CLOSING THE CYBERSECURITY GAP IN MEDICAL DEVICES – PROPOSING A SAFE HARBOR SYSTEM

ALLEE JOHNSON†

Over the last decade, the number of medical devices on the market have skyrocketed. While these devices allow for a better quality of life for their recipients, they come with their own host of concerns. Patients have been consistently victimized by data breaches, which expose their personal health information for the world to see.

Unfortunately for these patients, the adequate compliance and litigation tools do not exist to remedy the problem. The National Institute of Standards and Technology ("NIST") are experts in the field, creating benchmarks for companies to follow regarding cybersecurity. However, reports show that over 44% of medical devices do not comply with National Institutes of Standards and Technology ("NIST standards"). There are no mandatory regulations in place to tackle the rampant security issues in post-market devices.

The Food and Drug Administration ("FDA") is tasked with regulating the safety and efficacy of medical devices in the United States, so it is important for the administration to release new regulations to tackle security issues in post-market devices. The FDA should create a safe harbor regulation, requiring medical device manufacturers to comply with a series of security standards for post-market devices. If manufacturers fail to comply with the safe harbor, they could be held liable for any data breach affecting victims.

† J.D. Candidate, University of Colorado, Class of 2022; B.A., The University of Texas at Austin, Class of 2019. I would like to thank every person on CTLJ and in the sector who has reviewed, discussed, and edited this Note. I would like to dedicate this paper to Ayden Blotnick, whose curiosity and ardor for medical devices inspired my passion for this research. I could not have done it without you.

INTRODUCTION

For the approximately 500,000 individuals in the United States living with implanted cardiac devices,[1] these devices have vastly improved their quality of life. But what if these life-enhancing devices could be infiltrated by bad actors, causing data breaches, injuries, or even death? Unfortunately for patients, this is reality. Cardiac device manufacturers have not only failed to protect the valuable patient information within these devices, but have also blatantly ignored known cybersecurity issues within devices, placing profits over patients.[2] In 2017, an FDA investigation found that St. Jude's

1. BARBARA G. SILVERMAN ET AL., THE EPIDEMIOLOGY OF PACEMAKER IMPLANTATION in THE UNITED STATES 42 (1995).

2. *MW Statement on STJ/ABT Acknowledgment of Cyber Vulnerabilities*, MUDDY WATERS RSCH., https://www.muddywatersresearch.com/research/stj/stj-abt-acknowledgement/ [https://perma.cc/KS7K-AGPE]

(now Abbott) implantable cardiac pacemakers running legacy software could fall victim to unauthorized users with very minimal effort and equipment.[3] If an unauthorized user were to access the device, then they would have that patient's personal information.[4] Even worse, an unauthorized user could modify the pacemaker's electrical signals, which could result in patient injury or death.[5] A staggering 465,000 devices in the United States are mpacted by this vulnerability.[6] Sadly, the described cybersecurity issues are not only rampant within Abbott devices, but within the legacy medical devices as a whole. As of 2020, 70% of medical devices within the United States are considered legacy medical devices, meaning that the devices are no longer supported in some capacity.[7] To better protect vulnerable patients, the FDA should create a safe harbor system for medical device manufacturers to ensure that devices meet a minimum-security threshold.

Specifically, the FDA should require that manufacturers: (1) engage in cybersecurity information sharing and monitoring, (2) promote good cyber hygiene, (3) assess post-market vulnerability information, (4) employ a risk-based approach to characterizing vulnerabilities, and (5) implement necessary cybersecurity actions in a timely fashion. Should a manufacturer fail to comply with these safe harbor standards, they could be held liable for resulting harms to patients. In order to understand why a safe harbor provision is needed, this paper discusses important background information concerning legacy devices, current legal medical device security regulations, the workings of this proposed safe harbor system, and explains why

(last visited Sept. 28, 2021).

