Annals of Health Law

Volume 26
Issue 1 *Winter 2017*

Article 3

2017

Enhancing Cybersecurity for the Digital Health Marketplace

Charlotte A. Tschider

Recommended Citation

Charlotte A. Tschider *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 Annals Health L. 1 (2017).
Available at: https://lawecommons.luc.edu/annals/vol26/iss1/3

Enhancing Cybersecurity for the Digital Health Marketplace

Charlotte A. Tschider*

`Tis your own safety that is at stake, when your neighbour˘s wall is in flames, and fires neglected are wont to gather strength._ ¯ Horace[1]

INTRODUCTION

The global digital health market has grown exponentially in the past five years, fueled by Internet of Things (IoT) development, increased mobile device adoption, and Big Data investment.[2] Historically, the medical device industry focused on device implants and direct therapies, but future medical technologies also leverage network connectivity and data aggregation, necessitating comprehensive cybersecurity activities to protect consumers.[3]

Market leaders in digital health have recently invested heavily in technologies that simultaneously improve patient connectedness and convenience, yet increase the probability of cybersecurity threats

* Charlotte A. Tschider is an Affiliated Professor with the Mitchell Hamline School of Law˘s Cybersecurity and Privacy Law Program. She is also Owner/Principal for a cybersecurity and privacy consulting firm, Cybersimple Security, and a Board Member for the International Association of Privacy Professionals (IAPP) Training Advisory Board. Tschider writes on a variety of topics relating to the intersection of law and technology, including privacy and cybersecurity. She holds a B.S. and M.A. in Rhetoric and Scientific and Technical Communication from the University of Minnesota, and a J.D. from the Hamline University School of Law.

[1] Q. HORATIUS FLACCUS, EPISTULAE, Bk. 1, Ep. 8 in HORACE: SATIRES, EPISTLES AND ARS POETICA (H. RUSHTON FAIRCLOUGH, ED. TRANS., HARVARD UNIV. PRESS REV. ED. 1929) (c. 35 B.C.E.), http://www.archive.org/stream/satiresepistlesa00horauoft/satiresepistlesa00horauoft_djvu.txt.

[2] Bill Chamberlin & Ed Gretz, Internet of Things: Small IoT Projects Pay the Way for Future Transformation, BLUEMINE: HORIZONWATCH (Mar. 6, 2016), http://www.slideshare.net/HorizonWatching/internet-of-things-trends-to-watch-in-2016; see also Valerie Jennings, Denver and Kansas City-Based Custom Software Development Firm, Twentyseven Global, Discusses Digital Health Industry Developments, TWENTYSEVEN GLOBAL (Feb. 3, 2016), http://www.27global.com/denver-and-kansas-city-based-custom-software-development-firm-twentyseven-global-discusses-digital-health-industry-developments/.

[3] Mathias Cousin, Tadashi Castillo-Hi, & Glenn Snyder, Devices and Diseases: How the IoT is Transforming Medtech, DELOITTE UNIV. PRESS (Sept. 11, 2015), http://dupress.com/articles/internet-of-things-iot-in-medical-devices-industry/.

compromising system vulnerabilities.[4] While digital health technologies offer several benefits to patients and healthcare providers, connected technologies attract new threats, potentially resulting in both health data loss and compromise of patient physical safety.[5] The combination of technology connectivity with increasingly common third party involvement via the cloud, Software as a Service (SaaS), and big data, multiplies the probability of harm, due to the presence of high-volume data sets for multiple customers, often connected over the public Internet or home networks with unknown settings.[6]

The cybersecurity community, and increasingly, federal agencies, have recognized the inherent risks of connected devices both broadly within the IoT and for wirelessly connected medical devices.[7] In 2012, as both the Office for Civil Rights (OCR) was developing its Health Insurance Portability and Accountability Act (HIPAA) audit methodology and the Federal Trade Commission (FTC) was developing cybersecurity guidelines, the Government Accountability Office (GAO) called on the U.S. Food and Drug Administration (FDA) to develop a plan to address medical device security risk.[8]

[4] Sonali P. Gunawardhana, The Impact of Cybersecurity Vulnerabilities on Mobile Medical App Development, Med. Device Online (Dec. 4, 2015), http://www.meddeviceonline.com/doc/the-impact-of-cybersecurity-vulnerabilities-on-mobile-medical-applications-0001.

