THE FDA MUST FORTIFY CYBERSECURITY STEWARDSHIP

-ANDREW HENNESSY-STRAHS, J.D., LL.M., RAC, MPH CANDIDATE

APRIL, 2019

I. INTRODUCTION

Cybersecurity is a growing concern and impacts many aspects of the FDA regulatory process. Additionally, the threat could dwarf conventional evaluations may underestimate the potential for harm. On November 25, 2018, for example, the International Consortium for Investigative Journalism (ICIJ) released a year-long investigative report, which identified 83,000 deaths and 1.7 million injuries linked to medical devices in the United States over the last decade.[1] Notably, the ICIJ also identified 500,000 explant surgeries over the same time period.[2] Of these explant surgeries, nearly 14,000 explant surgeries were attributable to a software vulnerability in Medtronic's SynchroMed pain pump.[3] The Food and Drug Administration (FDA) issued the class I recall specifically "because a software problem may cause unintended delivery of drugs during a priming bolus procedure, used to quickly deliver large dose of medication from the device to the patient's spine."[4] A life-threatening cybersecurity vulnerability of implantable cardiac devices made by Abbott (formerly St. Jude Medical), which could have allowed an unauthorized user to deplete the battery life of these devices, led to the

---

[1] International Consortium for Investigative Journalism (ICIJ), The Implant Files, Nov. 25, 2018, *available at* https://www.icij.org/investigations/implant-files/. The ICIJ compiled this report using more than 250 journalists and a machine learning algorithm developed by the ICIJ.
[2] Spencer Woodman, *Patients Fight for Answers as Broken Implants Cause Unseen Agony*, ICIJ, Nov. 27, 2018, *available at* https://www.icij.org/investigations/implant-files/patients-fight-for-answers-as-broken-implants-cause-unseen-agony/.
[3] U.S. Food & Drug Admin., Medtronic Recalls SynchroMed II and SynchroMed EL Implantable Drug Infusion Pumps Due to Failure of Priming Bolus – Update Related to May 2013 Recall, https://www.fda.gov/medicaldevices/safety/listofrecalls/ucm546558.htm (last updated Aug. 3, 2018).
[4] U.S. Food & Drug Admin., Medtronic Recalls SynchroMed II and SynchroMed EL Implantable Drug Infusion Pumps Due to Failure of Priming Bolus – Update Related to May 2013 Recall, https://www.fda.gov/medicaldevices/safety/listofrecalls/ucm546558.htm (last updated Aug. 3, 2018).

recalls of 700,000 devices, a portion of which have been explanted in response to the recalls.[5] While the threats in these devices also impact traditional areas of regulatory focus, such as software design and validation, there is no denying that cybersecurity vulnerability was part of the FDA's calculus in issuing some of these recalls (i.e., the concern about "unauthorized users" gaining access to the devices).

Moreover, the likelihood that a cybersecurity threat will recur is becoming increasingly predictable. In other words, it is not a question of if but when the next cyberattack will occur. Among the most notable attacks, in recent history, the 2017 WannaCry ransomware attack, which froze health care providers' access to patient records in the United Kingdom, cost the National Health Service £92 million in total (£20 million in costs from 19,000 cancelled appointments over a one week period, and £72 million in computer system cleanup and upgrades).[6]

Although the WannaCry attack primarily impacted the United Kingdom, there have been significant cyberattacks involving companies in the United States. In June of 2017, for example, all of Merck's U.S.-based offices were attacked with the "NotPetya" ransomware virus, which shut down Merck's laboratories.[7] Merck disclosed the severity of the attack to its shareholders in

---

[5] U.S. Food & Drug Admin., St. Jude Medical Recalls Implantable Cardioverter Defibrillators (ICD) and Cardiac Resynchronization Therapy Defibrillators (CRT-D) Due to Premature Battery Depletion, https://www.fda.gov/MedicalDevices/Safety/ListofRecalls/ucm526317.htm (recall initiated Oct. 10, 2016) (last updated Feb. 16, 2018); U.S. Food & Drug Admin., Battery Performance Alert and Cybersecurity Firmware Updates for Certain Abbott (formerly St. Jude Medical) Implantable Cardiac Devices: FDA Safety Communication, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm604706.htm (Apr. 17, 2018); Spencer Woodman, *Patients Fight for Answers as Broken Implants Cause Unseen Agony*, ICIJ, Nov. 27, 2018, *available at* https://www.icij.org/investigations/implant-files/patients-fight-for-answers-as-broken-implants-cause-unseen-agony/

