.com/newsroom-newsletters-item-April_2017_PIF-NY_AG_Addresses_Key_Health_Care_Privacy_Gaps.html [https://perma.cc/DZ3Q-43KR].

undertake depends principally on the device's classification, which is determined by the level of risk posed by the device.[140] Class I devices pose the least risk and are subject only to general controls.[141] Class II devices, which are slightly riskier, must satisfy general controls and special controls.[142] Finally, Class III devices, which are used to support, or sustain human life or pose an unreasonable risk of illness or injury, are the most heavily regulated.[143]

Recognizing the developing intersection of medical devices and technology, FDA issued industry guidance titled *Postmarket Management of Cybersecurity in Medical Devices* on December 28, 2016.[144] This voluntary guidance sets forth FDA's recommendations for effectively managing post-market cybersecurity vulnerabilities.[145] FDA expressly recognizes that medical devices may now be "networked" and connected with other medical applications that comprise the IoMT.[146] The interconnected structure enables the exploitation of vulnerabilities and "may represent a risk to health" such that "continual maintenance throughout the product life cycle" is necessary to protect "against such exploits."[147] FDA thus recommends that medical device manufacturers proactively address cybersecurity vulnerabilities to reduce health and safety risks.[148]

Importantly, FDA acknowledges that risk management for cybersecurity vulnerabilities in medical devices "is a shared responsibility among stakeholders including the medical device manufacturer, the user, the Information Technology (IT) system integrator, Health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA."[149] While FDA encourages collaboration among these actors to enhance post-market cybersecurity, it cannot mandate cybersecurity protections in devices that are already approved and marketed.[150] Thus,

---

140. *See* 21 U.S.C. § 360c (2012).

141. Steve Kanovsky et al., *Chapter 8: The Medical Device Approval Process*, *in* A PRACTICAL GUIDE TO FDA'S FOOD AND DRUG LAW AND REGULATION 211, 213 (Kenneth R. Piña & Wayne L. Pines eds., 6th ed. 2017) [hereinafter FOOD & DRUG LAW GUIDE].

142. *See* 21 U.S.C. § 360c(a)(1)(B) (2016); Kanovsky et al., *supra* note 141, at 213–14.

143. *See* 21 U.S.C. § 360c(a)(1)(C) (2016); Kanovsky et al., *supra* note 141, at 213–14.

144. FDA, POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 1, 4 (2016) [hereinafter FDA, POSTMARKET GUIDANCE].

145. *Id.* at 4.

146. *Id.*

147. *Id.*

148. *See id.*

149. *Id.* at 6.

150. *See id.*

although FDA's guidance is a crucial step towards securing medical devices, including IoMT products, its voluntary nature does not adequately incentivize compliance.

Nearly two years later, FDA continues to recognize the overwhelming importance of cybersecurity in medical devices. Recently, FDA issued draft guidance regarding the *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*.[151] FDA again reiterated "[t]he need for effective cybersecurity to ensure medical device functionality and safety," and noted that this objective has become increasingly important with the continued use of wireless and network-connected devices, and the frequent electronic exchange of patient data.[152] As manufacturers design their medical devices and apply for pre-market approval, FDA hopes that they will mitigate cybersecurity risks.[153] However, as with the post-market cybersecurity guidance, the pre-market guidance is voluntary.[154]

While FDA has taken a proactive approach to encourage medical device cybersecurity, additional measures—particularly those that involve compliance incentives—must be adopted to protect patient safety.[155] Moreover, although FDA regulates the approval of medical devices, it does not provide relief for patients that are harmed by device malfunctions or hacking.[156] Although FDA's role is to regulate medical device safety and security, it lacks authority and frameworks to create a comprehensive mandatory cybersecurity system, and to apportion liability and remedies accordingly. Combined with HIPAA, this creates a regulatory gap that has not yet been resolved by the federal government.

---

151. FDA, CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2018).

152. *Id.* at 4.

153. *See generally id.* (presenting draft guidelines to strengthen medical devices against cybersecurity threats).

154. *See id.* at 1, 5; Louiza Dudin, Note, *Networked Medical Devices: Finding a Legislative Solution to Guide Healthcare into the Future*, 40 SEATTLE U. L. REV. 1085, 1093, 1098 (2017).

155. *See generally* Dudin, *supra* note 154, at 1093 (explaining that voluntary FDA guidance does "not appear to provide a strong incentive for manufacturers to meet their duty of care in ensuring the cybersecurity of their devices"). Dudin advised that 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 proactively rather than reporting adverse events after the fact." *Id.* at 1098.

156. *See id.* at 1093 ("[D]evices approved for market by the FDA are shielded from manufacturer liability claims.").

B. Industry Cybersecurity Frameworks

To help address federal regulatory gaps for the security of IoMT devices, numerous industry organizations have published their own voluntary cybersecurity frameworks that seek to illuminate best practice standards.[157] These frameworks are intended to enable digital health companies to adopt a cybersecurity structure that best meets their organizational needs.[158] A 2018 survey conducted by the Healthcare Information and Management Systems Society[159] reported that there are five primary security frameworks in use by healthcare organizations today: (1) National Institute of Standards and Technology (NIST);[160] (2) Health Information Trust Alliance (HITRUST);[161] (3) Center for Internet Security (CIS) Critical Security Controls;[162] (4) International Organization for Standardization (ISO);[163] and (5) Control Objectives for Information and Related Technologies (COBIT).[164] The framework established by NIST is the most well-recognized voluntary cybersecurity structure today,[165] and a cross-walk document exists highlighting the interaction between the NIST cybersecurity standards and the HIPAA Security Rule.[166] NIST has further proposed guidance for IoT devices

---

157. *See infra* notes 153–56.

158. *See* Tara Swaminatha, *The Rise of the NIST Cybersecurity Framework*, CSO (May 11, 2018), https://www.csoonline.com/article/3271139/data-protection/the-rise-of-the-nist-cybersecurity-framework.html [https://perma.cc/L3A7-XSYA].

159. HIMSS N. AM., 2018 HIMSS CYBERSECURITY SURVEY 18 (2018).

160. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY VERSION 1.1 (2018).

161. HITRUST, INTRODUCTION TO THE HITRUST CSF, VERSION 9.1 (2018).

162. CTR. FOR INTERNET SEC., CIS CONTROLS, VERSION 7 (2018).

163. JOINT TECH. COMM. ISO/IEC JTC 1, INT'L ORG. FOR STANDARDIZATION, ISO/IEC 27001 (2013).

164. IT GOVERNANCE INST., CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGIES 4.1 (2007).

165. *See* Scott Schlimmer, *Implementing the NIST Cybersecurity Framework Could Be Worth at Least $1.4m to Your Business*, CSO (Apr. 19, 2018), https://www.csoonline.com/article/3268937/implementing-the-nist-cybersecurity-framework-could-be-worth-at-least-1-4m-to-your-business.html [https://perma.cc/BN4X-SQT4].

166. DHHS, OFFICE FOR CIVIL RIGHTS, HIPAA SECURITY RULE CROSSWALK TO NIST CYBERSECURITY FRAMEWORK (2016).

in the form of a white paper on October 17, 2018,[167] and is in the process of creating a privacy framework for 2019.[168]

The current industry cybersecurity frameworks represent a collective effort to define best-practice standards in a constantly evolving technological environment without stifling innovation.[169] The frameworks incorporate flexibility to match organizational structure, yet they provide the benefit of shared expert experience among myriad organizational groups and industry actors.[170] This cooperative approach to cybersecurity enhances overall device safety and organizational response to security incidents by aggregating experience and ideas.[171] Thus, these cybersecurity models possess extreme merit, particularly in the face of legislative gaps.

