Nova Law Review

Volume 41, *Issue* 3 *Article* 7

Cardiac Defibrillators Need To Have A Bulletproof Vest: The National Security Risk Posed By The Lack Of Cybersecurity In Implantable Medical Devices

Michael Woods*

*

Copyright © by the authors. *Nova Law Review* is produced by The Berkeley Electronic Press (bepress). http://nsuworks.nova.edu/nlr

Cardiac Defibrillators Need To Have A Bulletproof Vest: The National Security Risk Posed By The Lack Of Cybersecurity In Implantable Medical Devices

Michael Woods

Abstract

Imagine a world where a patient wearing a pacemaker or an insulin pump, just fine moments before, drops dead after his implanted medical device turns seemingly against him.

KEYWORDS: medical, devices, privacy

CARDIAC DEFIBRILLATORS NEED TO HAVE A BULLETPROOF VEST: THE NATIONAL SECURITY RISK POSED BY THE LACK OF CYBERSECURITY IN IMPLANTABLE MEDICAL DEVICES

MICHAEL WOODS*

I. INTRODUCTION

Imagine a world where a patient wearing a pacemaker or an insulin pump, just fine moments before, drops dead after his implanted medical device turns seemingly against him.[1] Worse yet, imagine that an insulin

*. Michael Woods received his J.D. from Nova Southeastern University, Shepard Broad College of Law, and his LL.M. in National Security & U.S. Foreign Relations from the George Washington University Law School. He is grateful for his family and friends for their love and support throughout law school. Michael would like to thank Professors Kathy Cerminara, James Levy, Michael Richmond, and Randolph Braccialarghe for being a great influence on his legal education.

1. *See Homeland Security Investigating Medical Device Cybersecurity*, IHEALTHBEAT (Oct. 23, 2014), http://web.archive.org/web/20141028015215/http://www.ihealthbeat.org/articles/2014/10/23/homeland-security-investigating-medical-device-cybersecurity.

pump is giving false readings and a user relying on the readings injects too much insulin, thus being the instrument in his or her own demise.[2] These examples can be the work of malicious actors who hack into implanted medical devices, which has been possible for years.[3] The federal government has done little to regulate any type of cybersecurity on implantable medical devices, despite knowing that hacking these devices has been possible for almost a decade.[4] The number of patients with implanted medical devices is not miniscule either; millions of people in the United States already have implanted medical devices, and roughly 300,000 new people are getting them each year.[5] The implantable medical device "market is projected to be around [seventeen] [b]illion dollars by 2019," resulting in a large population of patients with this technology in them and little to no cybersecurity attached to those devices, which is a huge security risk.[6] Considering that "[t]he U[nited] S[tates] Department of Homeland Security has identified the . . . Public Health sector as . . . [a] critical cyber security infrastructure[]" to the United States, this lack of cybersecurity is a huge national security risk.[7]

This Article analyzes the vulnerabilities of implantable medical devices, such as pacemakers/defibrillators and insulin pumps, to hacking by malicious actors and the national security risk that those vulnerabilities pose.[8] Part II will explain the lack of cybersecurity of implantable medical devices, such as cardiac defibrillators and insulin pumps, and the vulnerabilities of implantable medical devices to cyberattacks that will harm

2. Benjamin Ransford et al., *Design Challenges for Secure Implantable Medical Devises*, *in* SECURITY AND PRIVACY FOR IMPLANTABLE MEDICAL DEVICES 157, 164 (Wayne Burleson & Sandro Carrara eds., 2014); *see also Homeland Security Investigating Medical Device Cybersecurity*, *supra* note 1.

3. *Homeland Security Investigating Medical Device Cybersecurity*, *supra* note 1. "In 2007 . . . Vice President . . . Cheney had some of the wireless features on his defibrillator disabled due to security concerns" that a terrorist group or an individual person with a vendetta could hack into his defibrillator and use it to kill him. *Id.*

4. *See* Mike Colias, *Cyber Security*, HOSP. & HEALTH NETWORKS, May 2004, at 60, 62, 64; *Homeland Security Investigating Medical Device Cybersecurity*, *supra* note 1.

5. Shyamnath Gollakota et al., *They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices*, ACM SIGCOMM COMPUTER COMM. REV., Aug. 2011, at 2.

6. Apurva Mohan, *Cyber Security for Personal Medical Devices Internet of Things*, *in* 2014 IEEE INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING IN SENSOR SYSTEMS 372, 372 (Lisa O'Conner ed., 2014).

7. Nicholas J. Mankovich, *Securing IT Networks Incorporating Medical Devices: Risk Management and Compliance in Health Care Cyber Security*, *in* ADVANCES IN CYBER SECURITY: TECHNOLOGY, OPERATIONS, AND EXPERIENCES 173, 173 (D. Frank Hsu & Dorothy Marinucci eds., 2013).

8. *See infra* Parts II–IV.

the patient.[9] It will then emphasize how this is a national security risk by providing instances of lack of cybersecurity causing harm in the United States and abroad, which includes the research conducted in hacking implantable medical devices.[10] Part III will analyze the current governmental legislation and regulations on implantable medical devices and how the government fails to address cybersecurity due to conflicting laws within agencies and branches of government.[11] Part IV delves into possible solutions for this national security risk by proposing possible governmental regulations, as well as other private sector-led solutions.[12] It will then conclude by stressing the dangers that poor regulations and laws can cause by failing to address the cybersecurity risks to the medical device industry.[13]

II. UNDERSTANDING HACKING IMPLANTABLE MEDICAL DEVICES

Manufacturers focus, first and foremost, on functionality of implantable medical devices, and almost all manufacturers skip any type of cybersecurity due to a multitude of reasons.[14] As devices are increasingly interconnected with the Internet and wireless functionalities, the lack of cybersecurity poses a huge security risk to patients wearing implantable medical devices from malicious actors.[15] Part A discusses manufacturer concerns about adding cybersecurity to implantable medical devices, and explains how the Food and Drug Administration ("FDA") echoes these fears.[16] It also highlights the lack of focus the healthcare industry has overall in tackling cybersecurity issues.[17] Part B examines the many ways hackers can take over and manipulate implantable medical devices.[18] Part C provides examples of cyberattacks on medical devices across the United States and overseas, and how preventative measures, such as anti-virus software, contribute to the harm.[19] Part C concludes by discussing laboratory simulations and public demonstrations of hacking implantable medical

9. *See infra* Part II.
10. *See infra* Section II.C.
11. *See infra* Part III.
12. *See infra* Part IV.
13. *See infra* Parts IV–V.
14. Ransford et al., *supra* note 2, at 170.
15. Mankovich, *supra* note 7, at 174–75; *Homeland Security Investigating Medical Device Cybersecurity*, *supra* note 1.
16. *See infra* Section II.A.
17. *See infra* Section II.A.
18. *See infra* Section II.B.
19. *See infra* Section II.C.

devices and demonstrating the clear and present threat the lack of cybersecurity has on these devices.[20]

A. *The Lack of Cybersecurity: A Problem with the Industry*

Implantable medical devices are, first and foremost, designed to provide enormous health benefits to patients.[21] These devices, such as insulin pumps and cardiac defibrillators, all feature wireless communication to monitor and treat patients through personalized care and send reports to their physicians.[22] They also are updated remotely with the latest firmware, all for the benefit of the patient.[23] As manufacturers keep improving quality of care and technology by making the devices lighter, smaller, and faster, they tend to ignore cybersecurity for the devices.[24]

Implantable medical devices do not have cybersecurity built into them when they are made.[25] This is due to a myriad of reasons: The "limitations in computing power or memory space" from having such a small device that is "[un]able to run traditional [anti-virus] software without impacting [the device's] performance;"[26] fear of creating "a critical, life-threatening situation if the system responds to a false positive if there is anti-virus software in the medical device;[27] standard security software is difficult to use with the limited memory in a customized/scaled back version of the operating system in the device;[28] authentication security measures on the devices risk patient safety in cases of an emergency when a medical professional may need to disable or alter the device to treat a patient;[29] and

---

20. *See infra* Section II.C.