[5] CGI, Cyberprivacy and Cybersecurity for Health Data 1 (2015), https://www.cgi.com/sites/default/files/white-papers/cgi-cybersecurity-for-health-data-white-paper.pdf.

[6] See generally Kimberly Crossland, 5 Big Privacy Problems that Come with Big Data, Techopedia (Jan. 29, 2014), https://www.techopedia.com/2/29682/trends/big-data/5-big-privacy-problems-that-come-with-big-data; see also Colin Wood, The Importance of Cybersecurity in the Age of the Cloud and Internet of Things, Gov˘t Tech. (Oct. 2, 2014), http://www.govtech.com/security/The-Importance-of-Cybersecurity-in-the-Age-of-the-Cloud-and-Internet-of-Things.html (explaining that Software as a Service, or SaaS, is a cloud service involving access to a Web-based application); see also Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS, Rackspace (2016), https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/ (juxtaposing the methodology and applicability of cloud services SaaS, Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)).

[7] See generally Gib Sorebo, Managing the Unmanageable: A Risk Model for the Internet of Things, RSA Conf. 2015 (Apr. 2015), https://www.rsaconference.com/writable/presentations/file_upload/grc-r01-managing-the-unmanageable-a-risk-model-or-the-internet-of-things.pdf; see U.S. Fed. Trade Comm˘n, Internet of Things: Privacy & Security in a Connected World 10 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter FTC]; see also U.S. Food & Drug Admin. Ctr. for Devices & Radiological Health, Postmarket Management of Cybersecurity in Med. Devices: Draft Guidance for Industry 4 (Jan. 22, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf (addressing the risks of data compromise inherent in medical device remediation).

[8] See generally U.S. Gov˘t Accountability Off., GAO-12-816, Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of

Since 2012, much has changed. Developments in consumer-facing IoT technologies combined with organizational foci on medical cost reduction and value-based health care have driven development of medical device applications and equipment that are network-aware.[9] Although an Internet connection alone does not increase risk criticality, network-aware devices dramatically increase exposure to a wide variety of globally dispersed threat vectors.[10] Largely because of the highly complex and multi-faceted nature of cybersecurity risk, the digital health regulatory landscape has become equally complex and, in some respects, incomplete for organizations not subject to HIPAA.[11]

This paper aims to demystify the science of cybersecurity and propose a common-sense approach to improve clarity for organizations developing medical device products for the digital health industry. In Part I, this Author describes the existing context for regulatory activity and the conditions precipitating increased risk. Part II describes in detail duplicative and frequently incomplete coverage within the existing regulatory framework regulated by the FDA and the OCR. In Part III, this Author proposes an adapted FDA regulatory framework to simplify and clarify regulation of the digital health marketplace.

PART I: SIGNIFICANT DIGITAL HEALTH GROWTH, CYBERSECURITY RISK

The United States spends nearly eighteen percent of its Gross Domestic Product (GDP) on healthcare each year, which is expected to rise to 20.1 percent by 2025.[12] Organizations investing in digital health have forecasted

DEVICES (Aug. 31, 2012), http://www.gao.gov/assets/650/647767.pdf.

[9] John Glaser, How the Internet of Things Will Affect Health Care, HOSP. & HEALTH NETWORKS (June 4, 2015), http://www.hhnmag.com/articles/3438-how-the-internet-of-things-will-affect-health-care.

[10] Networked Medical Devices: Security and Privacy Threats, SYMANTEC 7 (2011), https://www.symantec.com/content/en/us/enterprise/white_papers/b-networked_medical_devices_WP_21177186.en-us.pdf; see Cybersecurity of Network-Connected Medical Devices in the Netherlands, DELOITTE 1 (2015), http://www2.deloitte.com/content/dam/Deloitte/nl/Documents/public-sector/deloitte-nl-risk-cybersecurity-of-network-connected-medical-devices-in-the-netherlands.pdf (A `threat vector_ is a combination of a threat; or a person or event causing an impact to data confidentiality, integrity, or availability; with the steps used to leverage vulnerabilities and compromise a target, such as using a malicious file, SQL injection, or other method for gaining access to, or owning, a system).