While industry cybersecurity frameworks are crucial to bridging the gaps for IoMT device security, they suffer from the same drawbacks as FDA's medical device cybersecurity guidance: the standards are purely voluntary.[172] Presently, there is no way to enforce these standards to hold manufacturers of IoMT products accountable for unsafe coding or lax device security. If an IoMT device manufacturer elects not to follow a voluntary cybersecurity framework, it faces little consequences and, depending on the company, may remain unregulated by federal and industry actors.[173] Such a result does not encourage heightened device safety standards, but instead enforces the status quo. Thus, existing federal and industry cybersecurity standards—while a promising step in the right direction—do not create a comprehensive security structure for IoMT devices, and fail to address liability and relief for patients who suffer harm from breached or hijacked IoMT devices.

---

167. *See* JEFFREY VOAS ET AL., NAT'L INST. OF STANDARDS & TECH, NIST CYBERSECURITY WHITE PAPER: INTERNET OF THINGS (IOT) TRUST CONCERNS, at i–ii (draft 2018); *see also* Paez & La Marca, *supra* note 5, at 51 (explaining that in September 2015, NIST published a draft IoT framework called the Framework for Cyber-Physical Systems, which sought to create a shared understanding of Cyber-Physical Systems).

168. *See Privacy Framework*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/privacy-framework [https://perma.cc/3HFC-GX8A].

169. *See generally NIST Releases Second Draft to Cybersecurity Framework, ANSI Encourages Stakeholders to Comment*, AM. NAT'L STANDARDS INST. (Dec. 8, 2017), https://www.ansi.org/news_publications/news_story?menuid=7&articleid=cde5f62c-3ee2-4146-9753-9e6e0ddaff9f [https://perma.cc/5CWN-GHFL] (explaining that the NIST framework was created through collaboration between industry and government).

170. Swaminatha, *supra* note 158.

171. *See id.*

172. *See, e.g.*, NAT'L INST. OF STANDARDS & TECH., *supra* note 160, at v.

173. *See* PRESIDENT'S NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 12, at 6.

C. *Economic Realities and the "Race to Market"*

In addition to voluntary cybersecurity frameworks and regulatory gaps that permit IoMT developers to evade government oversight, economic realities for device creation unintentionally foster a "race to the market" mindset that prioritizes speed over safety.[174] Scholars note that the absence of effective cybersecurity measures is attributable, in part, to "weak economic incentives," and that these weak incentives and market failures "have led to an accumulation of insecure hardware and software."[175] While creating secure code can potentially result in a marketing advantage or impact brand reputation,[176] it is extremely difficult for consumers to compare product security.[177] Such benefits, therefore, may go unnoticed, causing manufacturers to lose money without seeing a sufficient return on their investment.[178]

Indeed, a 2017 study by the Ponemon Institute underscores the need for manufacturers to consider consumer safety and cybersecurity when developing IoMT devices.[179] Sixty-seven percent of medical device manufacturers surveyed in the Ponemon study believed that a cyberattack on one or more medical devices built by their organization is likely, yet only 17% of these manufacturers have taken any substantial steps to prevent such an attack.[180] Only one-third of medical device manufacturers encrypt traffic among IoT devices, and 53% of these manufacturers acknowledge that "there is a lack of quality assurance and testing procedures that lead to vulnerabilities in medical devices."[181] Further, despite the fact that 31% of medical device developers are aware of actual attacks involving connected medical devices, only 25% of these developers have added security protocols or architecture inside the devices to protect patients and clinicians.[182]

---

174. *See, e.g.*, DEAN, *supra* note 14, at 3–4.

175. *Id.*; *see* Paez & La Marca, *supra* note 5, at 52–53 ("IoT manufacturers often lack an economic incentive to provide software updates and support. . . ."); Daley, *supra* note 31, at 535 ("[T]he economic and legal structure of the software development industry leaves no single entity with strong enough incentives to secure software before it is shipped.").

176. *See* DEAN, *supra* note 14, at 3–4.

177. Daley, *supra* note 31, at 537–38. "[T]he vast majority of consumers lack the expertise to effectively evaluate security features. Consumers therefore lack the ability to effectively compare security across competitors." *Id.*

178. *See id.* DEAN, *supra* note 14, at 3–4.

179. *See* PONEMON INST., MEDICAL DEVICE SECURITY: AN INDUSTRY UNDER ATTACK AND UNPREPARED TO DEFEND 4 (2017).

180. *Id.* at 1.

181. *Id.* at 2.

182. *Id.* at 1–2.

Device manufacturers additionally note that few connected medical devices are actually tested in the design phase.[183] Only 28% of medical device respondents affirmed that testing is done prior to development and post-release, and only 9% of manufacturers test their deployed medical devices annually.[184] This lack of testing is explained, in part, by the pressure device manufacturers face to market connected devices quickly.[185] Where rushing devices to the market is a priority, software security becomes an unfortunate afterthought.[186] Moreover, just 51% of device manufacturers follow the existing voluntary cybersecurity framework, best practice security framework, or both.[187] Thus, current "[m]edical device security practices in place are not the most effective,"[188] and "[a]ccountability for the security of medical devices manufactured or used is lacking."[189] It is time to incentivize safer IoMT development, particularly given the life or death risks these devices can pose.

IV. DEVELOPING A COMPREHENSIVE LIABILITY STRUCTURE

Given the voluntary cybersecurity frameworks in existence today, the "race to market" reality, and the regulatory gaps that permit IoMT developers to evade government oversight, it is necessary that legislatures provide sufficient incentives for manufacturers to create safe and secure code for IoMT products.[190] While numerous bills have been proposed at the federal and state levels regarding regulation of IoMT products, these bills have a low probability of passage and have been met with fierce opposition by IoMT manufacturers.[191] These manufacturers claim that such legislation will not only drive developers out of the field, but will also hinder progress in the

183. *Id.* at 14.

184. *Id.* at 2, 14.

185. *Id.* at 2.

186. Paez & La Marca, *supra* note 5, at 53.

187. *See* PONEMON INST., *supra* note 179, at 3. Sixty-two percent of device manufacturers also do not follow a published Secure Development Life Cycle process for medical devices. *Id.* at 14.

188. *Id.* at 8.

189. *Id.* at 2.

190. *See* DEAN, *supra* note 14, at 8–11; Daley, *supra* note 31, at 538; Lemos, *supra* note 18.

191. *See* Daley, *supra* note 31, at 542; Evans, *supra* note 17; Rosenzweig, *supra* note 19; *see, e.g.*, Bethany Corbin & Megan Brown, *Partnerships Can Enhance Security in Connected Health and Beyond*, CIRCLEID (Dec. 14, 2007), http://www.circleid.com/posts/20171213_partnerships_can_enhance_security_in_connected_health_and_beyond/[https://perma.cc/9SAT-5766].

IoMT industry because these legislative proposals cannot be quickly and efficiently amended to keep pace with technological progress.[192] In fact, by the time many IoMT bills are passed, they will be outdated due to the rapid advances in technology that can occur over a short period of time.[193] Thus, IoMT has proven difficult for state and federal legislatures to regulate, and this lack of mandatory regulation has created a dearth of incentives for IoMT manufacturers to develop secure IoMT products.[194]

Provided this current state of affairs, a comprehensive IoMT liability model would offer critical incentives to manufacturers to increase the security of their products and comply with voluntary cybersecurity best practice standards. As is, there are limited incentives to encourage manufacturers to expend time, resources, and money on developing safer products when they are not subject to regulatory oversight and do not have a clear grasp on the potential liability they could face for unsecure code.[195] Part IV explains why current liability frameworks are ill suited to the IoMT context and advocates for the development of a comprehensive liability structure as the "stick" that encourages incentivizing safer code.

A. Existing Liability Standards: Evaluating the Application of Products Liability to IoMT

Pursuant to traditional tort doctrines, device malfunctions are typically addressed through products liability laws at the state level (when preemption is not implicated).[196] Products liability refers to the liability of a manufacturer, processor, or seller whose goods injure consumers.[197] Three legal paths may be pursued under the products liability framework: (1) strict liability; (2)

---

192. *See* BROWN ET AL., *supra* note 24; Ashton, *supra* note 28, at 834; Evans, *supra* note 17.