21. Wayne Burleson & Sandro Carrara, *Introduction* to SECURITY AND PRIVACY FOR IMPLANTABLE MEDICAL DEVICES 1, 1 (Wayne Burleson & Sandro Carrara eds., 2014).

22. Sarbari Gupta, Implantable Medical Devices — Cyber Risks and Mitigation Approaches, Abstract from the Nat'l Inst. of Standards & Tech.: Cybersecurity in Cyber-Physical Systems Workshop (Apr. 23, 2012).

23. *Id.*

24. Burleson & Carrara, *supra* note 21, at 1. This is according to Lessley Stoltenberg, the University of Texas MD Anderson Cancer Center's Chief Information Security Officer. Jim Finkle, *U.S. Government Probes Medical Devices for Possible Cyber Flaws*, REUTERS (Oct. 22, 2014, 7:11 AM), http://www.reuters.com/article/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022.

25. Finkle, *supra* note 24.

26. Axel Wirth, *Cybercrimes Pose Growing Threat to Medical Devices*, 45 BIOMEDICAL INSTRUMENTATION & TECH. 26, 31 (2011).

27. *Id.*

28. *Id.* at 28.

29. *See* Sharon R. Klein & Odia Kagan, *Unhack My Heart: FDA Issues Guidance to Mitigate Cybersecurity Threats in Medical Devices*, PEPPER HAMILTON LLP 2 (June 24, 2013), http://www.pepperlaw.com/uploads/files/clientalert062413b.pdf.

heavy encryption for security of the device may drain enough energy that it would require frequent device replacement, which would require surgery, resulting in burdening both the patient and the medical profession.[30] The FDA has echoed these fears of "medical device security measures doing more harm than good in emergency situations."[31] Implantable medical devices are meant to improve patients' lives, and thus, manufacturers and designers have apportioned this above all else to cybersecurity.[32]

The healthcare industry is estimated to be "'five to seven years behind' other industries in . . . cybersecurity."[33] This is because the healthcare industry is very diverse and fragmented compared to other industries, such as the energy industry.[34] Traditionally, "[t]he medical device industry has . . . ignored warnings that its products [are not] protected against [a] cyberattack."[35] If there is any type of security protection put into devices by manufacturers, it tends to focus on data theft, not device manipulation by malicious actors.[36] Also, compared to other industries that spend 12% of their information technology ("IT") security budget on data protection alone, a majority of healthcare organizations spend less than 3% of their IT security budgets on it.[37] With the percentage of healthcare organizations that have reported being hacked rising from 20% in 2009 to 40% in 2013, the medical industry's dismal security budget focus and funding, compared to industry standards of preventative IT security budget, could be considered negligent.[38] "[Ninety-four percent] of [all] healthcare institutions [have] reported . . . be[ing] victims of cyberattacks."[39]

Lastly, there is not an effective national reporting system for cybersecurity related failures that play a significant role in patient injuries or

30. *See* Burleson & Carrara, *supra* note 21, at 4.

31. Klein & Kagan, *supra* note 29, at 2.

32. Ransford et al., *supra* note 2, at 170.

33. Alex Ruoff, *Security Exec: Medical Device Industry at Least Five Years Behind on Cybersecurity*, 6 BNA HEALTH L. REP. 17, 17 (2014).

34. Daniel J. Barnett et al., *Cyber Security Threats to Public Health*, 5 WORLD MED. & HEALTH POL'Y 37, 38 (2013).

35. Ruoff, *supra* note 33, at 17.

36. *Id.*

37. Alex Ruoff, *Hacking Incidents on the Rise, But IT Security Budgets Remain Low, Execs Say*, 6 BNA HEALTH L. REP. 20, 20 (2014).

38. *See* Caroline Humer & Jim Finkle, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, REUTERS (Sept. 24, 2014, 2:24 PM), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924; Ruoff, *supra* note 37, at 20.

39. Eric D. Perakslis, *Cybersecurity in Health Care*, 371 NEW ENG. J. MED. 395, 395 (2014).

deaths.[40] "[A]pproximately 1.2 million adverse events of medical devices were reported to the FDA's Manufacturer and User Facility Device Experience . . . database" between 2006 and 2011,[41] but there is no information on those cybersecurity related failures, as cybersecurity problems are not included in the reporting system.[42] Out of the 1.2 million, 23% were listed only as computer-related failures, 94% of which "presented medium to high risk" of harm to the patient.[43]

Similarly, the FDA's Manufacturer and User Facility Device Experience "database is qualitative rather than quantitative," and it does not concern itself with security events.[44] For example, if a clinician is using a device that is slower because of a malware infection, it would most likely not be reported.[45] This is because admitting a role in infecting a medical device or a network, such as inserting an infected flash drive in a computer or connecting an infected phone to the network, would lead to disciplinary action.[46] Therefore, the actual number of what is reported is most likely low because of employees not realizing an issue or fearing retribution.[47]

B. *The Digital Vulnerabilities of Implantable Medical Devices*

Current implantable medical devices can be hacked into and taken over, overloaded with malware to slow them down, turned off completely, and overloaded to kill the host at the behest of a malicious actor or actors, and all harming the host of the device.[48] For instance, a Medtronic pacemaker does not need a password to access the device and the wireless communication is not encrypted, which makes it easy for a hacker to collect data from the device, reverse engineer the protocol, and take over the device.[49] Public information, such as any implantable medical device user's manual and the specifications for the device's radio chip, make the reverse engineering and finding of the remote control personal identification number

40. Kevin Fu & James Blum, *Controlling for Cybersecurity Risks of Medical Device Software*, COMM. ACM, Oct. 2013, at 35, 35–36.
41. *Id.* at 35.
42. *Id.* at 35–36.
43. *Id.* at 35.
44. *Id.* at 36.
45. Fu & Blum, *supra* note 40, at 36.
46. *Id.*
47. *See id.*
48. *See* Steven J. Templeton, *Security Aspects of Cyber-Physical Device Safety in Assistive Environments*, *in* PETRA 2011, THE 4TH ACM INTERNATIONAL CONFERENCE ON PERVASIVE TECHNOLOGIES RELATED TO ASSISTIVE ENVIRONMENTS, CRETE, GREECE, MAY 25–27, 2011 §1, 2.1.1 (Ass'n for Computing Mach. 2011).
49. *Id.*

to control the device relatively simple.[50] Once this is done with readily available information, the hacker can generate misleading information, such as false readings on an insulin pump or just cause it to inject "insulin into the patient's body."[51] Implantable medical devices are exposed to common cyber threats that normal computers experience because the operating system, central processing unit, and other software components are generally *off-the-shelf* components.[52] Medical devices still tend to rely on the original versions of their operating system—such as Windows XP—even long after support for the operating system has ended.[53] Hackers can also take control of the device as long as it is around any sort of wireless Internet, and the strength of the transmission and radio frequency of the implantable medical device does not matter.[54] This is possible because Federal Communications Commission regulations make it so that implanted medical devices have a certain radio frequency range, as implantable medical devices "[do] not normally initiate communication [and only] transmit [as a] response to a transmission from [another party] or if [they] detect[] a life-threatening condition."[55] No matter what the implantable medical device is, once it is connected to a network, it is essentially a node on the network that can be seen, interacted with, and controlled.[56] As these devices are increasingly using wireless communications among components to improve health and reporting, hackers have a larger avenue for control of a system.[57]

Unfortunately, the implanted medical devices already in patients cannot just have cybersecurity protocols and software patched into them to resolve this gaping security hole.[58] The medical device industry in the United States is tightly regulated by the FDA, which requires that the

50. Ransford et al., *supra* note 2, at 176.

51. *Id.*

52. Wirth, *supra* note 26, at 27.

53. Fu & Blum, *supra* note 40, at 36. In 2012, it was reported to the National Institute of Standards and Technology ("NIST") Information Security and Privacy Advisory Board that the Beth Israel Deaconess Medical Center in Boston was still using medical devices that were using the original versions of Windows 95 and Windows XP, despite the support for these ending in 2006 and 2010 respectively. *Id.* These devices were not even the final patch of these versions, and were never upgraded to include any of the patches that came out to these operating systems over the years. *Id.* This shows that, even if patching does occur to devices, hospitals and medical professionals need to apply them in order to be effective. *See id.*

54. *See* Gollakota et al., *supra* note 5, at 3–4.