[11] U.S. DEP`T HEALTH & HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 29 (July 17, 2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

[12] NHE Fact Sheet, CTRS. FOR MEDICARE & MEDICAID SERVS. (Aug. 10, 2016), https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/nhe-fact-sheet.html.

significant growth potential in digital health technologies, with venture capital firms investing $4.5 billion in 2015 and healthcare providers netting a projected $305 billion in savings from $32.4 billion spent on digital health investments.[13] Research firms approximate the health app market alone to reach $26 million.[14] Technology developments and increased pressure to develop low-cost care solutions have incentivized organizations to develop connected digital health products.[15] With sixty-four percent of American adults using mobile devices, the options for delivering health care or improving health overall have spurred significant growth in the digital health industry.[16] By September 2015, organizations had released 165,000 mobile health apps, with twenty-two percent related to medication reminders and information, women˜s health and pregnancy, and disease-specific treatment.[17]

A. Digital Health Technology

Although not defined in statute, `digital health,_ as adopted by the FDA, includes mobile health (`mHealth_), health information technology (IT), wearable devices, telehealth, telemedicine, and personalized medicine.[18] By

[13] Theresa Wang et al., Digital Health Funding: 2015 Year in Review, ROCK HEALTH (2015), https://rockhealth.com/reports/digital-health-funding-2015-year-in-review (last visited Oct. 13, 2016) (Venture funding had increased 115 percent between 2013 and 2014); see also Corey Stern, Goldman Sachs Says a Digital Healthcare Revolution is Coming´ and it Could Save America $300 billion, BUSINESS INSIDER (Jun. 29, 2015), http://www.businessinsider.com/goldman-digital-healthcare-is-coming-2015-6 (summarizing the projection reports of digital health savings); see also Michael D. Beauvais et al., Digital Health Pulse: Regulatory and Transactional Developments, LEXOLOGY (Aug. 16, 2016), http://www.lexology.com/library/detail.aspx?g=b22306c3-b081-4046-86e7-3e2f64d0427d (anticipating a unique regulatory framework for digital health oversight).

[14] MIT TECH. REV., Mobile Medical Apps: A Market on the Move (Nov. 18, 2014), https://www.technologyreview.com/s/532661/mobile-medical-apps-a-market-on-the-move/. Research activity also predicts future investment; see, e.g., John E. Ferguson & A. David Redish, Wireless Communication with Implanted Medical Devices Using the Conductive Properties of the Body, 8 EXPERT REV. MED. DEVICES 427, 433 (Jul. 2011); see also Ashraf Darwish & Aboul Ella Hassanien, Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring, 11 SENSORS 5561, 5562 (2011) (describing one such digital health investment in wireless sensor network technologies).

[15] Accelerating the Adoption of Connected Health, DELOITTE 2 (2015), http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-dchs-connected-health.pdf.

[16] Aaron Smith, Chapter One: A Portrait of Smartphone Ownership, PEW RESEARCH CTR. 2 (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/chapter-one-a-portrait-of-smartphone-ownership/.

[17] Patient Adoption of mHealth, IMS INST. FOR HEALTHCARE INFORMATICS 4 (Sept. 2015), http://www.imshealth.com/files/web/IMSH%20Institute/Reports/Patient%20Adoption%20of%20mHealth/IIHI_Patient_Adoption_of_mHealth.pdf (discussing that disease-specific apps constituted nine percent of all apps, or 14,850 apps in total).

[18] Digital Health, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/

means of example, sensor technologies, which physicians use for a variety of purposes in medical care, have the opportunity to be implanted and connected to external devices, improving real time monitoring as a patient continues in her daily life.[19] In order to remotely monitor patients, sensors transfer a large volume of health data and identifiable health information via the open Web, potentially increasing the data˘s exposure to misuse.[20]

It is critical to understand which technologies the digital health marketplace includes in order to determine appropriate recommendations for protecting patients and consumers. Practically speaking, digital health medical devices can be grouped by technological characteristics and type of implementation (See Table 1).[21] Implanted devices may be network-aware or not, such as an implanted device that is controlled remotely or continuously sends health data to another system versus a device that is calibrated prior to implantation.[22] Implanted devices can also include manufacturer-operated applications (such as a mobile app or a Web-based app) and data storage (such as a database).[23]

Non-implanted devices, by contrast, may aid in performing a medical procedure or diagnostics, but do not pervasively interact with the body. Non-implanted devices may include only the device used to perform a procedure, or devices can be connected to an information system that contains software to collect personal information about a patient and the procedure.[24] Devices with software can be configured as network-aware and may transfer data to a hospital data center or to a manufacturer˘s data center or cloud provider.[25]

Wearables receive information from an individual and provide

DigitalHealth/default.htm (last updated Aug. 30, 2016) [hereinafter Digital Health].

