Nova Law Review

Volume 41, *Issue* 3 2017 *Article* 6

Patient Safety Should Include Patient Privacy: The Shortcomings Of The FDA's Recent Draft Guidance Regarding Cybersecurity Of Medical Devices

Christopher Kersbergen*

*

Patient Safety Should Include Patient Privacy: The Shortcomings Of The FDA's Recent Draft Guidance Regarding Cybersecurity Of Medical Devices

Christopher Kersbergen

Abstract

Right now, a healthcare provider somewhere in the United States is being hacked or suffering the repercussions of a successful hack. Those healthcare providers that have not been attacked successfully likely have an individual attempting to penetrate the healthcare provider's network.

KEYWORDS: medical, devices, privacy

PATIENT SAFETY SHOULD INCLUDE PATIENT PRIVACY: THE SHORTCOMINGS OF THE FDA'S RECENT DRAFT GUIDANCE REGARDING CYBERSECURITY OF MEDICAL DEVICES

CHRISTOPHER KERSBERGEN*

I. INTRODUCTION

Right now, a healthcare provider somewhere in the United States is being hacked or suffering the repercussions of a successful hack. Those healthcare providers that have not been attacked successfully likely have an individual attempting to penetrate the healthcare provider's network. The attacker is targeting the weakest link in the healthcare provider's network, a connected medical device. The device is a wireless infusion pump that is present in nearly every hospital room and contains a host of cybersecurity vulnerabilities. A successful attack would allow the individual to change the dose of medicine the pump provides and potentially seriously injure or kill the patient, but the attacker only wishes to use the infusion pump to pivot

*. Christopher Kersbergen, M.S., J.D., is a Professor of Criminal Justice and the Program Director for the Legal Studies program at Keiser University. He is a United States Army veteran and received his law degree from Nova Southeastern University in 2015.

into the hospital's network. Once in the network, the attacker can access every device in the hospital and every patient's health record. The attacker then holds the hospital hostage by launching a ransomware attack.[1] The hospital is crippled by the attack and cannot access vital patient records, nurses' stations, test results, and monitoring equipment. The attacker holds the hospital hostage for a sum of money, which the hospital is forced to pay. The attack is over, but the repercussions to the hospital and the patients impacted last a lifetime. The hospital is fined millions of dollars for the loss of protected patient health information. The stolen patient information is sold and used.

A victim of the attack is denied a surgery by his or her health insurance carrier because a person used his or her stolen health information to have surgery a continent away. Another victim is billed for healthcare someone else received. Yet another person has private and embarrassing health information posted on the internet. All of the victims suffer in one form or another, many not realizing they have been a victim until it is too late. The frightening realization is that everyone, at one point, has been the victim of a cyberattack on a healthcare provider. The healthcare industry has become virtually dependent on medical devices, and individuals motivated by the enormous profits achievable by attacking medical devices are causing severe concerns for all stakeholders in the healthcare industry.[2]

The regulatory agencies that are responsible for protecting healthcare critical infrastructure from cybersecurity threats have been slow and reactive to the danger. Only within the last couple of years have they made cybersecurity a top priority.[3] The Food and Drug Administration ("FDA") is the government agency "responsible for . . . [ensuring] that medical devices are [both] safe and effective for use."[4] The FDA exercises its regulatory authority with regard to cybersecurity of medical devices in the form of

1. *Alert: Ransomware and Recent Variants*, US-CERT (Mar. 31, 2016), http://www.us-cert.gov/ncas/alerts/TA16-091A. "Ransomware is a type of malware that infects computer systems, restricting user[] access to the . . . system[] . . . [until] a ransom is paid . . . ." *Id.*

2. TRAPX LABS, TRAPX SEC., INC., ANATOMY OF AN ATTACK: MEDJACK (MEDICAL DEVICE HIJACK) 7–8 (2015).

3. *See Alert: Medical Devices Hard-Coded Passwords*, ICS-CERT (June 13, 2013), http://www.ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01; Billy Rios, *Hospira Plum A+ Infusion Pump Vulnerabilities*, BILLY (BK) RIOS (June 8, 2015), http://www.xs-sniper.com/blog/2015/06/08/hospira-plum-a-infusion-pump-vulnerabilities.

4. Laura Hagen, *Coding for Health: Cybersecurity in Medical Devices*, HEALTH LAW., June 2016, at 25, 25–26; *see also* 21 U.S.C. §§ 351, 360c(f), 360e(a) (2012); 21 C.F.R. § 806.1 (2016).

guidance documents issuing alerts about medical devices and product recalls.[5] In May of 2015, the FDA issued one such alert regarding a vulnerability identified with an infusion system that could allow an unauthorized user to control the device and change the dosage the pump delivers.[6] The alert came ten days after the U.S. Department of Homeland Security ("DHS") issued warnings on the very same pump.[7] It was the first time the FDA advised healthcare providers to discontinue use of a medical device because of cybersecurity concerns.[8] Both agencies and the manufacturer were aware of the vulnerability for over a year before the advisory was issued.[9] This prompted the increased focus by the FDA and other government agencies on the cybersecurity of medical devices.[10] The increased focus led to the FDA issuing guidance documents for the industry, titled *Postmarket Management of Cybersecurity in Medical Devices*.[11]

The FDA has largely been reactionary to cybersecurity threats but appears to be moving towards a proactive approach to ensure the safety of medical devices.[12] The guidance documents are a step in the right direction because of their risk-based approach to cybersecurity.[13] The guidance does have flaws, as it falls short on the issue of patient privacy protection, which is neither discussed nor mentioned.[14] The regulatory function of the FDA is

5. Hagen, *supra* note 4, at 25–26; *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, U.S. FOOD & DRUG ADMIN. (July 31, 2015), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm; *Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication*, U.S. FOOD & DRUG ADMIN. (May 13, 2015), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm.

6. *Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication*, *supra* note 5.