3. *See* U.S. FOOD & DRUG ADMIN., FIRMWARE UPDATE TO ADDRESS CYBERSECURITY VULNERABILITIES IDENTIFIED IN ABBOTT'S (FORMERLY ST. JUDE MEDICAL'S) IMPLANTABLE CARDIAC PACEMAKERS: FDA SAFETY COMMUNICATION (2017), https://wayback.archiveit.org/7993/20201222110125/https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals [https://perma.cc/2LGF-EERB].

4. *Id.*

5. *Id.*

6. *Id.*

7. Jessica Davis, *Majority of Healthcare Medical Devices Operate on Legacy Systems*, HEALTH IT SECURITY (May 15, 2019), https://healthitsecurity.com/news/majority-of-medical-devices-are-running-on-legacy-systems [https://perma.cc/QJG8-BXNH].

a safe harbor system is the best method to guarantee device security.

I. BACKGROUND

A. The Role of Legacy Devices in the United States

The vast majority of devices in the United States are considered "legacy devices."[8] For the purposes of this article, legacy medical devices are devices that include outdated software or equipment or are obsolete in some other fashion. In the medical device industry, it is common for a legacy device to run software that is no longer supported or patched by the manufacturer.[9] For example, in 2019, Microsoft announced that it would phase out support for Microsoft 7 and Windows 2008.[10] After this phase out date passed, Forescout Research Labs, a cybersecurity consultant group, found that as many as 34% of medical devices still utilized software that was no longer up to date, qualifying them as legacy devices.[11]

Devices can also be rendered legacy devices if it includes physical components that are more than ten years old, making them difficult or expensive to maintain.[12] Legacy medical devices are particularly important for cybersecurity, because they are inherently more vulnerable to attacks and make up a large portion of the devices in the United States.

Legacy medical devices also collect a vast wealth of information.[13] Depending on the exact device, doctors, manufacturers, and even insurers may have access to sensitive patient data such as information about heart arrythmias, blood

8. *Id.*

9. *Legacy Device*, TECHNOPEDIA, (Feb. 16, 2017) https://www.techopedia.com/definition/2230/legacy-device [https://perma.cc/R7UQ-5BGZ]

10. https://www.forescout.com/resources/connected-medical-device-security-a-deep-dive-into-healthcare-networks/ [https://perma.cc/PRZ3-XAKQ].

11. https://www.forescout.com/resources/connected-medical-device-security-a-deep-dive-into-healthcare-networks/ [https://perma.cc/PRZ3-XAKQ].

12. James Crotty & Ivan Horrocks, *Managing Legacy System Costs: A Case Study of a Meta-assessment Model to Identify Solutions in a Large Financial Services Company*, 13 APPLIED COMPUTING AND INFORMATICS 175 (2017).

13. Marshall Allen & Derek Kravitz, *Your Medical Devices Are Not Keeping Your Health Data to Themselves*, PROPUBLICA (Nov. 21, 2018, 5:00 AM), https://www.propublica.org/article/your-medical-devices-are-not-keeping-your-health-data-to-themselves [https://perma.cc/BTN6-MREF].

sugar levels, calorie intake, activity levels, and more.[14] Additionally, both medical device manufacturers and practitioners record this particular data in conjunction with sensitive patient information, including the patient's name, date of birth, medical ID information, and social security numbers.[15] Given the enormity of the patient data collected, the sensitivity of that information, and the technological vulnerability of legacy medical devices, the FDA ought to consider implementing a safe harbor swiftly.