55. *Id.*

56. Robert J. Caruso & Melissa Masters, *Applying Cyber Risk Management to Medical Device Design*, BIOMEDICAL INSTRUMENTATION & TECH., Spring 2014, at 32, 33.

57. Ransford et al., *supra* note 2, at 176.

58. Martha Vockley, *Safe and Secure? Healthcare in the Cyberworld*, 46 BIOMEDICAL INSTRUMENTATION & TECH. 164, 167 (2012).

cybersecurity for any medical device and its upgrades be applied by the manufacturer and not any person in the stream of commerce for the device.[59] Therefore, a hospital cannot upgrade or add any type of cybersecurity to any medical device without the manufacturer approving the upgrade.[60] In compliance with the FDA review process, a manufacturer needs to test the proposed patch on the device, making sure the changes to the operating system do not impact the behavior and functionality of the device.[61] That means that medical devices from a patch level are often "months, if not years, behind where the operating system manufacturer is," leading to a security gap that cannot be remedied swiftly.[62] When patches are approved and finally applied, "they may require complex installation procedures and acceptance testing" which may result in the patch not actually being applied.[63] Unlike in computers and other software, full automatic distribution and application of upgrades are difficult to implement in implantable medical devices because of the associated upgrade timing and the system reboot endangering the patient; if there were an issue, the patient would be vulnerable.[64] Implantable medical devices can last up to ten years, leaving the patients vulnerable to attack for a long time.[65]

The issue of patching and updating medical devices is not new, as it has been widely recognized by the FDA as being an issue.[66] The Department of Homeland Security has also recognized this issue; for example, it reported that the Conficker virus has not only been known to have infected pacemakers through wireless and other connections but, also, cannot be removed because removal of the virus would be considered a "modification to the certified software" under governmental regulations.[67]

Implantable medical devices can also be infected with viruses or targeted malware from networked devices.[68] Any type of medical equipment that is infected with a virus or malware and is connected to a network will spread it to the implanted medical device.[69] This can either give a hacker control—if that is the target—or the ability to disable or slow down the device.[70] Many hospitals tend to get medical technology—devices and

59. Wirth, *supra* note 26, at 27.
60. *Id.*
61. Vockley, *supra* note 58, at 167.
62. *Id.*
63. Wirth, *supra* note 26, at 28.
64. *See id.* at 32.
65. Gollakota et al., *supra* note 5, at 2.
66. Wirth, *supra* note 26, at 28.
67. Templeton, *supra* note 48, at § 2.2.
68. Vockley, *supra* note 58, at 167.
69. *Id.*
70. *See* Ransford et al., *supra* note 2, at 161; Vockley, *supra* note 58, at 167.

equipment—from a single vendor, and vendors tend to keep all of their "equipment on the same patch or configuration level," which makes the spread of the virus or malware very easy.[71] Even if a hospital purchased medical technology and devices from multiple vendors, having different devices from different manufacturers, each with its own structure and potential levels of security, would create an insecure tangled digital web of cybersecurity.[72] Targeted malware can move between different devices and systems passively until it reaches the implantable medical device where it is designed to activate.[73] Due to the fact that implantable "medical devices such as pacemakers [each] have [a] unique identifier[]," it is possible to target a specific individual or class of people.[74] This *Internet of things* that connects physical equipment all together on a network via computers has created many different avenues for cyberattacks.[75]

C. *National Security Risk*

Concerns about the varying lapses in cybersecurity in implantable medical devices and medical devices on the same network have merit.[76] "Between . . . 2009 and . . . 2011, the [Department of Veterans' Affairs] detected 142 . . . instances of malware infections affecting 207 medical devices found in [fourteen different parts of hospitals]."[77] In one instance, in the catheterization lab, the malware infection of equipment was so severe that it "required transport of [the] patients to a different hospital."[78] In 2010, a Veterans' Affairs catheterization laboratory in New Jersey was closed due to malware that infected hundreds of medical devices and computers on that network.[79] "[T]he Conficker worm [caused] . . . approximately 10[%] of the [healthcare] IT infrastructure in Sweden" to go dark in 2010.[80] That same year, the same worm took "15[%] of New Zealand's [total healthcare] system . . . offline."[81] These kinds of viruses that can take over computers

71. Vockley, *supra* note 58, at 167.
72. *Id.*
73. Templeton, *supra* note 48, at § 2.2.
74. *Id.*
75. Perakslis, *supra* note 39, at 396.
76. *See* Mankovich, *supra* note 7, at 174; Fu & Blum, *supra* note 40, at 36; Daniel B. Kramer et al., *Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance*, PLOS ONE, July 19, 2012, at 1, 4.
77. Kramer et al., *supra* note 76, at 4.
78. *Id.*
79. *See* Fu & Blum, *supra* note 40, at 36.
80. Mankovich, *supra* note 7, at 174.
81. *Id.*

and devices are not bound by country borders and infect anything that links into the network.[82]

In addition, there is a real danger of implementing already existing safety measures, such as anti-virus software, in implantable medical devices.[83] "On April 21, 2010, one-third of the hospitals in Rhode Island were forced to" stop elective surgeries and treatment of non-trauma patients in the emergency room because the "anti-virus software update had . . . misclassified a critical Windows [dynamic link library] as malicious."[84] Another example occurred when a "tornado hit St. John's hospital in Kansas City in May 2011."[85] The tornado "caus[ed] the electricity to go out, [and as a result] doctors and nurses lost access to . . . vital medicine[] in the [emergency room] and in [almost] every other department," because the drugs were in a powered metal cabinet which had an automatic lock controlled by software.[86]

"Researchers at [the] Massachusetts Institute of Technology and the University of Massachusetts, Amherst, . . . have demonstrated [in a laboratory] that it is possible to hack into wireless implantable medical devices," including pacemakers, heart defibrillators, insulin pumps, and even cochlear implants and neurostimulators, and take control of them to the detriment of patients.[87] Even a programmable radio could control an implantable defibrillator or an insulin pump by replaying messages, allowing the operator of the radio to stop the device or to cause it to kill the host.[88] Researcher Jerome Radcliffe inspected the Java-based configuration program in his own insulin pump and was able to "reverse-engineer[] the pump's packet structure, revealing that [it did not] encrypt the medical data . . . or . . . authenticate [when] the components [of the insulin pump communicated] to one another."[89] A researcher with Radcliffe also demonstrated his ability to take over and shut down a volunteer's insulin pump, showing how easy and swiftly it could be done.[90] To further the point, a group of researchers demonstrated how "analog signal injection of low-frequency waveforms . . . on the sensing leads of" an implantable defibrillator could be tricked by crafting electromagnetic interference waveforms to deliver a defibrillation shock.[91] This means that even an attacker who cannot perfectly match an

82. *See id.* at 174–75.
83. *See* Fu & Blum, *supra* note 40, at 36.
84. *Id.*
85. Klein & Kagan, *supra* note 29, at 2.
86. *Id.*
87. Vockley, *supra* note 58, at 170.
88. Ransford et al., *supra* note 2, at 161.
89. *Id.*
90. *Id.* at 164.
91. *Id.* at 166.

electromagnetic interference signal's wavelength to the length of the sensing leads could just increase the power to override and trigger the implantable medical device.[92] Researchers have not only been able to do something once thought of as science fiction in a laboratory, but they have also been able to do it in the course of a live demonstration.[93]