[6] Matthew Field, *WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Canceled*, THE TELEGRAPH, Oct. 11, 2018, *available at* https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[7] Andy Greenberg, *The Untold Story of NotPetya, The Most Devastating Cyberattack in History*, WIRED, Aug. 22, *2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*; *But see,* Kim Nash, et al., *One Year After NotPetya CyberAttack, Firms Wrestle with Recovery Costs*, WALL STREET JOURNAL,

2018 - $870 million in losses (dwarfing the more notorious WannaCry attack).[8] The attack forced Merck to borrow Gardasil 9 vaccine doses from the Centers for Disease Control and Prevention stockpile and triggered a Congressional inquiry from the House Energy and Commerce Committee on Sept. 20, 2017, followed by a private briefing in October, 2017.[9]

The FDA is beginning to enhance its cybersecurity efforts but must go further. The FDA acknowledged the increasing cybersecurity threat in October of 2018:

> "The need for effective cybersecurity to assure medical device functionality and safety has become more important with the increasing use of wireless, internet- and network-connected devices, and the frequent electronic exchange of medical device-related health information. In addition, cybersecurity threats to the healthcare sector have become more frequent, more severe, and more clinically impactful. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the United States and globally. Such cyberattacks and exploits can delay diagnoses and/or treatment and may lead to patient harm."[10]

FDA Commissioner Scott Gottlieb and CDRH Director Jeff Shuren then released a joint statement on November 20, 2018, announcing the FDA's commitment to post-approval safety reform, as well as the administration's intention to fundamentally modernize the 510(k) approval process.[11] Cybersecurity is an emerging focus of the FDA, which must coordinate with other

---

Jun. 27, 2018, *available at* https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906 (reporting a lower estimate of a $670 million loss, two months earlier).

[8] *Id*.

[9] Kim Nash, et al., *One Year After NotPetya CyberAttack, Firms Wrestle with Recovery Costs*, WALL STREET JOURNAL, Jun. 27, 2018, *available at* https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.

[10] U.S. Food & Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (proposed Oct. 18, 2018), *available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf

[11] U.S. Food & Drug Admin., Statement from FDA Commissioner Scott Gottlieb, M.D. and Jeff Shuren, M.D., Director of the Center for Devices and Radiological Health, on FDA's updates to Medical Device Safety Action Plan to enhance post-market safety, https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm626286.htm (Nov. 20, 2018); Susan Scutti, *FDA Overhauls Approval Process as Medical Devices Come Under Fire*, CNN, https://www.cnn.com/2018/11/27/health/fda-medical-devices/index.html.

administrative agencies (both within the Department of Health and Human Services, and in other departments such as Homeland Security and The Department of Defense) to strengthen all aspects of its cybersecurity regulatory framework, requiring all types of FDA-regulated companies (pharmaceuticals, biologics, medical devices) to develop cybersecurity defense and mitigation efforts at all aspects of the regulatory process (preclinical development, clinical testing, post-approval).

II. HISTORICAL CONTEXT

Historically, the FDA has undergone reform in reaction to crises in order to better confront public health threats.[12] The 1962 Kefauver-Harris Drug Efficacy Amendment was a response to a narrowly averted thalidomide birth defect crisis, on account of the sagacity of Frances Kelsey to delay U.S. market approval for the drug.[13] Similarly, the seminal 1938 Food, Drug, and Cosmetic Act (FDCA) was a direct response to deaths of over 100 children (and the averted deaths of thousands more) after the children ingested an antibiotic elixir that had been manufactured with diethylene glycol, a lethal fluid, better known as antifreeze.[14] Given the increasing connectedness of the world, the corresponding vulnerability of all classes of FDA regulated products to cyberattacks, and that patient harm has already occurred, the FDA, in an abundance of shrewd foresight, must strengthen its approach to cybersecurity by strengthening its capacity to respond to cyberattacks, upgrading its cybersecurity recommendations from voluntary to mandatory, extending HIPAA data privacy protections to the entities it regulates,

---

[12] *See, e.g.*, U.S. Food & Drug Admin., *A History of Drug Regulation in the United States* (2006), available at https://www.fda.gov/downloads/drugs/resourcesforyou/consumers/buyingusingmedicinesafely/understandingover-the-countermedicines/ucm093550.pdf.