B. Prevalence of Medical Device Cybersecurity Breaches & Vulnerabilities

In 2017, hundreds of thousands of medical devices were impacted by vulnerabilities.[16] In 2020, that number steadily rose, meaning that medical device breaches are becoming more and more common. As a result, bad actors are able to access a vast wealth of information. Even worse, unauthorized actors can adversely affect a device user's medical treatment, potentially resulting in severe injury or death. In 2020, IBM researchers discovered a vulnerability in Thales' insulin pumps where bad actors could alter the amount of insulin that the device delivered to patients.[17] Additionally, hackers could manipulate the device's readings that are shown to the patients. As a consequence, patients may choose to alter their dose of insulin when it is not needed.[18] Obviously, this is incredibly concerning and potentially life-threatening to diabetes patients. However, Thales did not disclose exactly which models of insulin pumps are affected by this security flaw.[19]

Of course, Thales does not want to signal exactly which models of pumps may be vulnerable to bad actors, as this would make it easier for bad actors to utilize these security flaws.[20] Both the Thales insulin pumps, and Abbott cardiac device incidents illustrate the pervasive major cybersecurity

14. *Id.*
15. *See id.*
16. *See* U.S. FOOD & DRUG ADMIN., *supra* note 3.
17. Greg Slabodkin, *Insulin pumps among millions of devices facing risk from newly disclosed cyber vulnerability, IBM says*, MEDTECH DIVE (Aug. 25, 2020), https://www.medtechdive.com/news/insulin-pumps-among-millions-of-iot-devices-vulnerable-to-hacker-attacks/584043/ [https://perma.cc/57BX-92DG].
18. *Id.*
19. *Id.*
20. *Id.*

vulnerabilities in legacy medical devices. Given the scope of the impacted devices, it is simply a matter of time before a legacy device patient suffers severe harm, injury, or even death due to insufficient security protections.

C. Medical Device Manufacturers' Current Cybersecurity Compliance Statuses

Despite an increase in the number of cyber-attacks on medical devices, manufacturers have consistently failed to conform to NIST cybersecurity framework standards previously recommended by the FDA.[21] In fact, the healthcare sector records the lowest NIST cybersecurity conformance rate of any studied sector within the report, with only 44% of healthcare providers conforming to NIST cybersecurity standards. [22] According to researchers, medical device providers improved their conformance to these standards by a mere 1% over the course of a year, spanning from 2018 to 2019.[23]

CynergisTek, a healthcare cybersecurity consulting firm, reported not only incredibly low rates of compliance, but a regression of compliance from 2017 to 2019.[24] Importantly, CynergisTek studied all actors within the healthcare sector, not only medical device manufacturers.[25] In order to gauge compliance, CynergisTek researchers employ the COBIT Maturity Model.[26] The COBIT Maturity Model is a scheme that evaluates a company's cybersecurity effectiveness by using a range from one to five.[27] Level Zero represents a company that does not have security plan, or only an unpredictable one.[28]

---

21. Jessica Davis, *Just 44% of Healthcare Providers Meet NIST Cybersecurity Standards*, HEALTHITSECURITY (Sept. 23, 2020), https://healthitsecurity.com/news/just-44-of-healthcare-providers-meet-nist-cybersecurity-standards#:~:text=September%2023%2C%202020%20%2D%20Only%2044,report%20from%20security%20firm%20CynergisTek [https://perma.cc/KFD3-ANEU].

22. *Id.*

23. *Id.*

24. *Moving Forward: Setting the Direction*, CYNGERISTEK (Sept. 17, 2020), https://insights.cynergistek.com/information-security-officer/2020-annual-report [https://perma.cc/Z7DT-WA63].

25. *Id.* at 1.

26. *Id.* at 26.

27. *CMMI Levels of Capability and Performance*, ISACA, https://cmmiinstitute.com/learning/appraisals/levels [https://perma.cc/B6XS-MXM7].

28. *Id.*

Level One represents a company that has an unpredictable and reactive IT management strategy.[29] Level Two reflects a company that consistently manages small projects.[30] Level Three is a company that has a proactive, not reactive strategy.[31] Level Four is an organization that is data-driven and meets predictable security objectives.[32] Finally, Level Five is an organization that is focused on consistent improvement and is able to innovate their security strategy.[33]

The CynergisTek report found that medical devices and applications manufactures had an average maturity score of 1.8 in 2019, well below the ideal mark of three.[34] In fact, the sector's collective score decreased by 0.3 between 2018 and 2019.[35] The report aptly states that a failure to "continually improv[e] security in today's threat environment is the same as doing nothing and it is not a sustainable model for risk reduction."[36] It is clear that manufacturers have little incentive to implement security measures for legacy devices, because the devices have already been sold to clients and do not generate active revenue for the manufacturers.[37] Despite the FDA's continued guidance on the issue of cybersecurity, the industry as a whole has failed to take appropriate action, signaling that guidance alone is not sufficient.