III. CURRENT STATE OF GOVERNMENTAL AFFAIRS

The FDA's mission is to protect "the public health by assuring the safety, efficacy, and *security* of medical devices."[94] The FDA regulates medical devices and approves them, but its authority is in flux regarding regulation of cybersecurity.[95] Part A of this Section delves into the FDA and its numerous attempts to tackle cybersecurity of implantable medical devices through voluntary guidance, regulations, and proposed regulations.[96] Part B examines various congressional attempts to tackle cybersecurity of implantable medical devices, along with other governmental bodies such as the Federal Trade Commission ("FTC"), the Department of Homeland Security, the Department of Defense, and the White House.[97] This Section highlights the contradictory nature of all of the various governmental bodies' solutions to the important issue of cybersecurity in implantable medical devices.[98]

A. *The Power of the FDA*

The FDA classifies a device as an "instrument, . . . machine, . . . implant, . . . or other similar . . . article, including any component, part, or accessory, which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals."[99] The FDA subjects all of these to the same laws and standards, with a definition that is vague enough that even a smartphone becomes a medical device when employing a cell phone camera to determine urine analytes.[100] "The FDA considers [most] [h]ealth IT products to be 'similar or related to' other medical device products," which results in the

92. *See id.*
93. Ransford et al., *supra* note 2, at 164.
94. Fu & Blum, *supra* note 40, at 36.
95. *See* Vockley, *supra* note 58, at 166–67.
96. *See infra* Section III.A.
97. *See infra* Section III.B.
98. *See infra* Section III.B.
99. 21 U.S.C. § 321(h)(2) (2012).
100. *See* U.S. FOOD & DRUG ADMIN., LETTER TO BIOSENSE TECHNOLOGIES PRIVATE LIMITED CONCERNING THE UCHECK URINE ANALYZER (2013).

FDA classifications referring back to themselves in defining medical devices and standards.[101]

The FDA has released numerous guidance documents on cybersecurity throughout the years, all echoing each other with no actual effect on implantable medical devices.[102] "In 2005, the [FDA] issued [a] 'Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software,'" which stated that it was "the responsibility of medical device manufacturers to maintain cybersecurity" and to keep them safe and effective through maintenance plans for its cybersecurity.[103] "On September 25, 2013, the FDA [released the] Mobile Medical Applications Guidance . . . ("MMA Guidance")," which declared that it "intend[ed] to regulate software that poses significant risks to patients . . . ."[104] The MMA Guidance also explained that devices classified as "[mobile medical applications] must have premarket approval or clearance [from the FDA] before commercialization may begin."[105] The MMA Guidance also defined "[a] manufacturer as [being] anyone who 'creates, designs, develops, labels, re-labels, . . . modifies, or creates a software system or application for a regulated medical device in whole or from multiple software components.'"[106] This software classification sweeps in all types of medical devices, including smartphones, although Congress has stated that the FDA does not have authority to do so.[107]

To further complicate things, in February 2011, the FDA reclassified its Medical Device Data Systems ("MDDS") rule from a Class III, highest risk, to a Class I, lowest risk classification.[108] This MDDS rule defines MDDS as devices intended to transfer, store, and convert from one format to another or display medical device data.[109] Implantable medical devices fall

101. Areta L. Kupchyk, *What's Trending with Mobile Medical Apps and Health IT? A New FDA Regulatory Framework May Be in the Making*, 6 HEALTH IT L. & INDUSTRY REP. 1, 2 (2014); *see also* 21 U.S.C. § 321(h).

102. *See* Mankovich, *supra* note 7, at 175; Kupchyk, *supra* note 101, at 2–3.

103. Mankovich, *supra* note 7, at 175; *see also* U.S. FOOD & DRUG ADMIN., CYBERSECURITY FOR NETWORKED MEDICAL DEVICES CONTAINING OFF-THE-SHELF (OTS) SOFTWARE: GUIDANCE FOR INDUSTRY (2005).

104. Kupchyk, *supra* note 101, at 2–3; *see also* U.S. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2015).

105. Kupchyk, *supra* note 101, at 2; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 104.

106. Kupchyk, *supra* note 101, at 3; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 104.

107. *See* Kupchyk, *supra* note 101, at 5.

108. *See* 21 C.F.R. § 880.6310(b) (2016); U.S. FOOD & DRUG ADMIN., *supra* note 104.

109. 21 C.F.R. § 880.6310(a)(1)(i)–(iv).

within this classification.[110] Under the new MDDS rule classification, the FDA does not consider "software that is critical to keeping a patient alive, such as blood pressure cuffs and glucose monitors, to be [a] MDDS product[]."[111] The FDA determined that the new classification to lowest risk is because these products pose the lowest risk to the patient, and the controls of the devices "would provide . . . reasonable assurance of safety and effectiveness."[112] Under this new classification, which incorporates implantable medical devices, "[m]anufacturers are only required to comply with the registration and listing requirements, the Medical Device Reporting regulation . . . and the Quality System Regulation" of the FDA.[113]

The FDA has numerous proposals in the works as well.[114] First, the "FDA has proposed to expand the types of . . . device[s] . . . [under the MDDS Rule] that would be exempt from FDA enforcement."[115] The FDA also plans "to revise its [MMA Guidance] to conform [to] the MDDS expansion and clarify the types of mobile medical [applications] that would be exempt from FDA enforcement as a medical device."[116] "The FDA [also] has proposed not to enforce compliance with any regulatory controls that apply to the MDDS;" "medical image storage device[s], [which provide] electronic storage and retrieval functions for medical images;" and "medical image communication device[s], [which are] device[s] that provide electronic transfer of medical image data between medical devices," "based on a determination that these devices pose low risk to patient safety."[117] The language of the proposal, however, is vague enough to incorporate implantable medical devices such as insulin pumps.[118] Lastly, the FDA published the Health Information Technology ("HIT") Report at the request of Congress in April 2014, in accordance with the Food and Drug Administration Safety and Innovation Act ("FDASIA"), which proposed another strategy based on classifying healthcare intellectual technology products.[119] The recommended categories were administrative products, health management products, and medical devices.[120] This report led to

110. *See id.*; Gupta, *supra* note 22.
111. Kupchyk, *supra* note 101, at 3.
112. *Id.*
113. *Id.*
114. *See id.*
115. *Id.*
116. Kupchyk, *supra* note 101, at 3; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 104.
117. Kupchyk, *supra* note 101, at 4; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 104.
118. *See* U.S. FOOD & DRUG ADMIN., *supra* note 104.
119. Kupchyk, *supra* note 101, at 2, 4.
120. *Id.* at 4.

proposed legislation based on a function-based framework when evaluating applications and products, and it does not address medical software or have any binding authority.[121]

The FDA came out with a new series of nonbinding recommendations in October 2014, after an investigation by the Department of Homeland Security into the cybersecurity of implantable medical devices was made public.[122] This new guidance began by recognizing "[t]he need for effective cybersecurity to assure medical device functionality and safety [in light of] increasing use of wireless, Internet, and network connect[ive] devices."[123] The FDA recognized the threat stemming from failure to maintain cybersecurity in these devices, including the possibility that compromising medical devices could cause harm and death to patients.[124] The FDA's nonbinding recommendations [were] modeled on the [National Institute of Standards and Technology ("NIST")] Cybersecurity Framework," recommended by the White House, and it "encourages manufacturers to develop controls to ensure the security of medical devices" in the *Internet of things*.[125] It also "encourages manufacturers to treat [cybersecurity] as a fundamental part of the development[] process" and "acknowledge[s] that device makers face [the] challenge[] [of] striking the balance between . . . cybersecurity" and making sure the device itself would remain usable.[126] "The FDA also recommends that manufacturers includ[e] certain documentation as part of the premarket submission process to ensure implementation of appropriate cybersecurity controls."[127] That "documentation includes a hazard analysis, a summary of [the] controls, and a *traceability matrix* that 'links actual cybersecurity . . . to the . . . risks that were considered.'"[128] The FDA guidance documents for software, however,

121. *Id.* at 2, 4.

122. U.S. FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2014); *see also Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, KING & SPALDING 2 (Oct. 27, 2014), http://www.kslaw.com/imageserver/KSPublic/library/publication/ca102714a.pdf.