7. *See id.* The FDA published a safety communication for Hospira's PCA 3 LifeCare, PCA 5 LifeCare, and Symbiq lines of products. *Id.* ICS-CERT published an advisory for Hospira's Plum A+, Plum A+3, and Symbiq lines of products. *Advisory: Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities*, ICS-CERT (June 10, 2015), http://www.ics-cert.us-cert.gov/advisories/ICSA-15-161-01; *Advisory: Hospira Symbiq Infusion System Vulnerability*, ICS-CERT (July 21, 2015), http://www.ics-cert.us-cert.gov/advisories/ICSA-15-174-01.

8. *See Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication*, *supra* note 5.

9. *See* RIOS, *supra* note 3.

10. *See* OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., WORK PLAN: FISCAL YEAR 2015 22 (2015), http://www.oig.hhs.gov/reports-and-publications/archives/workplan/2015/FY15-Work-Plan.pdf.

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

12. *See id.*

13. *See id.*

14. *See id.*

focused primarily on the safety of the devices it regulates, not privacy, and because of that focus, manufacturers are free to ignore many of the issues that are causing the cybersecurity crisis of medical devices.[15]

This Article restricts the scope of the discussion of the FDA guidance documents to three key recommendations newly introduced, rather than a review of their contents.[16] The newly introduced recommendations include the introduction for the manufacturer defined essential clinical performance of a medical device, the distinction between controlled and uncontrolled risks, and promotion of membership in Information Sharing and Analysis Organization ("ISAO") for manufacturers.[17] Additionally, the guidance documents focus on medical devices that are already in the market and deployed in healthcare organizations.[18] Therefore, cybersecurity issues related to premarket considerations of a device are outside the scope of this Article. First, this Article addresses why medical devices have become such an attractive target for attackers and the cybersecurity challenges facing manufacturers.[19] The cybersecurity challenges that are discussed include hard-coded passwords, old and outdated equipment, and the inability for devices to detect or scan for malware infections.[20] Next, this Article focuses on the newly introduced definitions and recommendations found in the guidance documents.[21] Finally, this Article points out key shortcomings of the guidance documents, including: the lack of attention to patient privacy due to language that could potentially allow manufacturers to leave known vulnerabilities that do not affect the safety of the device unaddressed, the vague and problematic description of ISAO, and the lack of enforceable rules in the guidance.[22]

II. CHALLENGES SECURING MEDICAL DEVICES

The use of medical devices that are connected to computer networks has proliferated, as have attacks on medical devices.[23] Medical devices are now part of the Internet of things, and are exposed to the same cybersecurity

15. *Id.* The Office of the Inspector General is currently examining whether FDA oversight of networked medical devices is sufficient to effectively protect patient health information. OFFICE OF INSPECTOR GEN., *supra* note 10, at 50.

16. *See infra* Parts II–IV.

17. U.S. FOOD & DRUG ADMIN., *supra* note 11.

18. *Id.*

19. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; *infra* Part II.

20. *See infra* Sections II.A–C.

21. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; *infra* Part III.

22. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; *infra* Part IV.

23. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.

threats to which anything connected to the Internet is exposed.[24] While networked medical devices facilitate care, they also introduce a host of new cybersecurity risks for patients and for the hospitals that are using the devices.[25]

Criminals can gain access to devices that contain little or no cybersecurity protection, and, once breached, they are able to access any personal or medical information that is stored on the device or potentially control the device itself.[26] Healthcare is increasingly targeted by cybercriminals for a relatively simple reason: Crime pays.[27] Patient health information is worth substantially more money on the black market than is credit card information.[28] Credit card information can be sold for one or two dollars; patient health information, though, can go for as high as forty dollars per record.[29] That information can be used to commit insurance fraud, identity theft for financial gain, or a specific targeted attack against an individual.[30] For example, an attacker can take information obtained from patient health information to disclose embarrassing or private and sensitive information to the victim's friends and family.[31] In terms of safety, they could possibly change the coding of a medical device—controlling anything from the amount of medicine that is dispensed, to even changing health data collected by a device.[32] A doctor could conceivably make wrong decisions based on altered information obtained from a medical device.[33]

Multiple government agencies have been focusing on the cybersecurity of medical devices in recent years.[34] Among them, the Federal Bureau of Investigation ("FBI") investigated healthcare as a high profile risk, releasing a private industry notification, FBI Case No. 140408-009, stating there will be a likely increase in cyber intrusions due to lax cybersecurity

24. *Internet of Things Poses Opportunities for Cyber Crime*, FBI: INTERNET CRIME COMPLAINT CTR. (Sept. 10, 2015), http://www.ic3.gov/media/2015/150910.aspx.

25. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; *Internet of Things Poses Opportunities for Cyber Crime*, *supra* note 24.

26. *Internet of Things Poses Opportunities for Cyber Crime*, *supra* note 24; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 11.

27. *See* TRAPX LABS, *supra* note 2, at 7–8.

28. *See id.* at 8.

29. *Id.*; Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, SECUREWORKS: CTU RESEARCH (July 15, 2013), http://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents.

30. INST. FOR CRITICAL INFRASTRUCTURE TECH., HACKING HEALTHCARE IT IN 2016: LESSONS THE HEALTHCARE INDUSTRY CAN LEARN FROM THE OPM BREACH 4, 25 (2016).

31. *See id.* at 3–4, 11, 16.

32. *Id.* at 48; *see also* Hagen, *supra* note 4, at 25.

33. *See* INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 48.