II. CURRENT LEGAL CLIMATE RELATING TO THE MEDICAL DEVICE INDUSTRY

Traditional tort claims do not provide protection to medical device recipients, because victims' suits are often dismissed at the pleading stage. Additionally, current device regulations fail to remedy current device security vulnerabilities, because the FDA cannot create additional requirements for devices that have previously been approved.

29. *Id.*
30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.*
34. CYNERGISTEK, *supra* note 24, at 30.
35. *Id.*
36. *Id.* at 20.
37. Fred Donovan, *AHA: Medical Device Makers Falling Short on Securing Legacy Devices*, HITINFRASTRUCTURE (Apr. 4, 2019), https://hitinfrastructure.com/news/aha-medical-device-makers-falling-short-on-securing-legacy-devices [https://perma.cc/TTP8-N6CH].

A. The Food and Drug Administration is Currently Unable to Regulate Legacy Medical Devices in any Meaningful Way

The Food and Drug Administration is tasked with regulating cybersecurity standards in the medical device industry as a whole. New devices seeking FDA approval must meet certain security standards in order to be approved for public use.[38] Additionally, medical devices using the abbreviated §510(k) approval process must meet the same stringent security standards as new devices.[39]

Importantly, the FDA is unable to regulate legacy devices that the agency approved prior to implementing any security requirements if the device is still in use to this day.[40] This means that the vast majority of devices on the market currently are not required to meet any government-regulated standards.[41] In 2016, the FDA released guidance concerning the regulation of post-market medical devices' security, but this is not binding.[42] While the guidance is a welcome shift in the regulation of the industry, if the FDA wants to ensure that manufacturers embrace the spirit of the guidance, the agency should implement a safe harbor system.

B. Victims Find Varied Degrees of Success When Bringing Traditional Tort Suits Against Companies That Retain Information, Creating Inequity in the Pursuit of Justice

Suing a device manufacturer under a traditional tort remedy in the United States has proven to be a difficult task for those harmed by breaches of medical devices. In order to bring any type of tort claim, including public disclosure of private fact,

38. 21 C.F.R. §807.81(a)(1)–(3) (2007), https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?FR=807.81 [https://perma.cc/J6ST-K493].

39. 21 C.F.R. §807.92 (2007), https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?fr=807.92 [https://perma.cc/Y42D-UXFL].

40. *See generally* U.S. FOOD & DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 8 (2016), https://www.fda.gov/media/95862/download [https://perma.cc/S8U9-T7BV].

41. *See* 21 C.F.R. § 10.115(d)(2) (West 2018).

42. U.S. FOOD & DRUG ADMIN., *supra* note 3 at 2, 4, 5.

simple negligence, or intrusion upon seclusion, a plaintiff must prove that they have standing to bring the claim.[43] To have standing, a plaintiff must prove: 1) injury in fact; 2) causation; and 3) redressability.[44]

As is the case in *Spokeo,* it is often difficult for claimants to prove injury in fact in data breach cases.[45] In order to prove this element of standing, plaintiffs must show that they have suffered a "concrete and particularized" and "actual or imminent" harm to a legally protectable interest.[46] The *Spokeo* case defines a particularized harm as one that affects the plaintiff in a personal manner.[47] Additionally, the Court notes that in order to satisfy the concrete harm, the harm must be "real, not abstract."[48]

Robins, the plaintiff in *Spokeo*, sought remedy under Fair Credit Reporting Act (the "FCRA") after a reporting website, Spokeo, had incorrectly reported a plethora of information about him, but he failed to note any ways in which the false information had already affected him.[49] The Court held that Robins did not have standing to bring suit, because his harms were not concrete in nature.[50] Instead, the court determined that Robins alleged no more than "mere procedural violation," under FCRA, because he could only argue that a harm could occur to him in the distant future.[51] As explained in *Spokeo*, it is often difficult for plaintiffs to show that they have a concrete harm if they can only claim that they may be injured in the future or the victim of data theft as a result of a future, rare, medical device hack.