[19] Ashraf Darwish, The Impact of Implantable Sensors in Medical Applications, 2 AUSTIN J. BIOSENSORS & BIOELECTRONICS 1016, 1016 (2016), http://austinpublishinggroup.com/biosensors-bioelectronics/download.php?file=fulltext/ajbb-v2-id1016.pdf.

[20] Gunawardhana, supra note 4 (explaining that when data is exposed to the Internet, absent cybersecurity controls, outside parties could change data, resulting in inaccurate treatment, or hackers could steal data, such as identifiable personal information, and use it for healthcare fraud).

[21] See generally Digital Health, supra note 18.

[22] Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm (last updated Oct. 9, 2014).

[23] E.T. van der Velde et al., Integration of Data from Remote Monitoring Systems and Programmers into the Hospital Electronic Health Record System Based on International Standards, 20 NETH. HEART J. 66, 68 (Jan. 10, 2012).

[24] CLAUDIO BECCHETTI & ALESSANDRO NERI, MEDICAL INSTRUMENT DESIGN AND DEVELOPMENT: FROM REQUIREMENTS TO MARKET PLACEMENTS 20 (2013), http://media.wiley.com/product_data/excerpt/09/11199524/1119952409-31.pdf.

[25] MELISA BOCKRATH, MEDICAL DEVICES BEGIN TO DRIFT INTO CLOUD, KELLY SERVICES 8 (ebook), http://www.kellyocg.com/uploadedFiles/Content/Knowledge/Ebooks/Medical%20Devices%20Begin%20to%20Drift%20Into%20Cloud.pdf.

information from a device to a recipient, such as a caregiver or healthcare provider, but often do not deliver any physiological change to the body (i.e. cause cardiac muscle to contract).[26] Wearables include devices like the Fitbit, which measures heartrate, exercise, and sleep data, combining information an individual enters and information gathered simply by being worn.[27] Wearables usually connect to an external mobile device via a wireless network or other communication protocol like Bluetooth to transmit data to a mobile application, an `app._[28] Mobile apps can receive data from an implanted device, non-implanted device, or wearable, and can store data either on the device (thick client) or immediately send data to another location (thin client).[29] Similar to mobile devices, organizations often design Web applications to facilitate medical consultations (telehealth or remote doctor visits), gather personal information, or provide treatment recommendations based on information gathered from an online Web form.[30]

Finally, general administrative IT software or Web applications provide support to health-related operations.[31] This might include scheduling software, time reporting and HR management, patient intake, or overall storage of medical records.[32]

Although all devices could pose some risk to patients or consumers, devices with the highest inherent risk of harm include implanted or affixed devices.[33] These devices may directly deliver medication or other stimulus to the human body or gather biological health information directly.[34] When combined with wearables, mobile apps, or Web applications that are exposed

[26] Tyler Hayes, What˜s Inside a Fitness Tracker, Anyway?, Digital Trends (Nov. 29, 2014, 1:00 PM), http://www.digitaltrends.com/wearables/whats-inside-fitness-trackeanyway/.

[27] Heather Landi, Health Systems Collaborating with Fitbit to Use Connected Health Technologies for Research and Patient Engagement, Healthcare Informatics (July 29, 2016), http://www.healthcare-informatics.com/news-item/patient-engagement/health-systems-collaborating-fitbit-use-connected-health-technologies.

[28] See generally FTC, supra note 7.

[29] Id.; see Vangie Beal, The Differences Between Thick, Thin & Smart Clients, Webopedia (July 14, 2006), http://www.webopedia.com/DidYouKnow/Hardware_Software/thin_client_applications.asp (distinguishing between thick and thin client applications and users).

[30] See Nat˜l Research Council, U.S. Comm. on Enhancing the Internet for Health Applications, Networking Health: Prescriptions for the Internet 194¯95 (2000), http://www.ncbi.nlm.nih.gov/books/NBK44714/.