193. Jonathan D. Klein, *2017: The Year of Big Shifts in Cybersecurity*, LEGAL INTELLIGENCER (May 30, 2017), https://www.law.com/thelegalintelligencer/almID/12027877 93676/?slreturn=20191011051937 [https://perma.cc/N3RC-PYDD].

194. *See* DEAN, *supra* note 14, at 4; Paez & La Marca, *supra* note 5, at 52–53; Klein, *supra* note 193.

195. *See generally* DEAN, *supra* note 14, at 4 (explaining the reasons for medical devices lacking security); Gorman, *supra* note 43.

196. *See* Gorman, *supra* note 43, at 4. While products liability claims for medical devices may be preempted by the Food, Drug, and Cosmetics Act and subsequent amendments, preemption is beyond the scope of this Article. For purposes of this Article, it is assumed that preemption does not bar state products liability claims.

197. DEAN, *supra* note 14, at 9; Gorman, *supra* note 43; Paez & La Marca, *supra* note 5, at 57.

negligence; and (3) breach of warranty.[198] The application of these doctrines to IoMT, however, is akin to fitting a square peg in a round hole.[199] As IoMT progresses, "it could reshape the law of products liability by redefining who can be held at fault and who will bear the financial consequences if something were to go wrong with a product."[200] This section explains the fundamentals of products liability and details why this tort doctrine, as currently structured, is ill-fitted to remedy harm from IoMT devices.

1. Strict Products Liability

First, strict products liability is used to combat harm caused by unreasonably dangerous products.[201] This doctrine is applicable to products that cause substantial harm, death, or property damage due to defects.[202] The purpose of strict products liability is to ensure that the manufacturers, developers, and sellers of defective devices bear the costs of any harm a consumer experiences due to that product.[203] In contrast to other tort doctrines, such as negligence, strict products liability does not require prior knowledge of a risk as a prerequisite to liability.[204] Rather, liability is automatic when it is proven that a device is defective, regardless of whether the manufacturer exercised all possible care when developing the product.[205] In this manner, strict liability is intended to incentivize manufacturers to "weigh the potentially small cost of mitigating the defective design or manufacturing element in their product against releasing the product with defects and having to cover potentially large damages that these defects may cause."[206]

While defective digital products are not new, strict products liability has only been applied in rare instances.[207] Its limited application is due to three

198. DEAN, *supra* note 14, at 9; Paez & La Marca, *supra* note 5, at 57.

199. *See, e.g.*, *Liability and IoT Devices—A Legal Can of Worms*, DATA FOUNDRY BLOG (May 15, 2018), https://www.datafoundry.com/blog/liability-IoT-devices-legal-can-of-worms [https://perma.cc/239C-8WTJ]. Determining the liability for IoT devices "will be more difficult than ever" because "the diversity of the IoT field has turned the typical regulatory landscape on its head." *Id.*

200. Paez & La Marca, *supra* note 5, at 57.

201. DEAN, *supra* note 14, at 10.

202. *Id.*

203. *Id.*

204. *Id.*

205. Paez & La Marca, *supra* note 5, at 57.

206. DEAN, *supra* note 14, at 10.

207. *Id.* at 16.

primary factors. First, the economic loss doctrine limits the type of damages that can be remedied through strict products liability.[208] As previously noted, strict products liability requires a demonstration of physical harm, death, or property damage that is directly attributable to the defective device.[209] The economic loss doctrine precludes claims based solely on financial losses, which are often the kind of impacts that insecure digital products have produced in the past.[210] IoMT, however, has the potential to skirt this economic loss limitation because its interconnectivity may result in physical harm or death, depending on the nature of the hack, breach, or hijack.[211] As digital technologies become increasingly integrated with devices, "the potential for physical harm may grow."[212] Thus, while the economic loss doctrine has traditionally barred strict products liability for digital devices, it is less of a concern for IoMT.[213]

Second, and more importantly, consumers face an uphill battle trying to prove that "missing security features or digital defects alone led to harm or damage," and most consumers do not have an "empirically-based cost-benefit calculation with supporting probabilities for claims."[214] Similarly, third-party interference with the device by hackers may constitute an intervening event that absolves the manufacturer of liability (though it may have been the manufacturer's insecure code that enabled the hacker to access the device in the first place).[215] Finally, ambiguity exists regarding whether software is a product or a service.[216] Products liability applies only to products, and in some U.S. states, software or code may be viewed as an intangible item.[217] Given the variability in products liability standards throughout the United States, it is possible that some jurisdictions may find strict products liability inapplicable to insecure code.[218] Thus, strict products liability may not provide a sufficient remedy for consumers despite the risk of harm presented by insecure IoMT code.

---

208. *See* Beery & Burns, *supra* note 20, at 55; *see also* Butler, *supra* note 21, at 919–21 (discussing the impact of the economic loss doctrine on IoT devices).

209. DEAN, *supra* note 14, at 16.

210. *Id.*

211. *See* Butler, *supra* note 21, at 919–21; Paez & La Marca, *supra* note 5, at 48.

212. DEAN, *supra* note 14, at 16.

213. *See* Butler, *supra* note 21, at 919–21.

214. DEAN, *supra* note 14, at 16.

215. *See id.* at 18.

216. *Id.* at 17; *see also* Paez & La Marca, *supra* note 5, at 58 (discussing whether software should be considered a product or a service).

217. DEAN, *supra* note 14, at 17.

218. *See id.* at 16–18; *see also Untangling the Web*, *supra* note 4.

The converse, however, also has the potential to be true. As IoMT develops, there may be greater application of strict products liability to IoMT devices in ways that were not originally intended.[219] For example, given that most IoMT products present a risk of death or bodily injury from device hacks or hijacks, courts could conceivably apply the strict products liability doctrine to *all* IoMT devices regardless of whether harm actually occurs.[220] The problem with this approach is three-fold. First, because there is no universally secure code, each IoMT device—regardless of whether it satisfies the strictest security requirements to date—will still have the *potential* to be hijacked and create life-or-death scenarios.[221] This places IoMT device manufacturers at a continuous risk for unfettered liability related to digital products, even if the manufacturer took all reasonable steps and adhered to voluntary industry frameworks. Such a risk for liability, in turn, may cause manufacturers to abandon the IoT market, which will derail and stifle innovation in an industry that promises to revolutionize health care.[222]

Moreover, it is still unclear *where* along the supply chain liability will fall for a malfunctioning device.[223] IoMT differs from past technological developments in that it has an extensive supply chain that involves numerous manufacturers, developers, suppliers, coders, and sellers.[224] At this time, there is no clear demarcation of liability along this chain.[225] "While contractual arrangements might allow for the allocation of liability between parties," strict liability cannot be transferred by contracts.[226] Companies would therefore need to show which manufacturer or party was responsible for the defect,

---

219. DEAN, *supra* note 14, at 19.

220. *See generally* Paez & La Marca, *supra* note 5, at 46, 48, 59.

221. *See* DEAN, *supra* note 14, at 7 (expounding on the vast amount of errors that always exist in code); Paez & La Marca, *supra* note 5, at 59; Wenzel, *supra* note 33, at 59 (stating that there is no such thing as a computer that cannot be hacked); Beery & Burns, *supra* note 20, at 55 (noting that all complex software is understood to have bugs).

222. *See* Paez & La Marca, *supra* note 5, at 59–60; Evans, *supra* note 17; *see also* Daley, *supra* note 31, at 542 (discussing that any liability borne by software vendors will extinguish the current startup ecosystem).

223. *See* DEAN, *supra* note 14, at 12–13, 21; *Untangling the Web*, *supra* note 4.

224. *See* Paez & La Marca, *supra* note 5, at 30 ("[T]he IoT ecosystem hinges on the interconnectivity of countless devices and participants, companies will need to account for the legal rights and obligations of multiple stakeholders involved throughout a product's entire lifecycle, from design and manufacturing to installation, operation, maintenance and decommissioning."); *see also* DEAN, *supra* note 14, at 12–13, 21; *Untangling the Web*, *supra* note 4.