It is true that certain district courts have previously considered activities such as having to monitor credit reports and receiving spam phone calls following a data breach to be sufficient harm to establish standing, but this is not the case in every jurisdiction.[52] In the preliminary stages of *Bass v. Facebook, Inc.*, for example, the court considered a motion to dismiss for lack of standing against the two plaintiffs and,

43. Ashcroft v. Iqbal, 556 U.S. 662, 664 (2009).
44. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
45. *See id.* at 1547–48.
46. *Id.* at 1548.
47. *Id.*
48. *Id.*
49. *Id.* at 1550.
50. *Id.*
51. *Id.* at 1549.
52. *See* Bass v. Facebook, Inc., 394 F. Supp. 3d 1024, 1036 (N.D. Cal. 2019).

bizarrely, reached a different holding for each individual.[53] The court held that Adkins's claim survived the motion, while Bass's claim did not.[54] The court distinguished the two plaintiffs, stating that Adkins received a breach notification from Facebook, while Bass did not.[55] Regardless of this fact, the court found that "where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiff's."[56] Ironically, both plaintiffs, prior to Bass's dismissal, in theory suffered the same injury-in-fact, being more open to future misuse of their respective information, and yet, were subjected to different judicial standards. Even within the same circuit that generally recognizes future fraudulent activity as an injury, in fact, data breach victims are often left with no remedy.[57]

Further, not every circuit recognizes the possibility of future fraudulent activity or other harms stemming from data breaches as an injury-in-fact. In *Beck v. McDonald*, the court dismissed the plaintiffs' case on the basis of lack of standing, holding that the class did not suffer an injury-in-fact.[58] There, a laptop was stolen from the Veterans' Administration Hospital in Columbia, South Carolina.[59] This laptop contained valuable, unencrypted patient information, including names, birth dates, the last four digits of social security numbers, age, race, and various other medical information.[60]

Like the plaintiffs in *Bass*, Beck, along with the class he represented, claimed that there was a higher likelihood of fraud or identify theft as a result of the breach.[61] Unlike *Bass*, this court found that the class did not adequately establish a substantial risk of harm, despite the offering evidence that at least 33% of those that have been affected by the breach will later become victims of identity theft.[62] The court arbitrarily

53. *Id.* at 1040.
54. *Id.*
55. *Id.* at 1036.
56. *Id.* at 1035 (quoting Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016)).
57. *See id.*
58. Beck v. McDonald, 848 F.3d 262, 277 (4th Cir. 2017).
59. *Id.* at 266–67.
60. *Id.* at 267.
61. *Id.* at 266–67.
62. *Id.* at 276.

found that at least 80% of the data breach victims must be later harmed in order to create standing.[63]

Although the above cases survey the reality of data breach claims within the U.S. justice system generally, the cases also offer valuable insight into the struggles that medical device users would realistically face if they were to bring suit against a manufacturer who fails to appropriately secure its device. Simply put, many medical device breach victims are unable to seek traditional remedy for very real harms, depending on where plaintiffs bring suit. This circuit split is not conducive to the administration of justice for all citizens, nor is it conducive to incentivizing manufacturers to reduce cyber vulnerabilities.