123. U.S. FOOD & DRUG ADMIN., *supra* note 122.

124. *Id.*

125. *Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, *supra* note 122, at 2; U.S. FOOD & DRUG ADMIN., *supra* note 122. The *Internet of things* is a term that describes all devices with the capability of connecting to the Internet, other devices, or other networks. *See Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, *supra* note 122, at 2; Perakslis, *supra* note 39, at 396.

126. *Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, *supra* note 122, at 2; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 122.

127. *Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, *supra* note 122, at 2.

128. *Id.*

generally always focus on "large-scale computer-based equipment [and] not computerized devices," with focus on data security and not safety.[129] All of these are purely recommendations with no binding authority.[130]

On December 28, 2016, the FDA published its final guidance for the Postmarket Management of Cybersecurity in Medical Devices.[131] The guidance states repeatedly that it in no way "establishes any rights . . . and it is not binding on [the] FDA or the public."[132] The FDA emphasizes "that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of [the] medical devices."[133] In an effort to streamline this process, the FDA states that it does not intend to enforce its own reporting requirements for device patches.[134] The FDA's rationale is that "cybersecurity . . . updates and patches are generally considered to be a type of device enhancement for which the FDA does not require advance notification or reporting."[135] However, should a cybersecurity vulnerability or exploit "pose a risk to health," the medical device manufacturer would be required to report this to the FDA.[136] Beyond finding a *risk to health*, the FDA also recommends that manufacturers use a cybersecurity vulnerability assessment tool in determining the probability of the occurrence of harm for a device, as well as for assessing the severity of harm to the patient.[137] The rest of the December 2016 guidance echoes the other FDA rules and regulations, particularly the October guidance in terms of cybersecurity practice.[138] The changes to the patching of medical devices in this guidance are non-binding and unclear as

129. Templeton, *supra* note 48, at § 1; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 122.

130. *Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, *supra* note 122, at 2; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 122.

131. U.S. FOOD & DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2016).

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.* (quoting U.S. FOOD & DRUG ADMIN., *supra* note 122).

136. U.S. FOOD & DRUG ADMIN., *supra* note 131. While a medical device manufacturer would be required to report a cybersecurity vulnerability or exploit that "pose[s] a risk to health," it is unknown under the Guidance when the notification would occur, or if the device manufacturer would be punished for patching the exploit before notification and approval by the FDA. *Id.*

137. *Id.*

138. *See id.*; U.S. FOOD & DRUG ADMIN., *supra* note 122.

to when reporting to the FDA would be necessary for *health risk* cybersecurity vulnerabilities in medical devices.[139]

The recent FDA regulations do not put forth any new ideas.[140] The FDA created "a cross-agency working group [as long ago as 2013] involving . . . the Office of the National Coordinator for Health Information Technology and the Federal Communications Commission," which called for recommendations and a risk-based regulatory framework but did not define what that meant.[141] In addition, the FDA also has recommended in the past that manufacturers provide "[a] specific list of all cybersecurity risks that were considered in the design of [the] device," controls for the device, and a plan for providing updates along the device lifecycle.[142] The working group also recommended that manufacturers send "[a]ppropriate documentation to demonstrate that the device will . . . [arrive] free of malware," include in the device instructions what kind of anti-virus software or firewall is on the device, if any, and that the manufacturers anticipate and include in the instructions whether a particular type of user will put their own anti-virus software on the device.[143] This is contrary to the FDA 510(k) certification process, which requires manufacturers to be the sole party to upgrade the device and to send the patch to the FDA for approval before it goes into effect.[144] There are so many FDA regulations and recommendations that are vague and contradictory to one another that something must be done to clarify this bureaucratic mess and establish a standard for cybersecurity of implantable medical devices.[145]

B. *Governmental Reclassifications, Power Shifts, and Executive Orders*

The Health Insurance Portability and Accountability Act ("HIPAA") pervasively regulates electronic health information through its privacy and security rules, but HIPAA focuses on data security rather than device

139. *See* U.S. FOOD & DRUG ADMIN., *supra* note 131; U.S. FOOD & DRUG ADMIN., *supra* note 122.

140. *See* U.S. FOOD & DRUG ADMIN., *supra* note 131; Fu & Blum, *supra* note 40, at 36; Perakslis, *supra* note 39, at 396.

141. Perakslis, *supra* note 39, at 396.

142. Fu & Blum, *supra* note 40, at 37.

143. *Id.*

144. *See* Ransford et al., *supra* note 2, at 162.

145. *See* U.S. FOOD & DRUG ADMIN., *supra* note 131; Wirth, *supra* note 26, at 27–28. While the agency itself has a process of reviewing and approving upgrades, the FDA itself recommends that manufacturers anticipate users putting on cybersecurity, which is contradictory to establishing any sort of standard for the device and help against the FDA's own regulations. *See* U.S. FOOD & DRUG ADMIN., *supra* note 131; Wirth, *supra* note 26, at 27–28. The agency has been so malleable on this issue that it contradicts itself. *See* U.S. FOOD & DRUG ADMIN., *supra* note 131; Wirth, *supra* note 26, at 27–28.

security.[146] Congress defined security under HIPAA as "physically protecting health information stored or transmitted electronically," thus, failing to include cybersecurity of medical devices against hackers who want to control the device.[147] Congress passed the FDASIA, which delves into levels of medical device classification for federal protection and addresses which type of FDA scrutiny they each undergo.[148] The FDASIA requires the FDA to propose a strategy and recommends it on "an appropriate risk based regulatory framework focused on functionality for Health IT."[149] In April 2014, the FDA published the HIT Report, which suggested a function-based framework companies could refer to, but it did not address the "multifunctional nature of medical software."[150] Overall, the FDASIA and the HIT Report attempted to reclassify certain aspects of medical technology and devices, but that was not a strong attempt at a solution, at least in part because Congress designated the HIT Report, which it petitioned the FDA to issue as having no authority.[151]

"As the FDA was completing the HIT Report [at the request of Congress], a bipartisan congressional coalition introduced the Sensible Oversight for Technology, which Advances Regulatory Efficiency Act of 2013 ("SOFTWARE Act") . . . ."[152] Just like the FDASIA, the SOFTWARE Act is another reclassification of medical device products under three different categories at the FDA.[153] However, the FDA would only have jurisdiction to regulate under one of the categories.[154] Clinical and health software, including software that analyzes and changes patient data, would be exempt from regulation.[155]

The United States Consumer Product Safety Administration has oversight of software vulnerabilities where the FDA does not, despite the FDA having the oversight of the medical devices that host the software.[156] However, the United States Consumer Product Safety Administration does not cover computer security on vulnerability assessments of software.[157]

146. R.L. Garrie & P.E. Paustian, *mHealth Regulation, Legislation, and Cybersecurity*, *in* MHEALTH: TRANSFORMING HEALTHCARE 45, 46 (2014).
147. *Id.*
148. Kupchyk, *supra* note 101, at 2.
149. *Id.*
150. *Id.*
151. *See id.* at 2, 4.
152. *Id.* at 2.
153. Kupchyk, *supra* note 101, at 2, 4.
154. *Id.*
155. *Id.*
156. Templeton, *supra* note 48, at § 3.3.
157. *Id.*

This is just proposed legislation and another contradictory attempt at reclassification from Congress.[158]

The Preventing Regulatory Overreach to Enhance Care Technology Act of 2014 ("PROTECT Act") is another proposed law, again attempting to reclassify medical devices within the FDA.[159] The PROTECT Act was a congressional response to the FDA's failure to respond to questions from the Health IT industry.[160] The congressional purpose of the PROTECT Act is to prevent FDA overregulation while protecting innovation and exempting low-risk health software from a new tax under the Affordable Care Act.[161] This is another attempt by Congress to reclassify medical devices, further muddying efforts to identify medical devices and implement protection at a federally consistent level.[162]