225. *See, e.g.*, Paez & La Marca, *supra* note 5, at 60.

226. DEAN, *supra* note 14, at 21.

which can be difficult to determine.[227] This will require the "development of digital technology failure standards and thorough incident investigation," which is costly and may drive developers out of the market.[228]

In short, the application of strict products liability in this manner will not result in a proper balancing of consumer harm and manufacturer responsibility. No clear guidelines exist for apportioning liability among an IoMT supply chain, and the mere risk of unfettered strict products liability for device manufacturers can inhibit fundamental innovation.[229] Thus, in its current form, strict products liability cannot be easily applied to IoMT.

2. *Negligence*

The second theory of liability potentially applicable to IoMT devices is negligence. Proof of negligence requires demonstration of five factors: (1) a duty or standard of care; (2) breach of that duty or standard of care; (3) cause in fact; (4) proximate cause; and (5) damages.[230] Negligence in the context of products liability can occur if a supplier, retailer, or manufacturer places an IoMT product into the stream of commerce with inadequate labeling, or if there are manufacturing or design defects.[231] The manufacturer or supplier will be liable if it failed to exhibit ordinary care to a party who suffers injury proximately caused by the manufacturer's negligent conduct.[232] For products liability, negligence can arise in numerous ways, including: design of the product, selection of materials, production process, product assembly and testing, and placement of inadequate warnings or directions.[233]

One of the most common applications of negligence to products liability occurs in the context of design defects.[234] A design defect claim alleges that the manufacturer's product design was not reasonable in light of the product's risk of harm and availability of safer alternative designs.[235] Accordingly, a design defect claim requires proof of at least three elements: (1) the product

---

227. *Id.*

228. *Id.* at 3, 21.

229. *See id.* at 12–13, 21; Paez & La Marca, *supra* note 5, at 60.

230. Lewison v. Renner, 905 N.W.2d 540, 548 (Neb. 2018) (citing Latzel v. Bartek, 846 N.W.2d 153 (Neb. 2014)).

231. *See* Scott, *supra* note 19, at 459.

232. *See Lewison*, 905 N.W.2d at 548 (explaining the general standards for prevailing in a negligence action).

233. *What Is Product Liability Negligence?*, ATTORNEYS.COM, http://www.attorneys.com/products-liability/negligence [https://perma.cc/9MCN-YCKF].

234. *See id.*

235. Scott, *supra* note 19, at 459.

posed a substantial likelihood of harm; (2) a safer and more feasible alternative product or design existed; and (3) the product, as designed, caused the plaintiff's injury.[236] In these cases, the factfinder must evaluate the manufacturer's intent and judgment in selecting the particular product design.[237] Some courts view this analysis in terms of risk versus utility.[238]

With respect to IoMT, it is conceivable that plaintiffs could bring design defect claims premised on insecure code. Specifically, a plaintiff may argue that the manufacturer's design of an IoMT product is inherently risky due to the manufacturer's selection of certain code, failure to use cybersecurity best practice standards in testing the code prior to launch, or both. Plaintiffs, however, will face numerous problems with such allegations.[239] First, there is no universally secure code, and plaintiffs will have difficulty establishing that the code and accompanying security processes selected by a manufacturer are inherently less safe than other alternatives.[240] In fact, it is estimated that "programmers make between 10 and 50 errors for every 1,000 lines of code."[241] Second, negligent design defect claims are premised on the existence and availability of a safer alternative product design.[242] Absent a safer alternative, negligence design claims can fail as a matter of law.[243] Given the rapidly evolving state of technology, it is possible that there may not be alternative products on the market for which a plaintiff could compare the manufacturer's product. Further, given the inherent flaws in software, it is possible that any similar products that do exist on the market would not be safer.

Third, plaintiffs may have difficulty establishing that the product posed a substantial risk of harm.[244] All implantable devices embedded with

---

236. *See* MICHAEL WEINBERGER, NEW YORK PRODUCTS LIABILITY § 18:3 (2d ed. 2018).

237. *Id.*

238. *See id.*; Butler, *supra* note 21, at 927.

239. *See* Butler, *supra* note 21, at 915.

240. *See* DEAN, *supra* note 14, at 7; VINCENT J. VITKOWSKY, THE INTERNET OF THINGS: A NEW ERA OF CYBER LIABILITY AND INSURANCE 15, 16 (2015); Paez & La Marca, *supra* note 5, at 59; Wenzel, *supra* note 33, at 59; Beery & Burns, *supra* note 20, at 58; Evans, *supra* note 17; *Untangling the Web*, *supra* note 4.

241. DEAN, *supra* note 14, at 7.

242. *See, e.g.*, KAREN SCHULTZ & THEODORE Z. WYMAN, TEXAS JURISPRUDENCE § 34 (3d ed. 2018).

243. *See* Connally v. Sears, Roebuck & Co., 86 F. Supp. 2d 1133, 1137 (S.D. Ala. 1999) (quoting Beech v. Outboard Marine Corp., 584 So. 2d 447, 450 (Ala. 1991)).

244. *See, e.g.*, Butler, *supra* note 21, at 915.

connectivity mechanisms are likely to pose similar risks of harm,[245] and it will be challenging to establish that one product is more or less risky than another device that is similarly implanted into a patient's body. Further, the courts would risk opening the litigation floodgates and driving manufacturers out of the IoMT field if they were to find that any IoMT device implanted into a patient's body poses a substantial likelihood of harm, given that there is no defect-free code.[246] Risk will exist with any IoMT device, and it is unclear at this stage what levels of risk are and are not acceptable.[247]

Moreover, to the extent a plaintiff attempted to apply general negligence principles outside the design defect context, she would face substantial difficulty establishing the existence of a duty of care.[248] As noted, negligence is premised upon the violation of an established standard of care.[249] There are no mandatory federal cybersecurity standards, however, for IoMT products.[250] As evidenced in Part III, IoMT products regularly fall within the cracks of federal legislation and sometimes are not subject to government oversight.[251] Additionally, federal agencies do not actively regulate cybersecurity of IoMT devices at this stage—as evidenced by the voluntary nature of the FDA's post-market cybersecurity guidance.[252] While industry cybersecurity frameworks exist, they are also voluntary, and there is no consensus on which cybersecurity framework should or must be adopted by healthcare organizations.[253] Without readily discernable and established standards in place, it is difficult to argue that these standards have been

245. *See* BURMEIER ET AL., *supra* note 76, at 11; Carmen Camara et al., *Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey*, 55 J. BIOMEDICAL INFORMATICS 272, 272 (2015).

246. *See* Paez & La Marca, *supra* note 5, at 59; *see also* Detsch, *supra* note 22 (discussing faulty codes in IoT devices that cause serious bodily harm or death).

247. *See* DEAN, *supra* note 14, at 7; Paez & La Marca, *supra* note 5, at 52–53.

248. *See* VITKOWSKY, *supra* note 240, at 16; *see also* Beery & Burns, *supra* note 20, at 57–58 (explaining that it will be difficult to establish an accepted duty of care).

249. Lewison v. Renner, 905 N.W.2d 540, 548 (Neb. 2018) (citing Latzel v. Bartek, 846 N.W.2d 153 (Neb. 2018)).

250. *See, e.g.*, Gorman, *supra* note 43, at 4–5; Merritt Baer & Chinmayi Sharma, *What Cybersecurity Standard Will a Judge Use in Equifax Breach Suits?*, LAWFARE (Oct. 20, 2017, 7:30 AM), https://www.lawfareblog.com/what-cybersecurity-standard-will-judge-use-equifax-breach-suits [https://perma.cc/AL27-BBV3].

251. *See* discussion *supra* Part III.

252. *See, e.g.*, FDA, POSTMARKET GUIDANCE, *supra* note 144.

253. *See, e.g.*, NAT'L INST. OF STANDARDS & TECH., *supra* note 160, at v.

breached.[254] Thus, the negligence model may fail to provide sufficient relief to injured consumers.