III. THE FDA SHOULD CREATE A SAFE HARBOR, SHIELDING DEVICE MANFUFACTURERS FROM LIABILITY IF THEY MEET CERTAIN CYBERSECURITY STANDARDS

The FDA has already released well-researched voluntary guidance to help device manufacturers manage post-market security risks, which could serve as the basis of the safe harbor system.[64] Specifically, the FDA suggests a proactive, risk-based approach to security by "engaging in cybersecurity information sharing and monitoring, promoting "good cyber hygiene" through routine device cyber maintenance, assessing post-market information [regarding vulnerabilities], employing a risk-based approach to characterizing vulnerabilities, and timely implementation of necessary actions."[65] To create the safe harbor, the FDA should require manufacturers to engage in the above standards. If the manufacturers meet the standards proposed in the safe harbor, then they will be shielded from potential liability resulting from data breaches or device vulnerabilities. However, if a company fails to meet the standards laid out in the safe harbor, then it could be held liable for that failure.

A. Information Sharing and Monitoring

Information sharing and monitoring is one of the most critical factors to ensuring greater security in the medical device

63. *Id.*
64. U.S. FOOD & DRUG ADMIN., *supra* note 3 at 4.
65. *Id.* at 6.

industry.[66] As such, the FDA has promoted the development and use of Information Sharing Analysis Organizations ("ISAOs").[67] These organizations facilitate the gathering of device vulnerabilities and ensure that this information can be shared between manufacturers that are involved in the device creation.[68] Device manufacturers' participation in this type of information sharing is critical, because it creates cyber resilience for all parties involved.[69]

ISAOs, in particular, are helpful because the organization's goal is to promote the sharing of information across different industries.[70] The medical device industry is particularly collaborative, meaning that manufacturers often source hardware or software from other manufacturers. In fact, some of the vulnerabilities within medical devices stem from the third party's product. ISAOs help rectify third party vulnerability risks by ensuring that both parties are aware of potential vulnerabilities and can collaborate in order to remediate these issues.

B. Maintaining Good Cyber Hygiene

Medical device manufacturers should ensure good cyber hygiene by routinely conducting device maintenance. In order to conduct proper maintenance, manufacturers must document which software programs and hardware devices are currently utilized.[71] Once manufacturers compile this information, they should then scrutinize the list for potential vulnerabilities.[72] Because legacy medical devices use decades-old software and hardware, the list of vulnerabilities is ever-growing and should be revisited often.[73] Based on the list of possible vulnerabilities, the manufacturer should consider: implementing a cyber

66. *Id.* at 7.

67. *Id.*

68. *Id.*

69. *ISCACS v. ISAOs: SUPPORTING THE CYBERSECURITY INFORMATION SHARING ECOSYSTEM*, ADVANCED CYBER SECURITY CENTER (Nov. 26, 2018), https://www.acscenter.org/blog/isac-vs-isao-supporting-the-cybersecurity-information-sharing-ecosystem [https://perma.cc/A3PD-WH8K].

70. *Id.*

71. Chris Brook, *What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More*, DIGITAL GUARDIAN (Oct. 6, 2020), https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more [https://perma.cc/KFU4-9339].

72. *Id.*

73. *Id.*

security framework, monitoring the number of users that have access to certain information, analyze whether software can be updated or patched to resolve the vulnerability, and when possible in certain medical devices. Ultimately, good cyber hygiene takes place when a manufacturer creates a cyber management plan, sets appropriate time frames for the plan, and actually follows the plan accordingly.[74]

C. Assessing Post-market Information

It is important for manufacturers to assess post-market information in their legacy device systems, as this will allow the company to focus its attention on the most vulnerable areas of the device.[75] However, it can be difficult for companies to assess post market information in any meaningful way due to the sheer amount of information collected amongst their devices.[76] Thus, the FDA recommends that manufacturers employ the common vulnerability scoring system for scoring various vulnerabilities.[77] The framework consists of three data points: 1) base score; 2) temporal score; and 3) environmental score.[78]

In order to derive a score using the system, a medical device would first receive a base score using the metrics listed in Table 1 below.[79] Then, an evaluator would assign appropriate values for temporal and environmental factors.[80] After assigning values to all applicable metrics located in Table 1, the evaluator produces a complex vector, which in turn, results in the final score.[81]

The base group represents the vulnerabilities in the device, no matter the time or environment.[82] This group is further

74. *Id.*

75. U.S. FOOD & DRUG ADMIN., *supra* note 40 at 4.

76. *Id.* at 16.