[31] The 20 Most Popular EMR Software Solutions, Capterra, http://www.capterra.com/infographics/top-emr-software (last visited Oct. 13, 2016).

[32] Top Electronic Medical Records (EMR) Software Products, Capterra, http://www.capterra.com/electronic-medical-records-software/ (last visited Oct. 13, 2016).

[33] Food and Drug Administration Safety and Innovation Act í 618, infra 124; General Wellness, infra 144.

[34] Implants and Prosthetics, U.S. Food & Drug Admin., http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ImplantsandProsthetics/ (last visited Oct. 13, 2016).

to the open Internet, the potential risks of physical injury or substantial data loss increase.[35] For these reasons, the FDA publicly announced both in 2015 and 2016 its intention to focus attention on high risk digital health medical devices, rather than all health-related mobile apps.[36]

B. Cybersecurity Risks ¯ Threats and Vulnerabilities for Digital Health Products

Cybersecurity is defined as `the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation._[37] The breadth of this definition is critical to understanding cybersecurity: not only do strong cybersecurity practices require technical solutions, but they also require strong organizational processes and continuous management.[38] In the cybersecurity field, both administrative controls, controls like processes and procedures regulating human behavior, and technical controls, or controls managed via computerized mechanisms, must be implemented in a complete cybersecurity program.[39] Much like medical device regulation and safety assessments, cybersecurity is, at its foundation, a creature of risk management.[40]

The cybersecurity field aims to protect the confidentiality, integrity, and availability of information.[41] For digital health, this means examining how a loss of confidentiality, integrity, or availability might result in risks to a patient or consumer for a particular type of device, ultimately causing an either physical or financial injury.[42] Understanding the risks for a specific

[35] Williams & Woodward, infra note 136, at 307.

[36] MOBILE MEDICAL, infra note 143; GENERAL WELLNESS, infra note 144.

[37] Cybersecurity: A Beginner˜s Vocabulary, CYBERSECURITY U, http://www.cybersecurityu.org/cybersecurity-a-beginners-vocabulary/ (last visited Nov. 16, 2016).

[38] A common example in cybersecurity is the practice of access management. Access management practices involve processes like access reviews, where user accounts are reviewed periodically to ensure individuals who have moved to a new role or have been terminated no longer have access to systems and information. See THE FIN. INDUS. REG. AUTH., REPORT ON CYBERSECURITY PRACTICES 19 (Feb. 2015), http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

[39] Stephen Northcutt, Security Controls, SANS TECH. INST., http://www.sans.edu/research/security-laboratory/article/security-controls (last visited Oct. 26, 2016).

[40] See generally THE N.Z. NAT˜L CYBER SECURITY CTR., CYBER SECURITY AND RISK MANAGEMENT: AN EXECUTIVE LEVEL RESPONSIBILITY (2013), http://www.ncsc.govt.nz/assets/cyber-security-risk-management-Executive.pdf.

[41] Dan Craigen et al., Defining Cybersecurity, TECH. INNOVATION MGMT. REV. 13, 15 (Oct. 2014) (citing Public Safety Canada 2014).

[42] Peter Sullivan et al., In Cybersecurity, No Harm Does Not Necessarily Mean No Foul, L. 360 (Feb. 17, 2016), http://www.law360.com/articles/759413/in-cybersecurity-no-harm-does-not-necessarily-mean-no-foul.

type of device is a critical step in effective cybersecurity because certain threats exploit different types of devices, and IoT devices, increasingly used as medical devices, already have significant vulnerabilities.[43]

The digital health marketplace provides almost unlimited opportunities for sensitive data exposure and financial gain for malicious actors.[44] Health data has become the most lucrative data type for sale on the black market, netting $10 per record;[45] fifty percent of identity theft events involve medical data, and health data is compromised in forty-four percent of data breaches.[46] Hackers and other malicious actors use health data to file tax returns, file false medical claims against insurance, or receive other benefits, such as free prescriptions.[47] In 2014, a new record was reached with one billion personal information records compromised in one year; in 2015, Anthem, Inc. reported a cybersecurity data breach impacting eighty million health insurance customers, the largest breach to date involving health information.[48] Opportunities for system compromise and the value of

[43] Ericka Chickowski, Internet of Things Contains Average of 25 Vulnerabilities Per Device, DARK READING (July 29, 2014, 9:15 AM), http://www.darkreading.com/vulnerabilities´ -threats/internet-of-things-contains-average-of-25-vulnerabilities-per-device/d/d-id/1297623; TJ McCue, $117 Billion Market For Internet of Things In Healthcare By 2020, FORBES (Apr. 22, 2015, 5:25 PM), http://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/#6e0c5af82471.