34. *Id.* at 2; Hagen, *supra* note 4, at 25.

standards.[35] Clearly, the main factor driving cyberattacks on connected medical devices is that successful attacks lead to enormous profits.[36] Compounding the problem are reports that the healthcare industry is not prepared to combat even the most basic of cyberattacks.[37] Healthcare organizations and the medical devices they use are low hanging fruit because there are no regulations that require a medical device to meet minimum cybersecurity standards before going to the market.[38] Over two-thirds of healthcare provider organizations have experienced a cyberattack in one form or another over the last few years, with the number of attacks possibly being much higher.[39]

Numerous other factors contribute to the explosion of attempts to attack medical devices, but one of the largest contributors is healthcare organizations converting to electronic health records.[40] It is frightening to consider that medical devices often run the same standard operating systems as copy machines and printers, and connect to the Internet in similar or the same way as laptops and smartphones connect through Wi-Fi or Bluetooth.[41] Unlike many personal devices, medical devices often do not receive updates to protect security, nor are they protected from outside intrusions.[42] Many have hard-coded passwords that can be looked up by anyone with knowledge of the device.[43] A medical device that provides the best example of just how difficult of a challenge securing medical devices can be is an infusion pump.[44] Infusion pumps are generally networked in nearly every hospital

35. *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIV. (Apr. 8, 2014), http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf.

36. *Id.*; *see also* INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 11.

37. *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, *supra* note 35.

38. *See* J.M. Porup, *Why Aren't There Better Cybersecurity Regulations for Medical Devices?*, VICE: MOTHERBOARD (Oct. 19, 2015, 7:00 AM), http://motherboard.vice.com/read/why-arent-there-better-cybersecurity-regulations-for-medical-devices.

39. Alex Ruoff, *Health-Care Industry Spending More on Security but Not Ready for Cyberattack*, BLOOMBERG BNA: HEALTH IT L. & INDUSTRY REP. (Nov. 10, 2015), http://www.bna.com/healthcare-industry-spending-n57982063383.

40. *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, *supra* note 35.

41. INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 44, 46, 61.

42. *Id.* at 3, 61.

43. *See id.* at 36, 70; *infra* Part II.B.

44. *See* Hagen, *supra* note 4, at 25.

room and have been on the market for years.[45] The cell phone in your pocket likely has more cybersecurity protection than an infusion pump, a critically important medical device.[46] Medical devices will never be completely secure from cybersecurity vulnerabilities.[47] However, many of the vulnerabilities that affect medical devices are self-inflicted by design.[48] The devices themselves do not deserve all of the blame, as healthcare organizations often do not consistently report security issues to the FDA reporting program.[49]

A. *Hard-Coded Passwords*

The majority of infusion pumps have both maintenance usernames, which allow for technical support, and passwords that are hard-coded.[50] In 2013, the DHS issued an alert stating that over 300 medical devices from forty different vendors contained hard-coded passwords that could be exploited in order to change critical settings in the device.[51] A hard-coded password is exactly what it sounds like, a password for the device that is programmed by the manufacturer and cannot be changed.[52] Devices affected included infusion pumps, ventilators, patient monitors, and surgical devices, among many others.[53] The dilemma facing medical device manufacturers that choose hard-coded passwords for their devices is a complicated one to reconcile.[54] A hard-coded password allows manufacturers to troubleshoot

45. *See* HEALTHCARE TECH. SAFETY INST., AAMI FOUND., SAFETY INNOVATIONS: BEST PRACTICE RECOMMENDATIONS FOR INFUSION PUMP-INFORMATION NETWORK INTEGRATION 3–4 (2012); Hagen, *supra* note 4, at 25.

46. *See* INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 36, 61.

47. U.S. FOOD & DRUG ADMIN., *supra* note 11.

48. *See* INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 48.

49. Russell L. Jones, *Networked Medical Device Cybersecurity and Patient Safety: Thoughts on Collaborative Approaches*, DELOITTE: DCHS (Oct. 21, 2013, 12:00 PM), http://www.deloitte.typepad.com/centerforhealthsolutions/2013/10/networked-medical-device-cybersecurity-and-patient-safety-time-to-step-up-to-the-plate.html#.

50. *See* GAVIN O'BRIEN, NAT'L INST. OF STANDARDS & TECH., WIRELESS MEDICAL INFUSION PUMPS 3–4 (2015); INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 33, 70; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3.

51. *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3.

52. JASON HEALEY ET AL., THE HEALTHCARE INTERNET OF THINGS: REWARDS AND RISKS 14 (2015); *see also* INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 33–34, 70; O'BRIEN, *supra* note 50, at 2; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3.

53. *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3; *see also* O'BRIEN, *supra* note 50 at 2–3.

54. HEALEY ET AL., *supra* note 52, at 14; INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 35, 70–74; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3.

any problems with the device remotely because, generally, only the device manufacturer can provide technical support and fixes to a malfunctioning device.[55]

Hard-coded passwords also allow medical personnel access to the device in case of an emergency.[56] For example, if a person with an embedded pacemaker collapses while on vacation, a hard-coded password allows medical personnel to quickly render assistance because they can look up the password for the device quickly.[57] The downside is that anyone can obtain the password to that device with a little bit of effort and a Google search.[58] When medical personnel leave the hospital, there is an inability to revoke the access to the device of the former employee.[59] The most distressing issue with hard-coded passwords is that an attacker can breach a device and actively be in a healthcare organization's network for months without detection.[60] The use of hard-coded passwords may be the easiest cybersecurity challenge to fix for manufacturers in the future, as all that would be needed is to not deploy devices with hard-coded passwords.

B. *Outdated Software and Operating Systems*

The FDA's alert regarding the Hospira's Infusion System shows the challenges of securing medical devices that have been in the market for years from attackers.[61] The pump was over ten years old at the time of the alert but

55. HEALEY ET AL., *supra* note 52, at 14; *see also* INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 36–37; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3.

56. HEALEY ET AL., *supra* note 52, at 14; *see also* INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 36–37; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3.

57. *See* HEALEY ET AL., *supra* note 52, at 14.

58. INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 73; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3.

59. *See* HEALEY ET AL., *supra* note 52, at 14; INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 3–4.

60. *See* HEALEY ET AL., *supra* note 52, at 14; INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 3, 70, 73–74; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3.