77. *Id.* at 28.

78. *Common Vulnerability Scoring System v3.1: Specification Document*, FIRST, https://www.first.org/cvss/v3.1/specification-document [https://perma.cc/2P9V-K4JU] (last visited Sept. 28, 2021).

79. *See id.*

80. *Id.*

81. *Id.* (for example, a "vulnerability with Base metric values of "Attack Vector: Network, Attack Complexity: Low, Privileges Required: High, User Interaction: None, Scope: Unchanged, Confidentiality: Low, Integrity: Low, Availability: None" and no specified Temporal or Environmental metrics would produce the following vector [for evaluation]:
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N"

82. *Id.*

broken down into two subparts – exploitability metrics and impact metrics.[83] Exploitability metrics explore the ease and technical means required to exploit a vulnerability in the device, looking specifically at the characteristics inherent to the device that create the vulnerability.[84] Impact metrics explore the direct consequences of any inherent vulnerability.[85]

The temporal group accounts for the capacity for vulnerability to change across time.[86] Essentially, this category measures the state of the exposed vulnerability and if an existing patch could remedy the issue.[87]

The vulnerability scoring system's environmental category refers to unique vulnerability challenges or benefits that may exist as a result of the device's location, either physically or within a larger system of devices.[88] For example, if the medical device's network prevented certain types of attack that otherwise would be problematic, the device could receive a higher score.[89]

D. Timely Implementation of Necessary Action

Finally, and most importantly, companies must implement necessary action within a timely manner in order to qualify for the FDA's safe harbor. The implementation of necessary action can take many different forms.[90] Where possible, manufacturers should augment its device in such a manner that the vulnerability is repaired. This could include creating a new patch for the particular vulnerability, replacing hardware in devices where possible, or simply updating the device's operating system. However, the implementation of action could take other forms, particularly when there is no known fix for the device.

83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *See id.*
90. *See generally* WORLD HEALTH ORGANIZATION (WHO), *GUIDANCE FOR POST-MARKET SURVEILLANCE AND MARKET SURVEILLANCE OF MEDICAL DEVICES, INCLUDING IN VITRO DIAGNOSTICS*, 9789240015326 (2020), https://apps.who.int/iris/bitstream/handle/10665/337551/9789240015319-eng.pdf?sequence=1&isAllowed=y [https://perma.cc/4AFB-NB97].

For example, when a manufacturer learns of an unrepairable, material vulnerability, it may be necessary to recall the device entirely. Or the manufacturer may need to continually monitor the potential vulnerability to ensure that it is not utilized and alert device users that there is a certain vulnerability that cannot be remedied. Importantly, some vulnerabilities simply cannot be remedied after implementation because the device is inside of a patient, making removal and modification extremely costly and potentially life-threatening. Ultimately, the question of necessary action is an inherently fact-based inquiry, and the FDA should afford device manufacturers discretion concerning what measures should be taken, so long as the manufacturer's primary focus is on its patients' care.

E. Liability Trigger for Manufacturers

Importantly, if a medical device manufacturer fails to satisfy any of the above standards for a particular device, the creators of that specific device should be held liable. It is incredibly important for device creators to conform to all of the standards, because a diverse range of tools is the only way to prevent patient harm arising out of vulnerability concerns.

IV. A COMPARISON OF A SAFE HARBOR APPROACH VS. OTHER REGULATION METHODS

Of course, there are many other potential approaches to regulating the cybersecurity standards of legacy medical devices. While any method of regulation is welcome in this area, this section discusses why a safe harbor system is the best method to tackle the issue at hand.