[13] Roberto McFadden, *Frances Oldham Kelsey, Who Saved U.S. Babies from Thalidomide, Dies at 101*, N.Y. TIMES, Aug. 7, 2015, *available at* https://www.nytimes.com/2015/08/08/science/frances-oldham-kelsey-fda-doctor-who-exposed-danger-of-thalidomide-dies-at-101.html.

[14] Carol Ballentine, *Sulfanilimide Disaster: Taste of Raspberries, Taste of Death: The 1937 Elixir Sulfanilamide Incident*, FDA CONSUMER MAGAZINE, June 1981, *available at* https://www.fda.gov/downloads/AboutFDA/WhatWeDo/History/ProductRegulation/UCM593517.pdf.

and requiring all regulated entities (not just medical device manufacturers) to implement state-of-the-art cybersecurity protections.[15]

The FDA does not explicitly mandate that companies implement cybersecurity measures; instead, the FDA gives broad interpretation to existing laws and regulations based on an approach originally developed in the 1990's. The FDA derives the legal authority to promulgate these regulations from §§201-903 (drugs and devices) of the FDCA and §351 of the Public Health Service Act (for biologics).[16] Specifically, after meeting with pharmaceutical companies in 1991 and convening the Task Force on Electronic Identification/Signatures, the culmination of which was the 1997 finalization of 21 C.F.R. § 11 et seq., which provided the FDA with the authority to require companies to ensure their electronic records comply with a minimum set of electronic recordkeeping standards.[17] The heart of the regulation as it pertains to cybersecurity for what the FDA then referred to as "closed systems" is as follows:

> "(1) System access be limited to authorized individuals; (2) operational system checks be used to enforce permitted sequencing of steps and events as appropriate; (3) authority checks be used to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform operations; (4) device (e.g., terminal) checks be used to determine the validity of the source of data input or operation instruction; and (5) written policies be established and adhered to holding individuals accountable and responsible for actions initiated under their electronic signatures, so as to deter record and signature falsification."[18]

[15] *See generally*, Mayra Rosario Fuentes, *Cybercrime and Other Threats Faced by the Healthcare Industry*, TRENDMICRO, (2017), *available at* https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-other-threats-faced-by-the-healthcare-industry.pdf (outlining the cybersecurity threats facing medical devices).
[16] Electronic Records; Electronic Signatures, 62 Fed. Reg. 13,464 (Mar. 20, 1997).
[17] *Id*.
[18] *Id.* at 13,430, elucidating regulations for closed systems

It is fair to say that the FDA's primary set of cybersecurity-related regulations derive from a 1991 Task Force.[19]

At the same time the FDA was considering strengthening electronic-recordkeeping regulations, Congress laid the groundwork for the increasing role cybersecurity would play in our lives. One year prior to the FDA's finalization of 21 C.F.R. § 11 et seq., Congress effectively decided to whom many of those electronic records belonged -- and the requisite level of protection those records warranted. The 104th Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which was signed into law by President Clinton on August 21, 1996.[20] The Department of Health and Human Services (DHHS) added the *privacy rule* in 2000, "which set national standards for when protected health information (PHI) may be used and disclosed."[21] However, as HIPAA defines it, the privacy rule only applies to covered entities and their associates (health plans, health care clearinghouses, health care providers), effectively exempting medical device and pharmaceutical manufacturers.[22] Three years later, the

[19] *See, e.g.*, Zenon, *Regulatory Compliance and Cyber Threats: Industrial Security in the Pharmaceutical Sector*, COPADATA (2016) at 4, *available at* http://www.samedanltd.com/uploads/pdf/white_paper/23ccbbdb4947fb9a6587a7fefe092aa8.pdf

> "The Food and Drug Administration (FDA) 21 CFR Part 11 is one of the most established regulations within the industry. The regulation requires organisations to implement controls, electronic audit trails and systems validations. It establishes the standard expectations for industrial security through reliable electronic documentation of the pharmaceutical manufacturing process."

[20] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[21] *Id.*; Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, codified at 45 C.F.R. Parts 160 and 164; CENTERS FOR MEDICARE & MEDICAID SERVICES, HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES (Sept. 2018), *available at* https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf; *See also,* HIPAA Journal, *Why is HIPAA Important to Patients?*, HIPAA J. (Mar. 8, 2018), *available at* https://www.hipaajournal.com/why-is-hipaa-important-patients/ (discussing significance of HIPAA and its amendments).