3. *Breach of Warranty*

The final liability model that is routinely applied to device defects is breach of warranty, including common law warranties and warranties under Article 2 of the Uniform Commercial Code (UCC). Unfortunately, the law surrounding whether Article 2 applies to IoMT devices—which can incorporate software, software-related services, and tangible goods—is unclear.[255] IoMT has transformed interactions between buyers and sellers, and created more elaborate hybrid transactions with increased levels of complexity.[256] This complexity has resulted in a lack of clarity regarding whether Article 2, which covers consumer goods, applies to hybrid transactions.[257] This uncertainty "belies the UCC's stated goals of uniformity and simplicity and can lead to unwarranted disputes between parties about the laws applicable to a transaction."[258] Thus, whether Article 2 and its warranty provisions apply to IoMT devices is in a state of flux, with such discussion extending beyond the scope of this Article.

Difficulties also exist with applying common law warranties to IoMT devices. Two types of common law warranties exist: (1) express warranties; and (2) implied warranties.[259] With respect to express warranties—which are explicit promises that devices will perform in a particular manner—it is possible that IoMT device manufacturers may expressly guarantee their products in limited contexts, but such a warranty is likely to only extend to the device itself, and not to any software, product monitoring, or guarantees against breaches, hacks, or hijacks.[260] Moreover, it is doubtful that any IoMT manufacturer will warrant its product for secure software code, given the

---

254. *See* VITKOWSKY, *supra* note 240, at 16; *see also* Beery & Burns, *supra* note 20, at 57–58 (quoting VITKOWSKY, *supra* note 240, at 16).

255. Stacy-Ann Elvy, *Hybrid Transactions and the Internet of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 79–80, 87–88, 104 (2017).

256. *Id.* at 103.

257. *See id.* at 88–89, 103–04.

258. *Id.* at 89.

259. *What are Express and Implied Warranties?*, FINDLAW, https://consumer.findlaw.com/consumer-transactions/what-are-express-and-implied-warranties.html [https://perma.cc/JBN3-PFYX].

260. Elvy, *supra* note 255, at 115; *see also What are Express and Implied Warranties?*, *supra* note 259 (explaining in more detail how express warranties are different from implied warranties).

intrinsic "bugginess" that exists in code today.[261] Indeed, software manufacturers routinely evade liability for software vulnerabilities through end-user agreements, which disclaim all responsibility and liability for breaches, hacks, hijacks, and other harm resulting from insecure code.[262] By using products associated with end-user agreements, consumers waive any rights they have regarding the safety and security of the software.[263] More concerning, only 8% of consumers even read this dense legalistic disclaimer.[264] Such end-user agreements make it difficult—if not impossible—to bring product liability actions, particularly for breach of warranty.[265]

Implied warranties, on the other hand, are not expressly provided by manufacturers, but are instead inferred when a manufacturer sells a product to a consumer.[266] An implied warranty may arise from the circumstances surrounding the transaction or from the product itself.[267] Typical implied warranties include the implied warranty of fitness for a particular purpose, the implied warranty of merchantability for goods, and the implied warranty of workmanlike quality for services.[268] Implied warranties, however, may be disclaimed, and sellers often do this in either the contract or the end-user licensing agreement.[269] Indeed, the implied warranty of merchantability—which is intended to assure consumers that the goods will meet baseline standards of quality—is so often disclaimed that scholars have questioned its

---

261. VITKOWSKY, *supra* note 240, at 16; *see* Paez & La Marca, *supra* note 5, at 59; Wenzel, *supra* note 33, at 59; Beery & Burns, *supra* note 20, at 58; *see Untangling the Web*, *supra* note 4. *See generally* DEAN, *supra* note 14, at 7 (noting that "buggy software is not exceptional" in that programmers make an estimated ten to fifty errors for every one-thousand lines of code that they write).

262. DEAN, *supra* note 14, at 10; Evans, *supra* note 17.

263. *See* Gorman, *supra* note 43, at 4.

264. Lemos, *supra* note 18, at 2.

265. Beery & Burns, *supra* note 20.

266. *See What are Express and Implied Warranties?*, *supra* note 259.

267. *See generally id.* (explaining the circumstances in which an implied warranty may arise).

268. *Can Implied Warranty Protection Be Disclaimed?*, ATTORNEYS.COM, http://www.attorneys.com/consumer-law-and-protection/can-implied-warranty-protection-be-disclaimed [https://perma.cc/3JWX-3NX8].

269. *See, e.g.*, Robert W. Gomulkiewicz, *The Implied Warranty of Merchantability in Software Contracts: A Warranty No One Dares to Give and How to Change That*, 16 J. MARSHALL J. COMPUTER & INFO. L. 393, 398 (1998); Charles H. Moellenberg, Jr. & Robert W. Kanter, *Be Wary of Warranties for Software Design*, JONES DAY INSIGHTS (Aug. 2018), https://www.jonesday.com/be-wary-of-warranties-for-software-design-08-27-2018/ [https://perma.cc/3KKX-VFHZ].

usefulness.[270] Thus, given the absence of defect-free code and the prevalence of end-user licensing agreements, products liability, in its various forms, is not a viable cause of action for injured consumers.

B. The Carrot and the Stick: Incentivizing Safer Code Through a New Liability Framework

As IoMT continues to evolve and define consumer experiences and expectations, it is crucial that safer code be prioritized in IoMT devices. As noted above, IoMT device manufacturers are currently well insulated from liability and are able to externalize the costs of insecure software.[271] The threat of liability, however, is a proven deterrent that can reduce the probability of consumer harm or damage.[272] Because IoMT developers are underinvesting in software security, it is necessary to create incentives that will be economically and legally attractive to manufacturers.[273] This requires combining "ex ante incentives to invest in security with ex post liability that, while sufficient to discipline developers, does not stifle innovation."[274] The goal is to balance consumer safety with technological advancement.[275] Thus, a reasonable and workable liability framework should be developed to provide consumers with relief for injuries and clarify manufacturer responsibilities and obligations.

The form that this new liability structure should take for IoMT devices, however, is less clear. Traditional products liability principles cannot be seamlessly applied to IoMT devices, given their unique design and extensive supply chains that make it difficult to not only apportion liability but also to determine relevant standards of care.[276] A rigid liability structure risks stifling innovation, but the laissez-faire attitude towards IoMT risks must be combatted with effective incentives to develop secure code and reduce consumer risk.[277] Further, it is necessary that this liability structure be created

---

270. *See* Gomulkiewicz, *supra* note 269, at 394.

271. Daley, *supra* note 31, at 538.

272. DEAN, *supra* note 14, at 9; *see* Merrion, *supra* note 35 ("[E]xperts on the Internet of Things said class-action product liability lawsuits could help pressure manufacturers to build more security into web-connected devices. . . . [L]itigation was mentioned repeatedly as a way to get the attention of web device manufacturers in the near term.").

273. Daley, *supra* note 31, at 538.

274. *Id.* at 541.

275. Detsch, *supra* note 22.

276. *See* Beery & Burns, *supra* note 20; *Untangling the Web*, *supra* note 4.

277. *See* Daley, *supra* note 31, at 537–38; *see, e.g.*, Lemos, *supra* note 18.

with manufacturer input, and not on an ad hoc or case-by-case basis, which risks inconsistent judicially-created standards.[278]

While it is uncertain what a finalized liability framework for IoMT devices may consist of,[279] there are two important steps that should be implemented now to begin building this framework. First, IoMT developers should be prohibited from disclaiming liability for insecure code in end-user agreements. Second, a safe harbor provision should be simultaneously implemented that provides IoMT manufacturers with a defense to liability if they have satisfactorily complied with cybersecurity best practices in developing and marketing their products. These recommendations can help form the basis of a final liability framework while demonstrating an early commitment to holding IoMT device manufacturers accountable for insecure products.