61. *See* U.S. FOOD & DRUG ADMIN., 510(k) No. K042081, PLUM A+ INFUSION SYSTEM WITH HOSPIRA MEDNET SOFTWARE AND PLUM A+3 INFUSION SYSTEM WITH HOSPIRA MEDNET SOFTWARE (2004), http://www.accessdata.fda.gov/cdrh_docs/pdf4/K042081.pdf; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3; *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, *supra* note 5; *Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication*, *supra* note 5.

still widely in use.[62] It was also in the process of being phased out for a newer model for reasons not related to cybersecurity.[63] It is likely that the pump was using an unsupported operating system that was no longer being updated or patched to address vulnerabilities.[64] The device had a staggering amount of vulnerabilities, the worst of which was that the pump could be accessed remotely and "allow . . . unauthorized user[s] to control the device."[65] The Hospira Infusion System case appears to be a common issue for medical devices.[66] Many medical devices are "running out of date . . . operating systems such as Windows 2000, Windows XP, or Linux."[67] These operating systems are patched less often than other connected systems.[68] Many manufacturers believe that changes to a device, including patches to address vulnerabilities, would require them to obtain re-approval from the FDA so they do not update and patch them.[69] The FDA guidance documents actually state that this common misconception, held by manufacturers about patching vulnerabilities, is not the case.[70] Even so, patching or updating a medical device to address vulnerabilities takes time.[71] Time is not a luxury if there is a severely dangerous vulnerability in a medical device, and if a medical device is surgically implanted, patching firmware or software may

62. *See* 510(k) No. K042081, *supra* note 61; *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, *supra* note 5; *Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication*, *supra* note 5.

63. *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, *supra* note 5.

64. *See id.*

65. *Id.*; *see also Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication*, *supra* note 5.

66. *See* INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 73; *Alert: Medical Devices Hard-Coded Passwords*, *supra* note 3; *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, *supra* note 5; *Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication*, *supra* note 5.

67. TRAPX LABS, *supra* note 2, at 10.

68. *See id.*

69. *See* HEALEY ET AL., *supra* note 52, at 14; TRAPX LABS, *supra* note 2, at 9–10.

70. *See* TRAPX LABS, *supra* note 2, at 9; U.S. FOOD & DRUG ADMIN., *supra* note 11.

71. *See* TRAPX LABS, *supra* note 2, at 9.

not be practical or feasible.[72] The fix is to disconnect the device from the network, but this defeats the purpose of having networked medical devices.[73]

C. *Lack of Malware Scanning*

The most serious cybersecurity threat to medical devices is malware.[74] As stated previously, the motivation for the majority of attacks on medical devices is financial, and the primary way an attacker obtains profitable information is through the deployment of malware.[75] A laptop, home computer, and a cellphone have the option to download a program that scans for malware that may be infecting those devices.[76] Many medical devices come without antivirus or malware protection, basic encryption, or vulnerability lifecycle management.[77] Even if there is malware scanning capabilities in a medical device, medical devices are generally unable to perform these scans because most are in use twenty-four hours a day, 365 days out of the year.[78] They are also closed systems, not open for installation of any third party software that could scan for viruses or malware.[79] If scanning software can be installed, it may void the warranty of the device.[80] This means that unless a device has a malware or virus scanner built in, there would be no way to determine that the medical devices are infected until it is much too late.[81] "Finally, even when sophisticated attacks are detected, it is still very difficult to remove the malware and blunt the attack without the full cooperation of the medical device manufacturer."[82]

---

72. *See* HEALEY ET AL., *supra* note 52, at 14; *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, *supra* note 5; *Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication*, *supra* note 5.

73. *See* HEALEY ET AL., *supra* note 52, at 13; TRAPX LABS, *supra* note 2, at 35; *Cybersecurity Vulnerabilities of Hospira Symbriq Infusion System: FDA Safety Communication*, *supra* note 5.

74. *See* HEALEY ET AL., *supra* note 52, at 12.

75. *See* TRAPX LABS, *supra* note 2, at 5–6; *Alert: Ransomware and Recent Variants*, *supra* note 1.

76. *See* HEALEY ET AL., *supra* note 52, at 13–14; TRAPX LABS, *supra* note 2, at 10; *Alert: Ransomware and Recent Variants*, *supra* note 1.

77. *See* TRAPX LABS, *supra* note 2, at 9, 16, 37–38.

78. *Id.* at 9–10, 35.

79. *Id.* at 35.

80. *See id.* at 10–11.

81. *See* HEALEY ET AL., *supra* note 52, at 16; TRAPX LABS, *supra* note 2, at 11.

82. TRAPX LABS, *supra* note 2, at 35.

III. FDA POSTMARKET GUIDANCE OVERVIEW

The FDA faces the challenge of promoting safe and secure medical devices while trying not to stifle innovation by issuing restrictive and burdensome regulations.[83] Through the use of guidance documents, the FDA tries to recommend the best possible practices for manufacturers to protect patient safety.[84] The guidance promotes a risk management process for manufacturers to address cybersecurity.[85] It also reiterates that cybersecurity is a shared responsibility among stakeholders.[86] Device manufacturers, vendors, information technology professionals, health information technology developers, and the users of medical devices are the stakeholders responsible for cybersecurity.[87] Stakeholders are numerous and varied, but the FDA only regulates manufacturers of medical devices, which makes cybersecurity even more difficult.[88] That is why the main goal of the FDA's cybersecurity approach is collaboration between stakeholders, because an effective cybersecurity program is only as good as the weakest link.[89] Often, this weakest link changes depending on the threat.[90] For example, a device that is perfectly secure from outside attackers may still end up being compromised and affect patient safety because the patients themselves tampered with the device, or a hospital employee infects a hospital network because they clicked on a link contained in a suspicious email.[91] What can the FDA do when a user of a medical device does not follow good cybersecurity practices and infects an entire network, putting patient safety at risk? The guidance attempts to achieve this goal of collaboration between stakeholders by issuing recommendations to manufacturers that help mitigate the various threats to medical devices.[92]

83. *See id.* at 6, 9–10.