[22] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996). Applicability § 1172; 42 U.S.C. § 1320d-1

> "Sec. 1172. (a) Applicability.—Any standard adopted under this part shall apply, in whole or in part, to the following persons:
>
> (1) A health plan.
>
> (2) A health care clearinghouse.

DHHS added the *security rule*, "which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)."[23]

In 2005, the FDA published its first official cybersecurity guidance documents.[24] However, this guidance only pertained to medical devices that used off-the-shelf (OTS) software, a type of third-party software that the FDA had first considered in 1999 and defined as "a generally available software component, used by a medical device manufacturer for which the manufacturer can not claim complete software life cycle control."[25] The 2005 guidance took the approach that cybersecurity fell under the responsibilities manufacturers had under the Quality System Regulations (QSR) that required manufacturers of Class III and II (and named Class I devices, automated with computer software) to "establish and maintain procedures to control the design of the device in order to ensure that specified design requirements are met."[26] Specifically, the FDA advised device manufacturers to *validate* the design of software, which "requires that devices conform to defined user needs and intended uses," pursuant to the 1996 final updates to the Quality System Regulations under 21 C.F.R. § 820.30 (f).[27]

---

(3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1)."

See also Transactions by Plans§ 1175."

[23] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. Parts 160, 162, and 164).

[24] U.S. Food & Drug Admin, Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (Jan. 14, 2005), *available at* https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm077823.pdf.

[25] *Id.*; U.S. Food & Drug Admin, Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices (Sep. 9, 1999), *available at* https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm073779.pdf .

[26] U.S. Food & Drug Admin, Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software; 21 C.F.R. § 820.30 (a) .

[27] U.S. Food & Drug Admin, Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software; Quality System Regulation, 21 C.F.R. § 820.30 (a); Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule; Quality System Regulation, 61 Fed. Reg. 52,602 (Oct. 7, 1996).

Four years later, the 111th Congress accelerated the adoption of electronic health records, with the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH), which provided $35 billion in incentives to hospitals to replace paper recordkeeping systems with electronic systems.[28] The HITECH Act also mandated the adoption of improved privacy and security standards (including updated notification of breach standards under §13402 of the Act) and the authorization of criminal and civil penalties for violations of security provisions under the Social Security Act.[29] As directed by the HITECH Act, the DHHS added the *breach notification rule* to its HIPAA regulations, "which requires covered entities to notify affected individuals; [DHHS] and, in some cases, the media of a breach of unsecured PHI."[30] The HITECH act formally extended the privacy, security, and breach notification rules to the business associates of covered entities.[31] The FDA should explicitly extend the privacy protections afforded by HIPAA to entities falling under its regulatory jurisdiction, under the theory that these companies will necessarily associate with health care providers, who ultimately direct patients to procure drugs and devices ,and health plans. Such an interpretation would most

---

[28] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[29] Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 111-5, 123 Stat. 227 (2009), 42 U.S.C. §17931, "§13401 Application of Security Provisions and Penalties to Business Associates of Covered Entities; Annual Guidance on Security Provisions;" Social Security Act, subsection (a), §§1176, 1177, 42 U.S.C. §1320d–5, 1320d–6; *See, e.g.,* Julia Adler-Milstein and Ashish Jha, *HITECH Act Drove Large Gains in Hospital Electronic Health Record Adoption*, 36 HEALTH AFFAIRS, (finding that, for eligible hospitals, the HITECH Act caused an 11.1 percentage point annual increase, from 2011-2015, in the adoption of HER systems, following the implementation of meaningful use incentives of the HITECH Act).
[30] Breach Notification for Unsecured Protected Health Information 74 Fed. Reg. 42, 740 (Aug. 24, 2009) (codified at 45 C.F.R. Parts 160 and 164); Centers for Medicare & Medicaid Services, HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules (Sept. 2018), *available at* https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf; *See also,* HIPAA Journal, *Why is HIPAA Important to Patients?*, HIPAA J. (Mar. 8, 2018), *available at* https://www.hipaajournal.com/why-is-hipaa-important-patients/ (discussing significance of HIPAA and its amendments).
[31] HITECH Act, 42 U.S.C. § 17,931

likely satisfy Chevron deference for the permissible scope of an agency's regulatory authority, subject to the King v. Burwell unsettled "economic and political significance" standard.[32]