C. Eliminating Liability Disclaimers in End-User Agreements

The first prong of this interim liability proposal requires the elimination of liability disclaimers in end-user agreements for IoMT devices. Software vulnerabilities have cost consumers and businesses tens of billions of dollars annually, yet software developers have refused to take responsibility for the security of their products, and have instead shifted the risk of insecure software to consumers.[280] It is unfair for consumers to shoulder the burden of insecure devices—particularly when such devices can be implanted into consumers' bodies and have life or death consequences—simply because software manufacturers have traditionally been permitted to disclaim liability through end-user agreements.[281] Permitting IoMT manufacturers to evade liability contributes to the weak economic climate that has permitted vulnerable code to develop in the first place.[282]

IoMT manufacturers should therefore not be free of all liability, but instead should be held to reasonable standards of care for their products.[283] IoMT developers are best positioned to identify risks with their software code

---

278. *See* Butler, *supra* note 21, at 927.

279. *See* DEAN, *supra* note 14, at 12 (noting that liability structures take time to develop).

280. Scott, *supra* note 19, at 426–27.

281. *See* Butler, *supra* note 21, at 926; Daley, *supra* note 31, at 538.

282. *See* DEAN, *supra* note 14, at 4; Paez & La Marca, *supra* note 5, at 52–53.

283. Butler, *supra* note 21, at 916 ("[H]olding manufacturers liable for downstream harms caused by their insecure devices is well aligned with the purposes of products liability law—to minimize harm by encouraging manufacturers (as a least-cost-avoider) to invest in security measures."); *see* Detsch, *supra* note 22; *see also* Wenzel, *supra* note 33, at 67 (presenting a similar argument for smart car technology).

and to mitigate those risks during the development process. Yet, the presence of an end-user licensing agreement eliminates any incentive that an IoMT developer has to consider consumer safety and security.[284] Without the risk of liability, and without the presence of mandatory federal standards for IoMT devices, manufacturers can place insecure products on the market without adequate testing and potentially compromise consumer well-being.[285] For any final IoMT liability model to be successful, there must be a foundational understanding among all parties that the failure to implement reasonable security measures into IoMT devices will be grounds for punishment.[286] Elimination of liability disclaimers in end-user agreements for IoMT products is a crucial step in setting the foundation for a future liability framework.[287] Such action will garner substantial attention among IoMT device manufacturers, as it represents a significant shift away from the laissez-faire attitude surrounding software products to date.[288] However, this shift is necessary to establish standards for connected devices that have the potential to cause serious bodily harm or death.

Further, attaching liability to IoMT developers can incentivize businesses to increase their security budgets.[289] Respondents in the Ponemon study indicated that their organizations would increase the security budget for connected medical devices only if a potentially life threatening attack occurred.[290] It is irresponsible to withhold adequate funding for security until tragedy takes place, particularly given that the majority of IoMT manufacturers are already aware of the real-life potential for such attacks.[291] By signaling that IoMT device manufacturers may be held liable for insecure code, the hope is that MedTech organizations will increase funding to strengthen device security now, as a proactive measure, before harmful attacks occur. The reactive model of security in place today fails to adequately protect consumers, and it is time for the incentive of liability to enhance the security environment.[292]

---

284. Daley, *supra* note 31, at 538.

285. Rosenzweig, *supra* note 19; *see* Daley, *supra* note 31, at 538 (describing the current environment of under-investment in software security); *see also Untangling the Web*, *supra* note 4 (discussing the risk of IoT devices caused by manufacturers that fail to provide security measures).

286. *See* Daley, *supra* note 31, at 538.

287. *See, e.g.*, Mitchell, *supra* note 26.

288. Daley, *supra* note 31, at 538.

289. *See* PONEMON INST., *supra* note 179, at 2, 10.

290. *Id.*

291. *Id.* at 1–2; *see* Rosenzweig, *supra* note 19.

292. *See* DEAN, *supra* note 14, at 12.

Indeed, the idea of eliminating disclaimers of liability in end-user agreements has also been recently proposed by Senator Mark Warner of Virginia, a member of the Senate Intelligence Committee.[293] Senator Warner explained that "eliminating software makers' long-held exemption from liability lawsuits could be a key part of a cybersecurity plan," and that a "fulsome debate" is needed regarding "whether the software sector's legal immunity has outlived its usefulness, especially in an age of relentless cyberattacks that frequently exploit software vulnerabilities."[294] Former White House Cybersecurity Coordinator Michael Daniel agreed with Senator Warner that it is time to debate this proposal in Congress, but cautioned that this dialogue should not be generalized to all software.[295] Instead, this "requires a more sectoral approach, such as medical devices or autonomous vehicles."[296] Such arguments and suggestions are in line with the approach proposed in this Article, which advocates for elimination of liability disclaimers in end-user agreements for the IoMT sector only, given the unique risks posed by connected medical devices.

While prohibiting liability disclaimers in IoMT end-user agreements will increase incentives for manufacturers to develop secure code, this action will likely be met with substantial resistance from the software and connected device industries.[297] The software industry has enjoyed protection from liability for decades, and will oppose any change to this status quo.[298] Software manufacturers may argue that the imposition of liability will stifle innovation in a developing field, and that manufacturers will flee the industry.[299] The likelihood of this occurring, however, is slim.[300] Almost all other industries hold manufacturers and developers liable for flaws in their products, and IoMT is projected to revolutionize health care.[301] The

---

293. *See* Mitchell, *supra* note 26.

294. *Id.*

295. *Id.*

296. *Id.*

297. *See id.*

298. Daley, *supra* note 31, at 538, 542 (explaining that protection from liability keeps costs down).

299. Daley, *supra* note 31, at 537, 542; Evans, *supra* note 17; *see also* VITKOWSKY, *supra* note 240, at 16 (explaining that some will argue holding software companies liable for defects will "discourage innovation and growth"); Paez & La Marca, *supra* note 5, at 60 ("Extending strict products liability to software defects could also dramatically obstruct technological progress for the IoT.").

300. *See* Daley, *supra* note 31, at 542.

301. *See* Paez & La Marca, *supra* note 5, at 59; *see also Why You Probably Don't Have Product Liability for the Software You Develop... Yet*, INSUREON: YOU'RE IT (June 21, 2016), https://it.insureon.com/news/why-you-probably-dont-have-product-liability-for-the-software-

elimination of liability protection is unlikely to hinder a rapidly evolving industry, given the numerous players in the market. Instead, the elimination of liability provisions in end-user agreements will likely increase competition among manufacturers to develop more secure products to avoid hefty fines or damages.[302] With manufacturers appropriately incentivized to prioritize security, standards and duties of care can also begin to develop for this industry.[303]

Moreover, as technology changes, liability structures must adapt. Just because policy makers determined that "business productivity software manufacturers should not be held liable for security flaws in their products during the growth period of this industry in the 1990s does not mean all software manufacturers for all applications in all industries should get the same exemption forever."[304] Instead, there must be a balancing of consumer safety with manufacturer liability.[305] As consumer risks increase, technology manufacturers must bear some of the burden for device safety.[306] Because society has entered a new technological age marked by increased cyber risk, it is crucial that liability models progress accordingly.[307]

D. Cybersecurity Safe Harbor

Given that the elimination of liability waivers in end-user agreements will represent a marked change for software and IoMT manufacturers, it is important that these manufacturers not be exposed to unbounded liability. Depending on the final liability model that emerges, it is necessary to guard against the imposition of liability on IoMT developers merely because their products use software code or connect over Internet networks. As noted, there is no defect-free code in existence today, and manufacturers should not be

---

you-develop-yet [https://perma.cc/UX2H-K28C]; Evans, *supra* note 17 (discussing industries that are subject to liability).

302. *See generally* ABBOTT & THE CHERTOFF GRP., WHY MEDICAL DEVICE MANUFACTURERS MUST LEAD ON CYBERSECURITY IN AN INCREASINGLY CONNECTED HEALTHCARE SYSTEM 6 (2018) ("[C]ybersecurity should not function as a competitive differentiator, but as a uniform device enabler."); Rosenzweig, *supra* note 19 (discussing some federal organizations consideration of fines for violating cybersecurity "best practices").