84. U.S. FOOD & DRUG ADMIN., *supra* note 11; *see also* TRAPX LABS, *supra* note 2, at 9–10.

85. U.S. FOOD & DRUG ADMIN., *supra* note 11; TRAPX LABS, *supra* note 2, at 9–10. "Th[e] [G]uidance applies to: (1) medical devices that contain software, including firmware, or programmable logic, and (2) software that is a medical device." U.S. FOOD & DRUG ADMIN., *supra* note 11.

86. U.S. FOOD & DRUG ADMIN., *supra* note 11.

87. *Id.*; *see also* TRAPX LABS, *supra* note 2, at 35.

88. U.S. FOOD & DRUG ADMIN., *supra* note 11.

89. *See id.*; TRAPX LABS, *supra* note 2, at 12.

90. *See* TRAPX LABS, *supra* note 2, at 12.

91. *See id.* at 9.

92. U.S. FOOD & DRUG ADMIN., *supra* note 11.

A. *Defining Essential Clinical Performance*

The inability to be completely secure from threats is a common statement made by the FDA, as it has appeared in nearly every cybersecurity related communication released by the agency.[93] The FDA introduces the term *essential clinical performance* as a way to compensate for the reality that a device will never be free of vulnerabilities.[94] Essential clinical performance is thus used to gauge whether a vulnerability in a device would trigger safety concerns for patients.[95] When a vulnerability compromises the essential clinical performance of a device, there is a situation where that vulnerability could result in severe injury or death in a patient.[96] In that event, manufacturers would be required to intervene and remedy that vulnerability as soon as possible to prevent those situations from occurring.[97] Manufacturers are directed to define the essential clinical performance of their device, the outcomes in terms of severity if compromised, and the level of risk that is acceptable.[98] Vulnerabilities that do not have an impact on the essential clinical performance are supposed to be assessed in case those vulnerabilities do impact the essential clinical performance of the device in the future.[99] Essentially, the FDA is telling manufacturers to triage cybersecurity of their devices.[100]

Manufacturers are recommended to assess the cybersecurity risk to their device by considering the exploitability of the vulnerability and the severity of the health impact to patients if the vulnerability were to be exploited.[101] Manufacturers are given latitude in how they assess these two considerations as long as it is industry accepted.[102] The FDA does recommend using the Common Vulnerability Scoring System, Version 3.0, to assess exploitability and ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices—Application of Risk Management to Medical Devices to assess severity of the health impact to patients.[103]

---

93. *Id.*

94. *Id.* Essential clinical performance is defined as "performance that is necessary to achieve freedom from unacceptable clinical risk." *Id.*

95. *Id.*

96. U.S. FOOD & DRUG ADMIN., *supra* note 11.

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.*

101. U.S. FOOD & DRUG ADMIN., *supra* note 11.

102. *Id.*

103. *Id.* "The Common Vulnerability Scoring System ("CVSS") is an open framework for communicating the characteristics and severity of software vulnerabilities." FORUM OF INCIDENT RESPONSE & SEC. TEAMS, COMMON VULNERABILITY SCORING SYSTEM

B. *Controlled and Uncontrolled Risks*

The FDA states that manufacturers determine if risks to essential clinical performance are acceptable or unacceptable.[104] Here, the guidance documents again introduce new terms: those that are controlled and uncontrolled.[105] If a risk is acceptable, it is labeled controlled, and unacceptable risks are labeled uncontrolled.[106] Again, acceptable risks do not impact patient safety.[107] Controlled risks do not affect a medical device's essential clinical performance, meaning that there is no impact on patient safety.[108] Here, the guidance issues its most important statement.[109] Any change made to the medical device to address a controlled risk is considered a device enhancement.[110] This means that a manufacturer deploying a patch or update of the device would not have to report it to the FDA.[111] This is welcomed news, as manufacturers are free to update and patch their devices without worry that their medical devices will need to be reapproved by the FDA because of changes or updates.[112]

An uncontrolled risk contains an unacceptable risk to the essential clinical performance of the device.[113] Patient safety is threatened with the presence of an uncontrolled risk, and control of the medical device could be compromised.[114] Manufacturers are recommended to remedy these risks as quickly as possible, or to at least reduce the risk to an acceptable level.[115] All uncontrolled risks to essential clinical performance are required to be reported to the FDA according to Title 21 of the Code of Federal Regulations part 806.[116] Interestingly, the FDA will not enforce reporting requirements if "[t]here are no known serious adverse events or deaths associated with the vulnerability."[117] This intent not to enforce the reporting requirements comes with the caveat that "[w]ithin [thirty] days of learning of the

---

v3.0: SPECIFICATION DOCUMENT 1 (2015), http://www.first.org/cvss/cvss-v30-specification-v1.7.pdf.

104. U.S. FOOD & DRUG ADMIN., *supra* note 11.
105. *Id.*
106. *Id.*
107. *See id.*
108. *See id.*
109. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.
110. *Id.*
111. *See* 21 C.F.R. § 806.1(b)(1) (2016); U.S. FOOD & DRUG ADMIN., *supra* note 11.
112. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.
113. *Id.*
114. *Id.*
115. *Id.*
116. 21 C.F.R. § 806.1; U.S. FOOD & DRUG ADMIN., *supra* note 11.
117. U.S. FOOD & DRUG ADMIN., *supra* note 11.

vulnerability, the manufacturer identifies and implements device changes . . . or compensating controls to bring the . . . risk to an acceptable level."[118] Manufacturers must also notify users and be a participant in an ISAO to avoid reporting requirements.[119] If a manufacturer cannot remedy the uncontrolled risk, the FDA would then consider that there is a reasonable probability that the device will cause serious injury or death, and the device would then "be considered [to be] in violation of the [Federal Food, Drug, and Cosmetic] Act . . . subject[ing it] to enforcement or other action."[120]