III. The FDA's Current Approach

As the FDA currently defines it, *cybersecurity* "is the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient."[33] Cybersecurity entails protecting *cyber* -- "of, relating to, or involving computers or computer networks (such as the Internet)" -- *assets* -- "anything that has value to an individual or an organization") -- from *threats* to the confidentiality, integrity, and accessibility of that data, as well as ensuring software and hardware do not have unacceptable *vulnerabilities* that could entice malfeasants to exploit those weaknesses.[34] Should a cybersecurity breach occur, the FDA expects the responsible companies to have mitigation plans to detect, respond, and recover from that breach.[35] However,

---

[32] Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984); King v. Burwell, 576 U.S. __ (2015)

> "(a) When analyzing an agency's interpretation of a statute, this Court often applies the two-step framework announced in Chevron, 467 U. S. 837. But Chevron does not provide the appropriate frame- work here. The tax credits are one of the Act's key reforms and whether they are available on Federal Exchanges is a question of deep "economic and political significance"; had Congress wished to assign that question to an agency, it surely would have done so expressly. And it is especially unlikely that Congress would have dele- gated this decision to the IRS, which has no expertise in crafting health insurance policy of this sort."

[33] *Id.*; 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), *available at* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

[34] U.S. Food & Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (proposed Oct. 18, 2018), *available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf; 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), *available at* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf; *Cyber*, Merriam-Webster, https://www.merriam-webster.com/dictionary/cyber (last updated Dec. 3, 2013).

[35] *See generally*, U.S. Food & Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (proposed Oct. 18, 2018), *available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf (discussing cybersecurity threats to medical devices).

these recommendations only pertain to medical devices and the associated software. Notably, any product regulated by the FDA that depends upon a computer at any point in its lifecycle is vulnerable to a cyberattack, as "[t]he default assumption is that everything is vulnerable."[36]

The genesis of the FDA'S current cybersecurity framework began in 2014, when the FDA introduced premarket cybersecurity guidance that broadened the scope of its 2005 guidance to now cover the premarket submissions of class II and III devices that contain "software (including firmware) or programmable logic."[37] The FDA also extended this guidance to software that, itself, "is a medical device," which -- significantly -- would include mobile apps.[38] The FDA reiterated its approach to extending the 21 C.F.R.§ 820.30 QSR validation regulations to cybersecurity validation, but issued mere velleities that manufacturers take additional steps to

---

[36] Why Everything Is Hackable: Computer Security Is Broken from Top to Bottom, THE ECONOMIST, Apr. 8, 2017, *available at* https://www.economist.com/science-and-technology/2017/04/08/computer-security-is-broken-from-top-to-bottom (quoting Robert Watson).

[37] 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, at 2 (Oct. 2, 2014), *available at* https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf. The types of premarket submissions are as follows:

> "•Premarket Notification (510(k)) including Traditional, Special, and Abbreviated
> •De novo submissions
> •Premarket Approval Applications (PMA)
> •Product Development Protocols (PDP)
> •Humanitarian Device Exemption (HDE) submissions."

[38] *Id.* For the definition of software as a medical device as used by the FDA, *see* U.S. Food & Drug Admin., Software as a Medical Device (SaMD) (last updated Nov. 19, 2018); *See also*, Int'l Med. Device Regulators Forum, Software as a Medical Device (SaMD): Key Definitions (Dec. 9, 2013), at 6:

> "The term "Software as a Medical Device" (SaMD) is defined as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device.
> NOTES:
> • SaMD is a medical device and includes in-vitro diagnostic (IVD) medical device.
> • SaMD is capable of running on general purpose (non-medical purpose) computing platforms3
> • "without being part of" means software not necessary for a hardware medical device to achieve its intended medical purpose;
> • Software does not meet the definition of SaMD if its intended purpose is to drive a hardware medical
> device.
> • SaMD may be used in combination (e.g., as a module) with other products including medical devices;
> • SaMD may be interfaced with other medical devices, including hardware medical devices and other SaMD software, as well as general purpose software
> • Mobile apps that meet the definition above are considered SaMD."

validate the design of their software.[39] The FDA articulated a 5-part cybersecurity core function framework to guide the QSR validation steps taken by medical device manufacturers to: identify, protect against, detect, respond to, and recover from security compromises.[40]

Of course, the FDA is just one administrative agency in a coalition of health, justice, and military administrative bodies that are responsible for cybersecurity in the United States. On December 18, 2015, President Obama and the 114th U.S. Congress extended HIPAA cybersecurity provisions to the FDA through passage of the Cybersecurity Information Sharing Act and directed the FDA to collaborate with other government stakeholders including, the Department of Homeland Security (DHS):