303. *See* Wenzel, *supra* note 33, at 69.

304. Mitchell, *supra* note 26.

305. *See* Detsch, *supra* note 22.

306. *See id.* ("[L]eading digital security experts are calling on US policymakers to hold manufacturers liable for software vulnerabilities in their products in an effort to prevent the bugs commonly found in smartphones and desktops from pervading the emerging IoT space.").

307. *See* DEAN, *supra* note 14, at 12 (noting that liability structures take time to develop); Evans, *supra* note 17.

liable at this stage for device malfunctions, hacks, or hijacks that occur despite the manufacturer's use of cybersecurity best practices and secure product development lifecycles.[308] The purpose of a robust liability framework is, in part, to incentivize the development of secure code.[309] It is not intended to saddle manufacturers with liability risks that no reasonable individual could guard against, even if all proper steps were taken.[310] Thus, a second proposal should be simultaneously adopted with the elimination of liability waivers: cybersecurity safe harbors.[311]

A cybersecurity safe harbor operates by preventing the imposition of liability on device manufacturers that adopt and adhere to recognized industry cybersecurity standards, frameworks, or both.[312] The safe harbor prioritizes proactive cybersecurity measures that protect consumer well-being instead of focusing on the reactive regulatory structure that exists today.[313] These industry frameworks can help fill the gaps that presently exist in cybersecurity and IoMT oversight by HHS and the FDA, and can be more readily and easily updated and amended than statutes or regulations.[314]

Moreover, safe harbors that encourage adoption of industry-developed cybersecurity frameworks enhance the public-private partnership model that has become a cornerstone of cybersecurity policy.[315] By design, cyberspace operates as "a network of both private-sector and public-sector infrastructure" and "requires a continuation of the partnership between the government and companies" to thrive.[316] There are limits to the government's technical skills and ability to develop workable practices for cybersecurity that are best left to industry cybersecurity experts. A partnership approach, such as the one envisioned by safe harbors, can enhance development of the IoMT and

---

308. Paez & La Marca, *supra* note 5, at 59; Beery & Burns, *supra* note 20, at 58.

309. *See* DEAN, *supra* note 14, at 8–10; Scott, *supra* note 19, at 469; Ashton, *supra* note 28, at 834–35; Merrion, *supra* note 35.

310. *See* Scott, *supra* note 19, at 469–70.

311. *See, e.g.*, Daley, *supra* note 31, at 541; Wenzel, *supra* note 33, at 69.

312. *See, e.g.*, OHIO REV. CODE ANN. § 1354.01–.05 (West, Westlaw through Files 1 to 9, immediately effective RC sections of File 10, and Files 11 to 14 of the 133rd General Assembly (2019–2020)).

313. Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 403 (2016) ("[P]ositive cybersecurity law," such as incentives, "requires a shift in thinking from our nation's longstanding mindset in which nearly all cybersecurity laws are punitive.").

314. *See* Davenport, *supra* note 12, at 260; Klein, *supra* note 193.

315. *See* Corbin & Brown, *supra* note 191.

316. Kosseff, *supra* note 313, at 411; *see* U.S. DEP'T OF HOMELAND SEC., EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 4 (2013).

cybersecurity industries without stifling innovation.[317] It is therefore strongly recommended that cybersecurity safe harbors be adopted simultaneously with the prohibition on liability waivers in IoMT end-user agreements.[318]

State legislatures have already begun to recognize the merit in adopting cybersecurity safe harbors. On November 1, 2018, Ohio became the first state to supplement its Data Protection Act with an "incentive-based mechanism to strengthen cybersecurity business practices"—namely a safe harbor against data breach lawsuits for businesses that "implement, maintain and comply with an industry-recognized cybersecurity program."[319] This law, formerly known as S.B. 220, offers protection to any business that accesses, maintains, or processes personal information, so long as the business implements recognized cybersecurity measures that are designed to: (1) protect the security and confidentiality of data; (2) protect against reasonably anticipated threats to the security or integrity of data; and (3) guard against unauthorized access to personal information that is likely to result in a material risk of identity theft or fraud.[320] In exchange for implementing an appropriate cybersecurity framework, businesses receive an affirmative defense to tort actions that arise from alleged "failure[s] to implement reasonable information security controls, resulting in a data breach."[321]

Similarly, New York recently passed the Stop Hacks and Improve Electronic Data Security (SHIELD) Act.[322] The original version of this bill intended to grant a safe harbor to a "certified compliant entity."[323] A "certified compliant entity" is one that meets the independent certification of compliance with government data security regulations (such as HIPAA and

317. *See* Kosseff, *supra* note 313, at 403.

318. *See, e.g.*, Daley, *supra* note 31, at 541.

319. Alysa Austin et al., *Ohio Enacts First Cybersecurity Safe Harbor*, JD SUPRA (Nov. 7, 2018), https://www.jdsupra.com/legalnews/ohio-enacts-first-cybersecurity-safe-80727/ [https://perma.cc/X5CT-8A82]; *see* Data Protection Act, S.B. 220, 132nd Gen. Assemb. (Ohio 2017); OHIO REV. CODE ANN. §§ 1354.01–1354.05 (West, Westlaw through Files 1 to 9, immediately effective RC sections of File 10, and Files 11 to 14 of the 133rd General Assembly (2019–2020)).

320. Austin et al., *supra* note 319.

321. *Id.*

322. N.Y. GEN. BUS. LAW § 899-bb (McKinney 2019) (effective Mar. 21, 2020).

323. S. 6933, 2017–2018 Leg., Reg. Sess. (N.Y. 2017); *cf.* Romaine Marshall & Craig Stewart, *Safe Harbor for Data Security: New York's Proposed Changes Could Be Followed by Other States, Legal Insights*, HOLLAND & HART (Nov. 11, 2017), https://www.hollandhart.com/safe-harbors-for-cybersecurity-new-yorks-proposed-changes-could-be-followed-by-other-states [https://perma.cc/9ARK-BJE3] (describing another New York act, the Stop Hacks and Improve Electronic Data Security Act, as an amendment that includes a safe harbor provision for companies that obtain certification).

Gramm-Leach-Bliley) or recognized industry-approved cybersecurity frameworks, including the ISO/NIST standards.[324] Pursuant to the original legislation, an organization could take advantage of this safe harbor by providing copies of its certification(s) to the Attorney General.[325] The final legislation, however, omitted this broad safe harbor language with respect to limiting liability for certified compliant entities, but still allows certain companies to be deemed compliant with New York's "reasonable safeguards" requirement if they are covered by—and comply with—certain regulations, such as HIPAA.[326] Thus, while there is flexibility in how cybersecurity safe harbors are structured, it is necessary to provide a level of protection to manufacturers as liability increases for insecure IoMT devices. This can incentivize adoption of safer code and more stringent cybersecurity programs by providing a more limited and tailored exception to liability than end-user agreements.[327]

In fact, numerous organizations expressed their support for the development of cybersecurity safe harbors in response to a request for comments issued by the Department of Homeland Security.[328] Tasked with evaluating and recommending incentives to encourage private sector participation in voluntary cybersecurity programs, the Secretary considered liability limitations as part of her review.[329] Organizations of all sizes —including large companies like Microsoft and small start-up companies—

---

324. *See* Marshall & Stewart, *supra* note 323.

325. *See* S. 6933, 2017–2018 Leg.

326. Alejandro Cruz & W. Scott Kim, *New York's SHIELD Act Heads to the Governor's Desk*, JD SUPRA (July 9, 2019), https://www.jdsupra.com/legalnews/new-york-s-shield-act-heads-to-the-49736/ [https://perma.cc/QZY5-HELK].