[44] ORG. FOR ECON. CO-OPERATION & DEV. DIRECTORATE FOR SCI., TECH. & INNOVATION COMMITTEE ON DIGITAL ECON. POL˘Y, MANAGING DIGITAL SECURITY AND PRIVACY RISK 13¯15 (2016). Malicious actors can be internal or external to a company, from state-sponsored hacking to individually motivated individuals. The range of malicious actors can be large, and with health information netting top dollar on the black market, the variety of malicious actors is quite large. See INST. FOR CRITICAL INFRASTRUCTURE TECH., HACKING HEALTHCARE IT IN 2016 1, 8¯22 (Jan. 2016), http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf (describing threats manifesting from malicious actors of various types).

[45] Compare Candid Wueest, Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services, SYMANTEC (Nov. 20, 2015), https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services (noting stolen email accounts go for $.10 to $10 per 1000 emails and stolen credit card information costs between $.10 and $20), with Caroline Humer & Jim Finkle, Your Medical Record Is Worth More to Hackers than Your Credit Card, REUTERS (Sept. 24, 2014, 2:24 PM), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 (stating stolen health credentials can amount to $10 per record, ten to twenty times the value of a stolen credit card number).

[46] Kristen Fischer, The 7 Biggest Health Data Breaches in the US (So Far), HEALTHLINE (Sept. 28, 2014), http://www.healthline.com/health-news/seven-biggest-health-data-breaches-092814; Humer & Finkle, supra note 45.

[47] See Fischer, supra note 46 (describing the ways hackers use health data).

[48] 1 Billion Data Records Compromised In Data Breaches, HELP NET SECURITY (Feb. 16, 2015), https://www.helpnetsecurity.com/2015/02/16/1-billion-data-records-compromised-in-data-breaches/; Elizabeth Weise, Massive Breach at Health Care Company at Anthem Inc., USATODAY (Feb. 5, 2015, 9:26 AM), http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/.

personal information continue to incentivize criminal activities.

Although identifiable health information has special value on the open market, digital health cybersecurity deserves enhanced scrutiny due to the multi-dimensional nature of digital health threats.[49] The digital health marketplace includes countless networked endpoints exposed to threats via the open Web; hardware that monitors, explores, or alters the human body; and highly sensitive biological, medical, and other health information.[50] Furthermore, efforts to improve convenience of treatment often involve consumer mobile devices and home networks with unknown security controls.[51]

Security vulnerabilities have been identified since 1988, when the Morris worm crashed thousands of machines causing millions of dollars in damage.[52] Since 1988, hackers have increasingly exploited system vulnerabilities affecting millions of systems and devices using various attack types.[53] However, it took twenty years before researchers hacked the first medical devices, hacking a pacemaker in 2008.[54] Since that time, hacks have progressed to include insulin pumps and other devices.[55] In 2014, the Department of Homeland Security (DHS), the FBI, and the FDA began issuing security alerts of known medical device vulnerabilities, and in 2015, hackers began using medical devices as an entry point onto hospital networks to access patient data by hacking Hospira˘s PCA infusion drug pumps.[56] So

[49] 2016 Threats Predictions, McAfee Labs 14, 33¯34 (2016), http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf.

[50] Barbara L. Filkins et al., Privacy and Security in the Era of Digital Health: What should Translational Researchers Know and Do about it?, 8 Am. J. Transl. Res. 1560, 1564 (2016).

[51] Pardeep Kumar & Hoon-Jae Lee, Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey, 12 Sensors 55, 59 (2012) (discussing how transmitting wirelessly, which is included in many sensor technologies, can be subject to eavesdropping during data transmission from device through a network to a recipient).