> "§1533. Improving ***cybersecurity*** in the health care industry
> (a)Definitions
> . . .
> (6) Health care industry stakeholder
> . . .
> (F) ***Pharmaceutical*** or ***Medical Device Manufacturer***
> . . .
> (d) Aligning health care industry security approaches
> . . .
> The Secretary shall establish, through a collaborative process with the Secretary of ***Homeland Security***, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes.
> (ii) the security and privacy regulations promulgated under section 264(c) of the ***Health Insurance Portability and Accountability Act of 1996***."[41]

---

[39] *Id.* at 4.
"Manufacturers should address cybersecurity during the design and development of the medical device, as this can result in more robust and efficient mitigation of patient risks. Manufacturers should establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g).
• Identification of assets, threats, and vulnerabilities;
• Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
• Assessment of the likelihood of a threat and of a vulnerability being exploited;
• Determination of risk levels and suitable mitigation strategies;
• Assessment of residual risk and risk acceptance criteria."

[40] *Id.* at 6.

One month and four days later, the FDA finalized its nonbinding postmarket cybersecurity recommendations, advising device manufacturers when to report cybersecurity modifications under 21 C.F.R. § 806.[42] The FDA again advised manufacturers that cybersecurity falls under the 21 C.F.R. § 820.30 QSR regulations.[43] Relying upon two cybersecurity executive orders from the Obama administration, the FDA encouraged medical device manufacturers to adopt a risk management approach, to implement the voluntary "Framework for Improving Critical Infrastructure - Cybersecurity," and to participate in Information Sharing and Analysis Organizations (ISAO's), which are organizations that aggregate and disseminate cybersecurity vulnerabilities to manufacturers, so that they can respond accordingly.[44]

Given the shifting cybersecurity landscape post-2014, the FDA published draft guidance on October 18, 2018 to replace its 2014 premarket submission guidance for medical devices.[45] This guidance proposed adopting a two-tiered risk classification system, consistent with the new NIST standards for medical devices, with tier one being connected devices that are vulnerable to cyberattacks that could impact multiple patients and tier two devices being a catch-all for other

---

[41] 6 U.S.C. § 1533 (2015); Cybersecurity Information Sharing Act, Pub. L. 114-113 (2015); 15 U.S.C. § 272 (2014), subject to cybersecurity standards developed by the National Institute of Standards and Technology (NIST), through the Cybersecurity Enhancement Act, Pub. L. No. 113-274, 123 Stat. 2971 (2014):
(ii) the security and privacy regulations promulgated under section 264(c) of the ***Health Insurance Portability and Accountability Act of 1996***" (emphasis added).
[42] Medical Devices; Reports of Corrections and Removals, 21 C.F.R. § 806 (rev. Apr. 1, 2018); U.S. Food & Drug Admin., Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (2016), *available at* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.
[43] U.S. Food & Drug Admin., Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (2016); 21 C.F.R. § 820.30.
[44] *Id.*, *citing* Exec. Order No. 13,636 (Feb. 12, 2013); Exec. Order No. 13,691, 3 C.F.R. § 13,691 (Feb. 3, 2015).
[45] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, 83 Fed. Reg. 52,835 (proposed Oct. 18, 2018); U.S. Food & Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (proposed Oct. 18, 2018), *available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf; 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), *available at* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

devices.[46] The FDA recommended that manufacturers steward their supply chains by implementing a cyber bill of materials to validate suppliers under the FDA's purchasing control device regulations at 21 C.F.R. § 820.50; the FDA also indicated that it may use labeling regulations to require manufacturers to strengthen cybersecurity to ensure their devices are still faithful to claims of safety.[47] Even so, on October 29, 2018, the Office of Inspector General (OIG) for the (DHHS) released the results of an FDA cybersecurity audit, advising the FDA that its efforts to buttress cybersecurity fell short.[48] The OIG made four recommendations to the FDA in the context of medical devices: (1) monitor cybersecurity risks and respond with strategic adjustments; (2) write protocols for dissemination of information about cybersecurity

---

[46] Cybersecurity Information Sharing Act *supra* note 38, (applying NIST standards); 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) at 10.