The FTC is also influencing the medical device field, as the devices use wireless frequencies available in the open air.[163] The data transmitted from these devices could be used and stolen as a result from cyberattacks, and this crosses over into the FTC's administrative realm.[164] The FTC issued an order in *GMR Transcription Services, Inc.*, stating that the cybersecurity issue of medical records on devices that they have are poorly defined.[165] The FTC then ordered GMR Transcription Services to have its security looked at and inspected for a set number of years, in order to make sure they were doing something with cybersecurity.[166] This demonstrates another agency recognizing the issue of poor cybersecurity and issuing compliance check-ins to make sure that some level of cybersecurity is achieved.[167]

In an executive order, President Obama issued the NIST Framework in 2013, which was designed to improve cybersecurity practices across all critical United States sectors vulnerable to cyberattack.[168] The executive order required the "NIST, a division of the Department of Commerce, to develop a [set] . . . of voluntary cybersecurity best practices for [United States] *critical infrastructure* sectors."[169] That framework would provide an entity with an understanding of where each critical United States sector is in

158. *See id.*; Kupchyk, *supra* note 101, at 2, 4.
159. *See* Kupchyk, *supra* note 101, at 2.
160. *Id.* at 5.
161. *Id.*
162. *See id.*
163. *See* Alex Ruoff, *supra* note 37, at 20.
164. *See id.*
165. *See id.*
166. *Id.* at 3–5.
167. *See id.* at 4.
168. Alex Ruoff, *Federal Security Officials Say Cyberattacks on Health Companies Expected to Increase*, 23 BNA HEALTH L. REP. 1282, 1282 (2014).
169. *Id.*

terms of vulnerability and attempt to analyze each level of security.[170] The NIST Framework analyzes the usefulness of controls to a particular device in three separate areas of cybersecurity—confidentiality, integrity, and availability—and sets control levels per device for risk assessment.[171] If an area is classified as high risk, the framework determines what controls need to be implemented to try to mitigate that risk.[172] This is another voluntary measure that brings in another agency, along with another reclassification, separated from the many that Congress and the FDA have, which makes having any cohesive protection of implantable medical devices' cybersecurity that much more complicated.[173]

Adding another layer of complexity, during the George W. Bush administration, the Department of Homeland Security was involved in trying to tackle the issue of cybersecurity of implantable medical devices.[174] The Bush Administration formed a private-sector group in partnership with the Department of Homeland Security and the Department of Health and Human Services, to convince the healthcare industry to conform to the Bush Administration's "National Strategy to Secure Cyberspace."[175] This group ended up finding that nobody knows the condition of the healthcare sector's collective security infrastructure, since the industry is fragmented, and each institution gauges its cybersecurity and its vulnerabilities differently.[176] The group recommended raising the bar for manufacturers, "possibly by establishing [a] minimum-security standard[] for certain products and . . . [even] creating a certification process for [cybersecurity]."[177] Finally, the group recommended devising a standardizing tool to help assess vulnerabilities for manufacturers, something that is still repeatedly mentioned over a decade later.[178]

In October 2014, the Department of Homeland Security revealed an investigation of cybersecurity vulnerabilities in medical devices and hospital equipment that may be exploitable by cyber criminals and are susceptible to malicious hacking.[179] The vulnerabilities investigated could cause severe injury and death; they were found in implantable medical devices including

170. *See id.*
171. Caruso & Masters, *supra* note 56, at 32.
172. *See id.*
173. *See id.*; Ruoff, *supra* note 168, at 1282.
174. *See* Colias, *supra* note 4, at 62.
175. *Id.*
176. *Id.*
177. *Id.* at 64.
178. *See id.*
179. *Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, *supra* note 122, at 1.

infusion pumps and implantable heart devices.[180] The Department, however, stated that the probe started when a deceased cybersecurity expert, Barnaby Jack, demonstrated in 2012 that he could hack wireless communications and remotely cause an implanted pacemaker to deliver a lethal shock to the host.[181] In response, the Department of Homeland Security said it had been "working with . . . manufacturers to identify and repair" the issues in the software of the implantable medical devices "that would allow . . . [hackers] to take control of them."[182]

In contrast to all these ambiguous regulations, proposals, executive orders, legislation, and proposed legislation, the Department of Defense has a very strict policy for all devices that the military uses.[183] The "Department of Defense Information Assurance Certification and Accreditation Process program mandates strict certification requirements for [all] . . . computer systems" provided for the military, including hospital equipment and medical devices of all kinds.[184] In order for these devices to be sold to the Department of Defense, they must meet a strict security certification.[185] This has caused problems, as most manufacturers are not willing or even capable of bearing the financial cost necessary of meeting the standards due to the size of the market.[186]

IV. PROPOSED SOLUTIONS

In all, at least five agencies have indicated intent to regulate cybersecurity in medical devices, but nothing is clear and concrete, and what exists is overlapping, confusing, and contradictory.[187] The private sector recognizes the need for an enforceable system pursuant to which medical devices can be tested on a baseline of cybersecurity standards through the FDA.[188] The nature of the medical industry, comprised of both private and public entities, requires a willingness to unify to address cybersecurity at a

180. *Id.*

181. *Id.* at 1–2.

182. Jai Vijayan, *DHS Investigates Dozens of Medical Device Cybersecurity Flaws*, INFORMATIONWEEK (Oct. 23, 2014, 9:06 AM), http://www.informationweek.com/healthcare/security-and-privacy/dhs-investigates-dozens-of-medical-device-cybersecurity-flaws-/d/d-id/1316882.

183. Templeton, *supra* note 48, at § 4.3.

184. *Id.*

185. *Id.*

186. *Id.*

187. *See* Mathias Klümper & Erik Vollebregt, *Navigating the New EU Rules for Medical Device Software*, 2009 REG. AFF. J. DEVICES, 83, 83; Ruoff, *supra* note 168; Ruoff, *supra* note 37.

188. *Homeland Security Investigating Medical Device Cybersecurity*, *supra* note 1; Ruoff, *supra* note 33.

consistent level nationwide.[189] This can be achieved by combining the strengths of the federal government—homeland security and public safety—with the innovative ability of the private sector to tackle cybersecurity for implantable medical devices.[190] This is important, for knowledge of the technological domain specific to implantable medical devices needs to be coupled with the regulation if it is to be strong and not a hindrance to the medical devices' purpose.[191] Just as the federal government and its agencies have developed ways to detect, track, identify risks, and prevent and combat epidemics with the help of the private sector, so too can the government, to an extent, do the same thing to mitigate the harm that can result from the vulnerabilities in implantable medical devices.[192] Standards are useful in creating secure products, as they can help a manufacturer ensure that all known issues have been considered, and this is especially important in very complex devices such as implantable medical devices.[193] Part A discusses possible federal solutions to clearing up the bureaucratic confusion among all of the various governmental bodies.[194] Part B explores various private sector solutions, including traditional and nontraditional solutions to tackling cybersecurity in implantable medical devices.[195] This also includes some potential private regulation.[196] Some persuasive examples emanate from the European Union ("EU") and an international standards body, both of which have attempted to secure implantable medical devices.[197] Lastly, Part C warns of the dangers of poorly drafted regulations in this area, highlighting how bad regulation can both compromise the user of an implantable medical device and harm the medical device industry.[198]

A. *Governmental Solutions*

Governmental solutions in the United States could vary greatly. One absolutely necessary step is for the agencies to collaborate on a set of universal definitions.[199] There are classifications that Congress, the FDA,

189. Barnett et al., *supra* note 34, at 43.
190. *Id.*
191. *See* Perakslis, *supra* note 39, at 396.
192. *Id.* at 397.
193. Templeton, *supra* note 48, at § 2.1.5.
194. *See Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, *supra* note 122, at 1; *infra* Section IV.A.
195. Vijayan, *supra* note 182; *see also* Kramer et al., *supra* note 76, at 4; *infra* Section IV.B.
196. *See* Vijayan, *supra* note 182.
197. Klümper & Vollebregt, *supra* note 187, at 83–84.
198. *See* Kramer et al., *supra* note 76, at 4; *infra* Section IV.C.
199. *See* U.S. FOOD & DRUG ADMIN., *supra* note 122.

the White House, and the other agencies must clarify, with the first step being the use of universal definitions.[200] "[M]edical applications can be of two types: [W]earable and implanted. Wearable devices are those that can be used on [the] body surface of a human or [in] close proximity [to] the user," such as, a heart rate monitor, blood pressure monitor, and glucose sensor.[201] Implantable medical devices, on the other hand, "are those [devices] that are inserted inside [the] human body," such as, an implantable defibrillator and insulin pump.[202] Having clear, non-ambiguous definitions used by all agencies, whether the list appears in legislation or regulations, would help alleviate some of the confusion.