A. Other Methods of Enforcing Cybersecurity Standards are Inadequate

Some advocates of legacy medical device cybersecurity reform commonly float the idea of trading "cash for clunkers," based on the former cash for clunker automobile program.[91] In

91. U.S. Dep't of Health and Human Services, HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY 29 (2017),

fact, the Healthcare Industry Cybersecurity Task Force advocated for this type of program in its Report on Improving Cybersecurity in the Health Care Industry.[92] Specifically, the task force recommends that thengovernment creates incentives to phase out legacy medical devices, but does not elaborate further on any potential program.[93] The task force references one bill in its report that could be used to create the incentive program. [94] However, this bill in its current form mainly helps the federal government in modernizing its own cybersecurity, mentioning nothing about legacy medical device modernization specifically.[95]

There is a plethora of other difficulties related to an incentive program for medical devices. To begin, Congress has been incredibly slow to act on the issue. Over the last few years, medical device breaches remained on the rise, but Congress has taken no meaningful action to ffOf course, Congress is not entirely to blame. Software within medical devices can become outdated in only a few years from the start of implementation.[96] This quick turnover could be incredibly difficult for Congress to grapple with, as members would have to create broad legislation that can actually address minute, technical issues. Additionally, this quick turnover can create a reoccurring issue that a cash for clunkers may not be able to solve for in its own right. Even if Congress is able to create such a program and phase out millions of devices, within a few years, hundreds of thousands, if not millions of devices will be considered legacy medical devices, because they are no longer supported in some capacity. If Congress were to only authorize this type of program in a vacuum, without post-market regulation of legacy devices, it would likely have the same problem on its hands in a decade, with not much to show for itself.

B. The Safe Harbor Proposal is the Optimal Balance

https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf [https://perma.cc/6LTJ-HRK9].

92. *Id.*

93. *Id.*

94. *Id.* at 43.

95. *See* Information Technology Modernization Centers of Excellence Program Act, Pub. L. No. 116–194, 134 Stat. 981 (2020).

96. *See* Davis, *supra* note 7.

Between Patient and Manufacturer Interests

FDA oversight coupled with a flexible safe harbor system would create a much more effective system than other alternatives. The FDA is an expert regulatory body in the realm of medical devices and their security. The FDA has previously released guidance for legacy medical devices that is proven to vastly reduce potential vulnerabilities, meaning that the FDA already has the tools and experts in place to ensure the program's success.[97] Ultimately, in a world where technology is rapidly changing, the FDA must be empowered to regulate these changes in a flexible manner.

It is important to provide a safe harbor to medical device manufacturers, because breaches are inevitable.[98] In fact, a cyberattack is not just a question if the attack will occur, but when it will occur.[99] In light of this, it is important to provide medical device manufacturers with some degree of lessened liability. If a company does everything in its power to mitigate cybersecurity vulnerabilities, but still falls victim to an attack, it would be unfair to hold the company liable for this. Therefore, the FDA should not implement a strict liability model.

CONCLUSION

Ultimately, device manufacturers, regulatory bodies, and current law have failed to ensure that legacy medical devices meet fair, necessary cybersecurity standards. As such, patients have been subjected to risk of which they are largely unaware. Thus, a flexible standard, such as a safe harbor with certain cybersecurity standards is necessary to move the industry forward and to ensure compliance.

97. *FDA 101: An Overview of FDA's Regulatory Review and Research Activities*, U.S. FOOD & DRUG ADMIN. (Jul. 7, 2020), https://collaboration.fda.gov/pz3amek9omjo/ [https://perma.cc/822R-ZH2M] (at 2:46:46).

98. David Barton, *Manufacturers Must Prepare for the Inevitable Data Breach*, INDUSTRYWEEK (Nov. 25, 2014), https://www.industryweek.com/technology-and-iiot/article/21964213/manufacturers-must-prepare-for-the-inevitable-data-breach [https://perma.cc/CZ3P-8NA7].

99. *Id.*