C. *Information Sharing and Analysis Organizations*

The guidance documents state that the sharing of risk information and intelligence within the medical device community is of critical importance in the adoption of a risk-based approach to cybersecurity, and ISAOs fulfill that critically important role.[121] These ISAOs are intended to serve as focal points for information and collaboration of cybersecurity issues between the private sector and government.[122] The stated purpose of an ISAO is to develop a shared understanding of risks to medical devices so stakeholders can efficiently assess patient health risks.[123] Participation in an ISAO is voluntary for manufacturers; however, the FDA considers participation a critical component of an effective cybersecurity risk management program.[124] The guidance stresses the importance of participation by calling it "a significant step toward assuring the . . . safety and effectiveness of . . . medical devices."[125] The FDA further incentivizes participation by indicating that it "does not intend to enforce certain reporting requirements of the Federal Food, Drug, and Cosmetic Act."[126] Participation in an ISAO and following the other recommendations in the guidance are prerequisites to the FDA using discretion in enforcement of reporting requirements.[127]

ISAOs are intended by the FDA to include groups from any sector, not just healthcare, and participation is inclusive and open to any that wish to join.[128] The FDA states that ISAOs would also allow participating members

118. *Id.*
119. *Id.*
120. *Id.*
121. *Id.*
122. U.S. FOOD & DRUG ADMIN., *supra* note 11.
123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. U.S. FOOD & DRUG ADMIN., *supra* note 11.
128. *Id.*

to receive "[a]ctionable . . . useful, and practical cybersecurity [information] . . . and incident information [through] automated, real-time mechanisms," although it does not elaborate on how that will be accomplished.[129] The FDA envisions ISAOs as transparent in terms of providing information to potential members on how the ISAO operates because they are intended to be trusted.[130] The information shared will be safeguarded to preserve business confidentiality.[131] "[P]articipants in an ISAO can request that . . . information [provided] be treated as Protected Critical Infrastructure Information."[132] This "information is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is [also] exempt from regulatory . . . and civil litigation" use.[133]

IV. SHORTCOMINGS OF THE FDA GUIDANCE

The guidance can essentially be broken down into two components, both of which fall short of addressing the severe cybersecurity challenges facing medical devices.[134] The FDA recommends that manufacturers adopt risk management programs consistent with, and incorporating elements of, the "[National Institute of Standards and Technology] Framework for Improving Critical Infrastructure Cybersecurity."[135] The basic elements of which are "[i]dentify, [p]rotect, [d]etect, [r]espond, and [r]ecover."[136] The framework is risk based, designed to manage risk, and intended to complement an organization's already existing cybersecurity program.[137] The framework is a good recommendation, however, it should be tailored to fit the healthcare industry, as the framework is not industry specific and is intended to complement existing cybersecurity management programs.[138] Where the recommendations in the guidance fall short is incorporating the newly introduced "essential clinical performance" and "controlled and uncontrolled risk" into the risk management process.[139] The second component that is problematic is the pressure to join "information sharing and analysis organizations" without providing any detail on how they will

129. *Id.*
130. *Id.*
131. *Id.*
132. U.S. FOOD & DRUG ADMIN., *supra* note 11.
133. *Id.*
134. *See id.*
135. *Id.*
136. *Id.*
137. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.
138. *Id.*; *see also* Hagen, *supra* note 4, at 34–35.
139. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.

operate, what information will be available, and how information shared will be protected.[140]

A. *Patient Privacy v. Patient Safety*

The guidance, as written, fails to address privacy concerns because the distinction between controlled and uncontrolled risk will allow manufacturers to ignore cybersecurity vulnerabilities that impact patient privacy.[141] Essential clinical performance is directly tied only to patient safety concerns, implying that any vulnerability that will not result in injury or death could be ignored.[142] Manufacturers are free to address any vulnerability that does not impact safety at their leisure.[143] The manufacturer could also ignore the vulnerability altogether, since there are usually no consequences for the manufacturer when a healthcare organization has a breach and patient health information is stolen.[144] The guidance documents do not address any patient privacy concerns and reinforce a view that privacy is not a cybersecurity priority for the FDA.[145] Granted, the FDA's primary purpose is to ensure medical devices are safe for patients above anything else.[146] The focus on safety is understandable, as a device that can seriously injure or even kill a patient is much more harmful than a device that has stolen the personal and financial information of perhaps every patient in a given healthcare organization.[147] What is not considered is that the loss of patient privacy can also result in harm to a person's reputation, economic situation, and mental health.[148] Although patient information is covered by laws such as the Health Insurance Portability and Accountability Act ("HIPAA"), manufacturers are not usually subject to that law.[149]

140. *See id.*

141. *See id.*; Comment Letter from American Association for Justice, Comment Letter on Postmarket Management of Cybersecurity in Medical Devices, (Apr. 21, 2016), http://www.regulations.gov/document?D=FDA-2015-D-5105-0031.

142. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.

143. *See id.*; Hagen, *supra* note 4, at 28.

144. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; Comment Letter from American Association for Justice, *supra* note 141.

145. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; Comment Letter from American Association for Justice, *supra* note 141.

146. *See* OFFICE OF INSPECTOR GEN., *supra* note 10, at 47.

147. *See* Hagen, *supra* note 4, at 26.

148. INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 8–9.

149. *See* Hagen, *supra* note 4, at 30; *When May a Covered Health Care Provider Disclose Protected Health Information, Without an Authorization or Business Associate Agreement, to a Medical Device Company Representative?*, U.S. DEP'T HEALTH & HUM. SERVS. (Feb. 4, 2004), http://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-

HIPAA regulates either covered entities, which consist of healthcare providers or health plans, and business associates, which can be entities that either "create[], receive[], maintain[], or transmit[] [patient] health information" or perform other services on behalf of a covered entity that involve the disclosure of patient health information.[150] A medical device manufacturer would generally not be considered a covered entity, but a medical device manufacturer is subject to HIPAA if they are business associates of a covered entity.[151] While this means that medical device manufacturers must comply with HIPAA as business associates, manufacturers can avoid business associate classification altogether by ensuring that they merely sell or provide software or equipment to a covered entity and the manufacturer does not have access to the patient health information.[152] Even when there is a situation where patient health information may need to be accessed by the manufacturer, the manufacturer could avoid having to comply with HIPAA by ensuring the health information is not personally identifiable.[153] In these cases, a medical device manufacturer is not subjected to any regulation that protects patient privacy.[154]

The College of Healthcare Information Management Executives ("CHIME") and the Association for Executives in Healthcare Information Security ("AEHIS"), in their public comment to the FDA's guidance, proposed a solution for addressing the patient privacy shortcomings of the guidance.[155] They suggested inserting patient safety and patient information subcategories under both controlled and uncontrolled risk.[156] This would ensure that uncontrolled vulnerabilities that do not cause any patient safety issues, and as such do not affect essential clinical performance, are still addressed, and any harm to patients and healthcare organizations is

---

a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html.