> "Tier 1 'Higher Cybersecurity Risk'
>
> A device is a Tier 1 device if the following criteria are met:
>
> 1) The device is capable of connecting (e.g., wired, wirelessly) to another medical of non-medical product, or to a network, or to the Internet; AND
> 2) A cybersecurity incident affecting the device could directly result in patient harm to multiple patients.
>
> Examples of Tier 1 devices, include but are not limited to, implantable cardioverter defibrillators (ICDs), pacemakers, left ventricular assist devices (LVADs), brain stimulators and neurostimulators, dialysis devices, infusion and insulin pumps, and the supporting connected systems that interact with these devices such as home monitors and those with command and control functionality such as programmers.
>
> Tier 2 'Standard Cybersecurity Risk'
>
> A medical device for which the criteria for a Tier 1 device are not met."

[47] Purchasing controls 21 C.F.R. § 820.50 (Dec. 2018); Failure to Reveal Material Facts 21 C.F.R. §1.21 (Dec. 2018); Labeling 21 C.F.R. § 801 (Dec. 2018).

[48] U.S. Dep't Of Health and Human Services, Office for the Inspector General, The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices: Full Report (Oct. 29, 2018), *available at* https://oig.hhs.gov/oas/reports/region18/181630530.pdf; U.S. Dep't Of Health and Human Services, Office for the Inspector General, The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices: Report in Brief (Oct. 29, 2018), *available at* https://oig.hhs.gov/oas/reports/region18/181630530RIB.pdf; U.S. Dep't Of Health and Human Services, Office for the Inspector General, The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices (Oct. 29, 2018), *available at* https://oig.hhs.gov/oas/reports/region18/181630530.asp

> "FDA agreed with our recommendations and said it had already implemented many of them during the audit and would continue working to implement the recommendations in the report. However, FDA disagreed with our conclusions that it had not assessed medical device cybersecurity at an enterprise or component level and that its preexisting policies and procedures were insufficient. We appreciate the efforts FDA has taken and plans to take in response to our findings and recommendations, but we maintain that our findings and recommendations are valid."

events for key stakeholders; (3) formalize a cybersecurity partnership with the DHS; and (4) establish recall protocols for medical devices that lack sufficient cyber-security.[49] The FDA should strenuously and comprehensively implement all four of the OIG's recommendations. The FDA's jury-rigged cybersecurity framework (the QSR validation approach, along with the FDA's unpersuasive threats to use labeling and purchasing regulations) is insufficient to rectify the harms of a cybersecurity event: "because [the] FDA had not sufficiently assessed the risks of medical device cybersecurity events, existing policies and procedures did not include effective practices for responding to those events."[50] The FDA's voluntary recommendation for medical device manufacturers to enter into information sharing partnerships with ISAO's is also not strong enough; this intervention is likely to have a high cost-benefit ratio, and, as such, should be made mandatory, and extended to all classes of FDA regulated products.[51] The promised cooperation with the DHS further leaves something to be desired as it simply "formalizes and enhances" an existing relationship and recommends that the FDA and the DHS' National Protection and Programs Directorate (NPPD) "should collaborate . . . but not in a capacity that interferes with any other roles and responsibilities of the parties" to form standard operating procedures to share information.[52]

[49] *Id.*
[50] U.S. Dep't Of Health and Human Services, Office for the Inspector General, The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices, at 7; Purchasing controls 21 C.F.R. § 820.50 (Dec. 2018); Failure to Reveal Material Facts 21 C.F.R. §1.21 (Dec. 2018); Labeling 21 C.F.R. § 801 (Dec. 2018); U.S. Food & Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (proposed Oct. 18, 2018).
[51] *See, e.g.,* AT&T, *Tackling Cybersecurity Head-On in Texas*, GOVTECH, May 30, 2018, *available at* http://www.govtech.com/pcio/articles/Tackling-Cybersecurity-Head-On-in-Texas.html, reporting on cost-effective cybersecurity interventions recently enacted in Texas, including ISAO involvement.
[52] Department of Homeland Security, U.S. Food & Drug Admin., Memorandum of Agreement Between The Department of Homeland Security, National Protection and Programs Directorate And The Department of Health and Human Services, Food and Drug Administration, Relating to Medical Device Cybersecurity Collaboration at 1,3 (signed by all parties on Oct. 15, 2018); *See also,* Ana Mulero, *Cybersecurity: FDA Spells Out Updated Premarket* Policies, Oct. 17, 2018, which categorizes agreement as "merely" formalizing existing agreement between the two agencies.