Another solution would be to expand HIPAA to give the Department of Health and Human Services power over cybersecurity issues in this realm and teeth to enforce the new regulations.[203] The Department of Health and Human Services Office for Civil Rights estimates that 66% of providers have not complied with the HIPAA-mandated audit of security controls for their electronic health records.[204] Organizations generally "wait until an attack or breach has occurred to perform an audit," and apparently are willing to take the risk of incurring civil monetary penalties imposed for noncompliance with HIPAA.[205] Even if organizations complied with HIPAA, most of the HIPAA protection relies on standard methods of isolating critical data, which is bypassed by attackers when taking over or overloading an implantable medical device.[206] A possible solution would be to give HIPAA coverage of cybersecurity of devices and put power into the enforcement of its provisions for cybersecurity.

The FDA has already recommended a set of regulatory improvements.[207] The October FDA Guidance included recommendations that would help to address the cybersecurity issues if they were implemented as requirements in a regulation on implantable medical devices.[208] Starting with the premarket submission process to the FDA, demonstrating the existence of a hazard analysis, a summary of controls, and a traceability matrix that links actual controls to the cybersecurity risks foreseen by the manufacturer would ensure that devices incorporate some sort of

200. *See id.*

201. Moshaddique Al Ameen et al., *Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications*, 36 J. MED. SYSTEMS 93, 93 (2012).

202. *Id.*

203. *See* Ruoff, *supra* note 37, at 20.

204. Ruoff, *supra* note 168, at 1282.

205. *Id.*

206. Perakslis, *supra* note 39, at 395–96.

207. U.S. FOOD & DRUG ADMIN., *supra* note 122.

208. *Id.*; *see also Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices*, *supra* note 122, at 2.

cybersecurity precautions.[209] "Manufacturers should address cybersecurity during the design and development of the medical device," with a vulnerability and management approach for the life of the device.[210] Due to the longevity of implantable medical devices, it is important that a cybersecurity plan—from the beginning—is in place, instead of being reactionary and doing ad hoc fixes once problems occur.[211] This can be coupled with the "software validation and risk analysis" that is already required for certification of an implantable medical device by the FDA.[212]

The cybersecurity and vulnerability approach should assess threats and vulnerabilities, mitigation strategies, risk, and accepted risk.[213] It should also balance the safeguards that the manufacturer decides to put in place, to make them appropriate to the user and location of use, so that security controls will not hinder access in an emergency situation.[214] There should also be features in implantable medical devices that recognize and detect breaches, log them, and act on them during normal use, as well as have a failsafe mode for when the device is compromised, so that the critical functionality is still protected.[215] The current language is only persuasive and suggestively vague to consider all devices; yet, having it as a pre-market approval requirement would force manufacturers and the FDA to take cybersecurity into account as part of the FDA approval process.[216]

B. *Other Solutions*

The private sector also has recommendations on ways to implement a national cybersecurity standard.[217] One is to certify third-party testers to test security vulnerabilities in devices.[218] Another is a national information sharing system for medical device cybersecurity to detect the latest security vulnerabilities and tackle them.[219] This, coupled with a federal safe harbor provision for reporting cybersecurity breaches of medical devices, would allow a clearer picture of the state of cybersecurity of the devices and allow

209. U.S. FOOD & DRUG ADMIN., *supra* note 122.
210. *Id.*
211. Caruso & Masters, *supra* note 56, at 33.
212. U.S. FOOD & DRUG ADMIN., *supra* note 122.
213. *Id.*
214. *Id.*
215. Templeton, *supra* note 48, at § 2.1.6; U.S. FOOD & DRUG ADMIN., *supra* note 122.
216. *See* U.S. FOOD & DRUG ADMIN., *supra* note 122.
217. *See* Vijayan, *supra* note 182.
218. *Id.*
219. *See* Kramer et al., *supra* note 76, at 7.

new cybersecurity issues to be addressed.[220] "[A]ctive and real-time surveillance and communication of emerging cyberthreats" can only help in securing all implantable medical devices.[221] While there is an inherent perceived danger to knowing and reporting cybersecurity of devices, security experts have long stated that secret cybersecurity protocols are commonly reversed engineered and easily defeated.[222] A better method of security is to have a system that is completely open to critique, thus making it more secure across the board.[223] This follows "[a] fundamental tenant of cryptography . . . known as Kerckhoffs' principle," which states that a system "should be secure even if the adversary knows everything about the system except its key."[224] By choosing a system that is in the public, the community as a whole only strengthens the end product's security by working on it together.[225]

A Host Intrusion Detection and Prevention System ("HIDS/HIPS") is another means of protecting implantable medical devices.[226] HIDS/HIPS, "technologies are based on managing a known behavior of a system," and preventing any unknown behavior from happening or taking over.[227] This kind of system would work well in implantable medical devices because it provides strong protection against attacks that have never occurred before.[228] However, there is always the possibility of a HIDS/HIPS preventing critical support from the device, and it can be tricked by a hacker.[229] Despite this, a HIDS/HIPS addresses some concerns for cybersecurity of implantable medical devices and warrants further exploration of implementation in implantable medical devices.[230]

There are other means to address cybersecurity concerns of implantable medical devices outside of conventional cybersecurity methods.[231] One involves "tattooing the encryption key" to an encrypted implantable medical device on the patient in an "invisible, UV-light-readable ink" for emergency situations.[232] Along the same vein of modifying the user for added cybersecurity protection is one type of cybersecurity control, tested

220. *See id.* at 2–3.
221. Perakslis, *supra* note 39, at 397.
222. Templeton, *supra* note 48, at § 2.1.8.
223. *See id.*
224. Ransford et al., *supra* note 2, at 160.
225. *Id.*
226. Wirth, *supra* note 26, at 31.
227. *Id.*
228. *Id.*
229. *See id.*
230. *See id.* at 31–32.
231. *See* Templeton, *supra* note 48, at § 3.1.
232. *Id.*

in a pacemaker, that allows access in emergency situations to medical personnel by connecting to a computer and using the patient's heartbeat as authorization for commands by an external system.[233] This, however, defeats the purpose of a wireless implantable medical device, and it would require surgery to access the internal medical device, putting the patient at risk.[234] Another option is a subcutaneous push switch that would be implanted under the skin of the patient for the purpose of reprogramming the device and allowing access, thus, allowing emergency personnel to be able to be reset in a failsafe mode.[235] Additionally, RF-shielding wearable pouches can accompany the patient, which would restrict the wireless communication of the implantable medical device to millimeters and require a security token to access.[236] Lastly, a standardizing score that applies to a device that answers in a satisfies/does not satisfy evaluation for each aspect of the device can be used to evaluate whether or not a device meets a certain score, which would determine whether it should be marketed.[237] While a high score in this area could be used by medical device manufacturers to promote their products as a new type of marketing edge over competitors, it trivializes cybersecurity and is not focused enough towards tackling specific issues.[238] If this system was coupled with suggestive FDA regulations, however, it could prove to be a general solution.[239]

Lastly, the United States can look towards the EU as a guidepost for how to approach cybersecurity in medical device software.[240] In Directive 2007/47/EC, the EU imposed stricter rules on software used with medical devices, although it only applies to software that directly controls the device.[241] The directive makes it so that all software is updated, validated, and approved from an authoritative agency, and does not change the risk classification of the device.[242] While this echoes what the FDA already does to an extent, the fact that it specifically covers and classifies the software of the medical device should be taken into consideration.[243] Additionally, the EU conducted a cybersecurity "exercise involving 29 countries and 200