150. 45 C.F.R. § 160.103(4)(1)(i) (2013).

151. *Id.* § 160.103(4)(3)(i).

152. Public Welfare, 78 Fed. Reg. 5566, 5571 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160).

153. *Id.* at 5574.

154. *See id.*; *When May a Covered Health Care Provider Disclose Protected Health Information, Without an Authorization or Business Associate Agreement, to a Medical Device Company Representative?*, *supra* note 149.

155. Comment from CHIME & AEHIS, Comment Letter on Postmarket Management of Cybersecurity in Medical Devices (Apr. 21, 2016), http://chimecentral.org/wp-content/uploads/2014/11/CHIME-AEHIS-Letter-to-FDA-on-Device-Cyber.pdf.

156. *Id.*; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 11.

minimized.[157] The guidance as it is written now would potentially allow an attacker to access a networked medical device with a controlled vulnerability, and then once inside a healthcare organization's network, pivot, and potentially access other devices and subsequently impact patient safety by exploiting vulnerabilities in other devices.[158] Attackers are overwhelmingly focused on, and targeting, patient data.[159] The disproportionate focus by the FDA on patient safety, when there has not been an event where a patient has been harmed, may send the message to those intent on stealing information that cybersecurity in devices that do have vulnerabilities that impact safety is weak.[160] The perception of weak security is already driving motivations to attack, and the guidance setting aside privacy concerns could lead to a greater numbers of attacks.[161]

B. *ISAO Poorly Defined and Full of Risk*

The guidance suggestion that manufacturers join an ISAO is problematic because the language implies any group or individual can join an ISAO and have access to the information being shared about vulnerabilities.[162] Indeed, the guidance specifically states that membership is inclusive for anyone and everyone that wishes to join.[163] The assumption from the language indicates that information shared with the ISAO would be publicly available, meaning good intentioned members will be participants in ISAOs with members that do not have good intentions.[164] Hackers and other opportunists looking for information on exploitable vulnerabilities will no doubt be members of those very same ISAOs as well.[165]

In August 2016, MedSec, a startup cybersecurity firm based in Florida, provided an example of just how badly information-sharing of

157. Comment from CHIME & AEHIS, *supra* note 155; *see also* U.S. FOOD & DRUG ADMIN., *supra* note 11.

158. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; HEALEY ET AL., *supra* note 52, at 11; INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 10; Hagen, *supra* note 4, at 25.

159. INST. FOR CRITICAL INFRASTRUCTURE TECH., *supra* note 30, at 3–4.

160. *See id.*; Comment from CHIME & AEHIS, *supra* note 155.

161. *See* Comment from CHIME & AEHIS, *supra* note 155; U.S. FOOD & DRUG ADMIN., *supra* note 11.

162. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.

163. *Id.*

164. *See id.*

165. *See* Clarke, *supra* note 29; Comment from CHIME & AEHIS, *supra* note 155.

cybersecurity vulnerabilities can go.[166] The firm discovered alleged security flaws in pacemakers made by St. Jude Medical, a medical device manufacturer.[167] Rather than offer to sell the information to the manufacturer, or report the information to the FDA like some researchers do, they sold the information to Muddy Waters, an investment research firm.[168] Muddy Waters promptly announced it was shorting St. Jude stock based on the information.[169] Based on the reported vulnerabilities, the FDA and the DHS also announced they were investigating the manufacturer's device.[170] The fees for MedSec were predicated on how well Muddy Waters' short position did.[171] If the stock tanked, which it did, the fee would be higher.[172] St. Jude vigorously denied the allegations and cybersecurity researchers have panned the report released by MedSec as flawed.[173] The damage had already been done though. Not only are medical devices exploitable, so too is the information about vulnerabilities affecting those devices.[174]

The guidance documents are silent on any statutory, or regulatory, protections members of ISAOs would receive.[175] While information-sharing is important, the value of information diminishes if it is not actionable, or, if there are large amounts of information.[176] The guidance documents require manufacturers to report all uncontrolled vulnerabilities, even those that do not affect patient safety, possibly flooding ISAOs with information on vulnerabilities, many of them harmless.[177] Worse, some vital information may be excluded based on the different regulatory environments of the varied stakeholders.[178] Whether healthcare delivery organizations could

166. *See* Elaine Ou, *Hacking a Company's Stock Price*, BLOOMBERG: VIEW (Sept. 12, 2016, 10:30 AM), http://www.bloomberg.com/view/articles/2016-09-12/hacking-a-company-s-stock-price.

167. *Id.*

168. *Id.*

169. *Id.*

170. Jim Finkle, *U.S. Health Regulator Plans 'Thorough' Probe of St. Jude Case*, REUTERS (Sept. 8, 2016, 7:05 PM), http://www.reuters.com/article/us-st-jude-medical-cyber-fda-idUSKCN11E32Y.

171. Ou, *supra* note 166.

172. *See id.*; Aaron Pressman, *Hacking Report on St. Jude Pacemakers Was Flawed, Researchers Say*, FORTUNE (Aug. 31, 2016, 9:02 AM), http://www.fortune.com/2016/08/31/hacking-st-jude-pacemakers-flawed/.

173. Ou, *supra* note 166; Pressman, *supra* note 172.

174. *See* Finkle, *supra* note 170.

175. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.