Self-interest should also motivate pharmaceutical companies to implement the highest caliber cybersecurity protections possible, as the value and scope of their intellectual property (from copyrighted data sets and computer algorithms to clinical trial notebooks, production process trade secrets, and unpublished patent filings) form the lifeblood of their organizations.[53] From the FDA's perspective, as an organization entrusted with protecting the public, the FDA should unequivocally extend cybersecurity obligations to pharmaceutical companies because the theft, destruction, or dissemination of intellectual property (by a hacker, competitor, or disgruntled employee) could jeopardize public safety (e.g., by interfering with the development of new drugs or facilitating the introduction of counterfeit drugs into U.S. commerce).

Additionally, by focusing on the performance reliability of medical devices in its 2018 guidance, the FDA fails to meaningfully address another common form of cyberattack, which does not compromise functionality per se, but instead seeks patient's ePHI. In this common cyberattack, a cybercriminal circumvents privacy restrictions to gain access to electronic data in medical records (valuable because it can allow unfettered access to open new financial accounts, to deplete existing financial accounts/lines of credit, and to procure medical services) and either uses the data him/herself or resells it on the secondary market.[54] So long as these data do not compromise the functionality of a medical device (i.e., its safety and efficacy), the FDA would have no regulatory opportunity to compel action by a device manufacturer. Because the HIPAA privacy rule covers only health care providers, health plans, and health care clearinghouses, there is effectively no substantive regulatory or legal obligation for pharmaceutical companies or

---

[53] *See*, Guidebook: Cybersecurity in the Pharma, Biotech, and Medical Devices Industries, FOLEY & LARDNER, LLP, Apr. 3, 2017, *available at* https://www.lexology.com/library/detail.aspx?g=70004fd3-f3cf-456d-8510-fba65d00e32f (prepared by Michael C. Sweeney, J.D.), discussing types of intellectual property vulnerable to a cyberattack.

[54] *See generally*, Mayra Rosario Fuentes, *Cybercrime and Other Threats Faced by the Healthcare Industry*, TRENDMICRO, (2017), *available at* https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-other-threats-faced-by-the-healthcare-industry.pdf (outlining the cybersecurity threats facing medical devices).

medical device manufacturers to ensure that patient data cannot be breached.[55] A search of the breaches and sanctions reported by the Office of Civil Rights for the DHHS confirms this regulatory gap and does not return any cases involving FDA regulated products.[56]

IV. Conclusion

In light of the reports of cyberattacks and abrogation of medical device regulatory stewardship, the FDA must coordinate with other administrative agencies (Department of Health and Human Services, Department of Homeland Security, Department of Defense), and require all classes of FDA-regulated companies to develop cybersecurity defense and mitigation efforts at all aspects of the regulatory process (preclinical development, clinical testing, postapproval). Moreover, in order to prevent a data breach, the FDA should require all classes of FDA-regulated companies to strengthen HIPAA data privacy protections.[57] The FDA has an opportunity – one, which it must take – to strengthen its regulatory approach to avoid a significant cyberattack.

[55] *See* HIPAA, *supra* note 23, listing the covered entities subject to compliance with the privacy rule.

[56] Office for Civil Rights, DHHS, Breach Portal Search Engine, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[57] *See generally*, International Consortium for Investigative Journalism (ICIJ), The Implant Files, Nov. 25, 2018, *available at* https://www.icij.org/investigations/implant-files/ and Spencer Woodman, *Patients Fight for Answers as Broken Implants Cause Unseen Agony*, ICIJ, Nov. 27, 2018, *available at* https://www.icij.org/investigations/implant-files/patients-fight-for-answers-as-broken-implants-cause-unseen-agony/; U.S. Food & Drug Admin., St. Jude Medical Recalls Implantable Cardioverter Defibrillators (ICD) and Cardiac Resynchronization Therapy Defibrillators (CRT-D) Due to Premature Battery Depletion, https://www.fda.gov/MedicalDevices/Safety/ListofRecalls/ucm526317.htm (recall initiated Oct. 10, 2016) (last updated Feb. 16, 2018); U.S. Food & Drug Admin., Battery Performance Alert and Cybersecurity Firmware Updates for Certain Abbott (formerly St. Jude Medical) Implantable Cardiac Devices: FDA Safety Communication, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm604706.htm (Apr. 17, 2018) (discussing medical device regulation gaps and cybersecurity vulnerabilities in medical devices).