233. Caruso & Masters, *supra* note 56, at 35.
234. *See* Ransford et al., *supra* note 2, at 162.
235. Templeton, *supra* note 48, at § 3.1.
236. *Id.*
237. Caruso & Masters, *supra* note 56, at 35.
238. *See id.*
239. *See* U.S. FOOD & DRUG ADMIN., *supra* note 122; Caruso & Masters, *supra* note 56, at 32, 35.
240. *See* Klümper & Vollebregt, *supra* note 187, at 83.
241. *Id.* at 83.
242. *Id.* at 85–86.
243. *See* U.S. FOOD & DRUG ADMIN., *supra* note 122; Klümper & Vollebregt, *supra* note 187, at 84–85.

agencies deal[ing] with attack scenarios against *critical infrastructure[s]*," which included hospitals and hacking into medical devices.[244] As the EU Commission Vice President stated, "[t]he sophistication and volume of cyberattacks are increasing every day. . . . They cannot be countered if individual states work alone or just a handful of them act together."[245] Outside of the EU, international standards bodies, such as the Association for the Advancement of Medical Instrumentation, have formed working groups and issued standards on medical device security that include manufacturers and regulators.[246] Regardless of whether the United States follows the EU or an international standardizing body, international harmonization of cybersecurity is almost inevitable due to the nature of the Internet.[247]

C. *Dangers with Governmental Regulation*

There are dangers with increased regulations that must be considered.[248] Regulations can become burdensome to technological advancement, with Congress—or any executive administrative body—failing to take into account the concerns of the healthcare industry and the knowledge of how to make a device that would not harm a patient by running slowly when implementing the regulations.[249] The industry itself must understand the capital and operating costs of implementing a cybersecurity system and factor that in, or else face potential inept and burdensome regulations.[250]

The FDA Guidance also recommends that manufacturers consider implementing things like authentication protocols, automatic timers to terminate connections with a device after a period of time, placing physical locks on the devices, and making stronger passwords to the devices.[251] It also recommends a layered user authentication procedure and restriction of updates, allowing users to download and update their own software and

244. *EU Holds Largest-Ever Cyber-Security Exercise, Defense of Critical Infrastructure the Focus*, FOX NEWS (Oct. 31, 2014), http://www.foxnews.com/tech/2014/10/31/eu-holds-largest-ever-cyber-security-exercise-defense-critical-infrastructure/.html.

245. *Id.*

246. Fu & Blum, *supra* note 40, at 37.

247. *See id.*

248. *See* Robert Mittman & Mary Cain, *The Future of the Internet in Healthcare: A Five-Year Forecast*, *in* THE INTERNET AND HEALTH COMMUNICATION: EXPERIENCES AND EXPECTATIONS 47, 55 (Ronald E. Rice & James E. Katz eds., 2001).

249. *See id.* at 55.

250. *Id.* at 55.

251. U.S. FOOD & DRUG ADMIN., *supra* note 122, at 5.

firmware from the manufacturer.[252] These recommendations, however, have already been considered to be dangerous by medical device manufacturers and have been proven to be harmful in locking out medical personnel in an emergency to a patient.[253] Many good cybersecurity requirements, in fact, conflict with the need for emergency access to a device.[254] Additionally, requiring implantable medical devices to incorporate certain software can have a major impact on the battery life of the device, reducing the longevity of the device and causing other potential issues.[255] This carries over into the plain fact that there are different levels of severity of vulnerabilities in implantable medical devices.[256] For example, a cardiac defibrillator can kill its user, while a non-actuating glucose sensor cannot do lethal damage on its own.[257] This danger must be taken into consideration when making any sort of regulations for implantable medical devices.[258]

Another regulatory concern is that there are usually compromises that specifically exclude certain areas from needing to be secured in making any regulation.[259] One example is "the NERC-CIP cybersecurity standard for the North American bulk power system," which specifically excludes non-routable protocols and narrowly defines devices considered critical assets bound by the regulatory standards.[260] Organizations typically do the minimum to meet regulatory compliance, which means excluding some areas, which would highlight weak areas for attackers to gain access.[261] Due to this practice, numerous people in the medical industry and the government are concerned that if standards are written and enforced, they may actually undermine the purpose of trying to protect the user of the implantable medical device.[262]

Finally, of course, increased regulation of certain medical devices can lead to an increase in the cost of certification and testing of the devices themselves.[263] An example is in the aviation industry, "where over 50% of the resources required to develop new, safety critical systems" are used in

252. *Id.*
253. *See* Gupta, *supra* note 22.
254. *See id*.
255. Ransford et al., *supra* note 2, at 159.
256. *Id.* at 161.
257. *Id.*
258. *See* Gupta, *supra* note 22.
259. Templeton, *supra* note 48, at § 4.2.
260. *Id.*
261. *Id.*
262. *Id.*
263. *See* Radhakisan Baheti & Helen Gill, *Cyber-Physical Systems*, *in* THE IMPACT OF CONTROL TECHNOLOGY 161, 163–64 (Tariq Samad & Anuradha Annaswamy eds., 2011).

just certifying the system.[264] For medical devices and cybersecurity, much of the hardware and software are still incapable of being reliant due to the need for more advanced and integrated technology, as current widely used techniques and protocols are inappropriate for the confined space of an implantable medical device.[265] The right balance needs to be found in regulation to establish security without creating expensive and complicated standards that are contradictory in nature.[266] Legislation and regulation can facilitate increasing cybersecurity through base guidelines for implantable medical devices, but they can also harm patients if they fail to take into account industry knowledge and dangers.[267]

V. CONCLUSION

Hackers have turned from hacking businesses and governments for fame and fortune to covert organized cybercrime, which is estimated to be exceeding the illegal drug trafficking trade.[268] It is dangerously naïve for the federal government and medical device manufacturers to fail to understand that "many individuals . . . are highly intelligent, skilled, and motivated" to find and exploit weaknesses in medical devices.[269] These devices were "'not designed to withstand terrorist attacks. . . . 'Permitting control of a component in a human body without authentication seems grossly negligent, and should raise the ire of the FDA.'"[270] Former Secretary of Defense, Leon Panetta, was correct in stating that an organized attack focused on vulnerabilities of implantable medical devices "could be a cyber Pearl Harbor, an attack that would cause physical destruction and the loss of life."[271]

The problem facing implantable medical device manufacturers is complex, requiring a balance of usability, performance, and safety, while taking into consideration the cybersecurity threats of a growing digitally connected world.[272] Without a standardized baseline for specifications, the interconnectivity of every medical device will negate some security features of others and create opportunities for attacks.[273] The "healthcare industry needs to . . . [become] involved in [the current] legislative process [on

264. *Id.* at 163.
265. Gupta, *supra* note 22.
266. Perakslis, *supra* note 39, at 397.
267. *See* Garrie & Paustian, *supra* note 146, at 45.
268. Wirth, *supra* note 26, at 26, 29.
269. Templeton, *supra* note 48, at § 2.1.7.
270. *Id.* at § 3.1.
271. Barnett et al., *supra* note 34, at 44.
272. Caruso & Masters, *supra* note 56, at 32.
273. *See* Templeton, *supra* note 48, at §§ 2.1, 4, 4.2.

implantable medical devices] or risk the imposition of . . . regulations" that can harm the product through unintended consequences and hinder the technological growth of implantable medical devices.[274]

The threat of cyberattacks is a clear and present danger, and it is time to focus on ways to protect the user from a technology that can be altered remotely to be a weapon instead of a significant life-changing tool.[275] It is up to key players—the "[p]roviders, manufacturers, security experts, industry organiz[ers], [and the government] . . . to work together to . . . protect [the] integrated healthcare" industry that is becoming more connected with the Internet every day.[276]

274. Mittman & Cain, *supra* note 248, at 55.
275. Perakslis, *supra* note 39, at 397.
276. Wirth, *supra* note 26, at 33.