327. *See generally* Scott, *supra* note 19, at 469 (arguing that imposing liability on software companies will encourage more security measures); Ashton, *supra* note 28, at 834–35 (arguing that incentives will help to produce safer and more consistent security measures for software products); Merrion, *supra* note 35; Rosenzweig, *supra* note 19 (discussing the current use of end-user agreements in software contracts which disclaim liability).

328. *See generally* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 343, 345 (2015) ("The incentive reports issued by the DHS . . . included discussion on some form of limited liability for companies who voluntarily adopt the Framework."); U.S. DEP'T OF HOMELAND SEC., *supra* note 316, at 62 ("A common suggestion among respondents was the need for indemnity, at some level, from liability for security breaches [for] organizations adopting cybersecurity measures."); NAT'L TELECOMM. & INFO. ADMIN., DISCUSSION OF RECOMMENDATIONS TO THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS TO JOIN A VOLUNTARY CYBERSECURITY PROGRAM 11 (2013).

329. U.S. DEP'T OF TREASURY, TREASURY DEP'T REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636, at 2–3, 10–12 (2013).

indicated that liability safe harbors offset the costs of participation in voluntary cybersecurity frameworks and can serve as an effective cost reduction mechanism.[330] These companies further explained that liability protection creates tangible benefits and adds predictability to an otherwise unclear and unsettled area of law.[331] Moreover, these safe harbors recognize the inherent flaws present in all connected devices and signal that targeted IoMT organizations are also victims of cybercrime.[332]

It is important, however, that cybersecurity safe harbors be implemented in *conjunction* with the end-user agreement prohibition, and not as the sole method to enhance device security. The rationale for this is that the adoption of a cybersecurity safe harbor, on its own, fails to incentivize manufacturers to increase the security of their IoMT products. IoMT device manufacturers will still have a shield against liability through end-user agreements. With the ability to contractually limit their liability for insecure code, manufacturers will remain un-incentivized to protect consumer welfare and can continue placing unsecure devices on the market.[333] Additionally, given the limited IoT lawsuits to date, as well as courts' varying interpretations of standing requirements, IoMT manufacturers may question whether such lawsuits can be successfully maintained.[334] An IoMT manufacturer may believe it is cheaper to fight a future lawsuit—with a potential for success at the motion to dismiss stage depending on the jurisdiction and harm suffered by the plaintiff—than to implement a comprehensive cybersecurity program. A recent survey of over 800 companies noted that only 35% of organizations currently view regulatory or liability risk as one of the largest concerns

---

330. *See* Letter from Robert W. Holleyman, II, President & CEO, BSA, to Alfred Lee, NTIA (Apr. 29, 2013).

331. *See* HITRUST, FRAMEWORK FOR REDUCING CYBER RISKS TO CRITICAL INFRASTRUCTURE 3, 10 (2017); Letter from Jim Wunderman, President & CEO, Bay Area Council, to The Honorable Dennis Hightower, Deputy Sec'y, Nat'l Inst. of Standards & Tech. (July 29, 2011).

332. Craig Spiezle, *Uber, Equifax Hacks Signal Need for Accountability and Breach Regulation*, INT'L BUS. TIMES (Dec. 5, 2017), http://www.ibtimes.com/uber-equifax-hacks-signal-need-accountability-breach-regulation-2623606 [https://perma.cc/YVQ6-FHEB].

333. *See* Daley, *supra* note 31, at 538; Lemos, *supra* note 18 ("What we have is an incentive gap, and we are not going to see something different unless we incentivize something different.").

334. *See generally* Doug Olenick, *IoT Liability: Legal Issues Abound*, SC MEDIA (Mar. 30, 2017), https://www.scmagazine.com/iot-liability-legal-issues-abound/article/647579/ [https://perma. cc/U42Y-8CMB] (discussing that "few cases have been filed" regarding IoT liability, so case law is sparse).

associated with poor cybersecurity practices.[335] In the IoMT context, this may be because of the insufficient regulatory structures and ability to contractually avoid liability.[336] Without fear of liability, organizations are not properly incentivized to adopt a voluntary cybersecurity framework.[337] Thus, safe harbors are a crucial component of the new liability framework, but will fail to achieve their purpose if enacted as the sole remedy.

Combining liability and safe harbors into a joint proposal, therefore, offers sufficient incentives for manufacturers to not only continue investing in the IoMT industry, but to also adopt appropriate cybersecurity frameworks and strengthen the code that is used in connected medical devices.[338] This model represents an appropriate balancing of consumers' need for safer products with manufacturers' need to prevent unlimited liability in a nascent industry with ever-evolving standards.[339] By taking these first two steps towards creating a comprehensive IoMT liability structure, the legislature can demonstrate its commitment to medical device security while helping the industry grow in a safe and secure manner.

V. CONCLUSION

It is undeniable that IoMT is set to revolutionize the healthcare industry and redefine standards for patient care. Utilizing its connectivity to monitor chronic patient conditions and increase care convenience, IoMT contains fascinating new opportunities, with manufacturers only scratching the surface to date. As IoMT becomes more readily adopted, however, it presents challenges with respect to device security and patient safety that can result in consumer harm or death.[340] With risks for data breaches, hacks, and hijacking increasing in the medical industry, it is essential that IoMT manufacturers create secure products that do not expose consumers to unnecessary

---

335. CTR. FOR STRATEGIC & INT'L STUDIES, TILTING THE PLAYING FIELD: HOW MISALIGNED INCENTIVES WORK AGAINST CYBERSECURITY 3, 7 (2017).

336. *See* Lemos, *supra* note 18.

337. *See Carrots for Cybersecurity*, BLADE (Dec. 4, 2017), http://www.toledoblade.com/Editorials/2017/12/04/Carrots-for-cybersecurity.html [https://perma.cc/77UT-L6WT]; *see also* U.S. DEP'T OF HOMELAND SEC., *supra* note 316, at 62.

338. *See, e.g.*, DEAN, *supra* note 14, at 8–10 (explaining that liability incentivizes developers to weigh the cost of mitigating known defects with the potential for large damages); Ashton, *supra* note 28, at 834–35; Merrion, *supra* note 35.

339. *See generally* Detsch, *supra* note 22 (explaining the need to balance the security of consumers with the technology development of software companies).

340. *See supra* Part I.

vulnerabilities and risks.[341] Unfortunately, given the legal and regulatory frameworks in place, appropriate incentives do not exist for IoMT manufacturers to prioritize device security.[342] Manufacturers may avoid liability through end-user agreements and can fall outside the bounds of regulatory oversight by HHS and FDA.[343] As new devices proliferate on the market, however, it is essential that a comprehensive liability structure be created to incentivize adoption of cybersecurity best practices and provide relief to injured consumers.

The two-prong approach to liability proposed in this Article operates as a foundation for the broader IoMT liability discussion and ultimate liability framework. This interim proposal creates incentives to secure IoMT products by eliminating manufacturers' ability to disclaim liability and proposing the adoption of safe harbors that can restrict liability to reasonable levels if manufacturers comply with voluntary cybersecurity frameworks.[344] The goal is to signal a strong interest by the legislature in holding IoMT manufacturers accountable for the security of their products while recognizing the reality that no IoMT device will ever be 100% secure. Further, by implementing these two steps now, the legislature can help foster a dialogue on what the ultimate IoMT liability framework should consist of, and can encourage, IoMT manufacturers to participate in this discussion at an early stage. This prevents the imposition of an ad hoc liability framework by the judiciary.[345] The adoption of a comprehensive IoMT liability structure will result in consistency and predictability for manufacturers while benefiting consumers through safer code and remedies for unreasonably insecure devices.

---

341. *See* Lemos, *supra* note 18.

342. *See id.*; DEAN, *supra* note 14, at 4; Paez & La Marca, *supra* note 5, at 52–53.

343. *See supra* Part III.

344. *See* DEAN, *supra* note 14, at 8–9; Scott, *supra* note 19, at 469; Daley, *supra* note 31, at 538.

345. *See* Butler, *supra* note 21, at 927 (noting that without clear guidance, IoT tort outcomes by courts come become random).