176. *See id.*

177. *Id.*

178. Comment from Rapid7, Comments to FDA's Draft Guidance for Postmarket Management of Cybersecurity in Medical Devices (Apr. 19, 2016), http://www.rapid7.com/globalassets/_pdfs/rapid7-comments/rapid7-comments-to-fda-draft-

potentially violate a regulation or law, such as HIPAA, by providing information regarding a vulnerability to an ISAO that puts patient information at risk, is a question that should be addressed by the guidance documents.[179]

Without any detailed criteria about how these organizations work, the governance process, or safeguards of information, it is unlikely that manufacturers would join even though participation is greatly incentivized.[180] The FDA also includes a red herring regarding the incentive to manufacturers to join an ISAO.[181] Medical device manufacturers would not be required to report uncontrolled cybersecurity vulnerabilities under Title 21, section 806 of the Code of Federal Regulation if certain requirements are met.[182] The most important requirement is that there are no known serious adverse events or deaths associated with the vulnerability.[183] As previously stated, that means the guidance obligates manufacturers to report to an ISAO all uncontrolled vulnerabilities, increasing the burden on manufacturers that right now do not have to report those vulnerabilities.[184]

C. *Recommendations Not Requirements*

Obligating manufacturers to report based on what is written in the guidance is a misnomer, as nothing in the guidance requires manufacturers to do anything different than what they are doing now.[185] The guidance is inadequate because it is not enforceable and does not hold manufacturers "responsible for unsecured or defective [cybersecurity of] medical devices."[186] Cybersecurity threats and attacks are getting worse.[187] Healthcare organizations are being subjected to ransomware attacks,

---

guidance-for-postmarket-management-of-cybersecurity-in-medical-devices---docket-no.-fda-2015-d-5105---apr.-19-2016.pdf.

179. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.

180. *See id.*; Comment from Fresenius Kabi, Comment Letter on FDA Draft Guidance on Postmarket Management of Cybersecurity in Medical Devices (Apr. 21, 2016), http://www.regulations.gov/contentStreamer?documentId=FDA-2015-D-5105-0038&attachmentNumber=1&disposition=attachment&contentType=pdf.

181. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; Comment from Fresenius Kabi, *supra* note 180.

182. U.S. FOOD & DRUG ADMIN., *supra* note 11; Comment Letter from American Association for Justice, *supra* note 141; *see also* 21 C.F.R. § 806.1(b) (2016).

183. U.S. FOOD & DRUG ADMIN., *supra* note 11.

184. *See id.*; Comment Letter from American Association for Justice, *supra* note 141.

185. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.

186. Comment Letter from American Association for Justice, *supra* note 141.

187. Comment from Fresenius Kabi, *supra* note 180.

intrusions that steal patient data from millions of people.[188] An attacker using a pacemaker to kill a patient has gone from being a once clever plot in Hollywood fiction to something that is only a matter of time from happening. The guidance is non-binding on every stakeholder to which it applies.[189] The guidance urges collaboration, risk sharing, and risk management.[190] Lofty outcomes can only be accomplished by making the recommendations in the guidance requirements.[191] Nothing in the guidance places an undue burden on manufacturers of medical devices; it merely calls for cybersecurity risks to be effectively managed through a risk management program.[192] The FDA has been providing guidance to the medical device manufacturer community for nearly two decades related to cybersecurity.[193] Medical devices continue to be delivered to the market with either unsupported operating systems, no software maintenance plans in place, or a host of other vulnerabilities.[194] The FDA must go from making recommendations that manufacturers should follow to making standardized requirements if it wants to seriously protect patient safety and privacy.[195]

V. CONCLUSION

The FDA guidance as discussed is merely a draft.[196] However, based on the generally positive reception by the medical device industry, it is very likely that the draft will be adopted unchanged in the final guidance document.[197] The guidance proposes effective risk management ideas that should already be in use by manufacturers to prevent attackers exploiting cybersecurity vulnerabilities.[198] Attempting to protect, or anticipate and remedy every vulnerability a medical device may have now or in the future is unrealistic. A risk based approach allows manufacturers to adapt to threats that tend to adapt quicker than those tasked with guarding against them.[199] The guidance is a step in the right direction but should be faulted for the lack

188. *Id.*

189. U.S. FOOD & DRUG ADMIN., *supra* note 11; *see also* Comment from Rapid7, *supra* note 178.

190. U.S. FOOD & DRUG ADMIN., *supra* note 11.

191. *See* Comment from Rapid7, *supra* note 178.

192. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11.

193. *See id.*; Comment from Rapid7, *supra* note 178.

194. *See Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, *supra* note 5; *supra* Section II.B.

195. *See* Comment from Rapid7, *supra* note 178.

196. U.S. FOOD & DRUG ADMIN., *supra* note 11.

197. *See* Comment Letter from American Association for Justice, *supra* note 141; Comment from Fresenius Kabi, *supra* note 180; Comment from Rapid7, *supra* note 178.

198. *See supra* Section IV.A.

199. *See supra* Section IV.

of privacy considerations.[200] Patient health should be a priority alongside patient safety.[201] Essential clinical performance should include patient privacy.[202] Furthermore, the guidance suggests that ISAOs are critical to effective medical device cybersecurity, yet spends very little time fleshing out their vision on how exactly they will work and reassuring manufacturers that information about cybersecurity vulnerabilities will not be exploited by opportunists.[203] Finally, recommendations should turn into requirements.[204] Nothing in the guidance as proposed places an undue burden on manufacturers, nor does it stifle innovation.[205] The FDA has a track record of issuing guidance that is ignored by those towards whom the recommendations are directed.[206]

200. *See supra* Section IV.A.
201. *See supra* Section IV.A.
202. *See supra* Section IV.A.
203. *See supra* Section IV.B.
204. *See supra* Section IV.C.
205. *See* U.S. FOOD & DRUG ADMIN., *supra* note 11; *supra* Section IV.C.
206. *See* Comment Letter from American Association for Justice, *supra* note 141.