[52] Craig Timberg, Net of Insecurity, Wash. Post (May 30, 2015), http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/ (explaining how the Morris worm used the openness of the Internet to quickly spread malicious codes that crashed thousands of machines, exploiting a security flaw believed to be corrected).

[53] See Taylor Armerding, The 15 Worst Data Security Breaches of the 21st Century, CSO Online (Feb. 15, 2012, 7:00 AM), http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html?page=2 (documenting major security breaches of the 21st century).

[54] Medical Device Security, Symantec 1 (2016), https://www.symantec.com/content/dam/symantec/docs/data-sheets/symc-med-device-security-en.pdf.

[55] Id.

[56] Id.; Chris Brook, Vulnerability-Riddled Drug Pumps Open to Takeover, threatpost (May 5, 2015, 2:34 PM), https://threatpost.com/vulnerability-riddled-drug-pumps-open-to-takeover/112629/; Michael Mezher, Cybersecurity Researcher: Recent Device Vulnerabilities Should Be a Wake-Up Call to FDA, Reg. Aff. Profs. Soc˘y (Apr. 5, 2016), http://raps.org/Regulatory-Focus/News/2016/04/05/24704/Cybersecurity-Researcher-Recent-Device-Vulnerabilities-Should-Be-a-Wake-Up-Call-for-FDA/.

far in 2016, organizations like CareFusion have responded more productively, actively owning and driving remediation of research-identified vulnerabilities.[57] Despite improved organizational awareness to medical device vulnerabilities, organizations have resisted proactive vulnerability disclosure and risk management.[58]

Taken together, the presence of a variety of new digital health technologies against a backdrop of lucrative health data sales on the black market appears to have created an ideal scenario for data exposure and increasingly exploited vulnerabilities.[59] In lieu of market-driven improvements in cybersecurity for the digital health marketplace, regulatory schemes could effectively drive cybersecurity improvements.[60] The HIPAA and the Food, Drug, and Cosmetic Act (FDCA) with associated regulatory activity from the OCR and the FDA could provide appropriate oversight for digital health cybersecurity improvements.

PART II: CYBERSECURITY REGULATORY ACTIVITY

A. Health Insurance Portability and Accountability Act

The U.S. Department of Health & Human Services˘ (HHS) OCR actively drives privacy and cybersecurity requirements in the digital health market for entities subject to HIPAA.[61] HIPAA, updated in 2003, and the Health Information Technology Economic and Clinical Health (HITECH) Act, passed in 2009, establish a compliance framework for a limited subset of digital health providers: Covered Entities (CE) and corresponding Business Associates (BA).[62]

[57] See Mezher, supra note 56 (explaining that researchers found 1418 vulnerabilities in one tool, the Pyxis SupplyStation, and half of which are considered `high severity_ according to commonly accepted Common Vulnerability Scoring System (`CVSS_) ranking); see NVD Common Vulnerability Scoring System Support v2, NAT˘L INST. STANDARDS & TECH. (Aug. 25, 2016), https://nvd.nist.gov/cvss.cfm (explaining that CVSS is a standard measuring system used to determine vulnerability impact scores and is used by public and private enterprises).

[58] Mezher, supra note 56.

[59] See supra notes 44¯58 and accompanying text (discussing the financial incentives for hackers to capitalize on the security vulnerabilities in the digital health marketplace).

[60] See, e.g., Health Privacy: HIPAA Basics, PRIVACY RIGHTS CLEARINGHOUSE (Feb. 1, 2015), https://www.privacyrights.org/content/health-privacy-hipaa-basics#coveredentities [hereinafter HIPAA Basics].

[61] Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. No. 104-191, 110 Stat. 1938 (1996); HIPAA Basics, supra note 60.

[62] Health Insurance Portability and Accountability Act (HIPAA) of 1996, 45 C.F.R. í 160 et seq. (1996); Health Insurance Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. í 17921 (2016); 42 U.S.C. í í 17934¯40 (2010); HIPAA Basics, supra note 60; Vadim Schick, After HITECH: HIPAA Revisions Mandate Stronger Privacy and Security Safeguards, 37 J.C. & U.L. 403, 408¯18 (2011). HITECH˘s contributions included expansion of BA HIPAA compliance responsibilities (including execution of Business

1. Classification and Applicability

For HIPAA to require organizational compliance, organizational activities must involve Protected Health Information (PHI), which is information that relates to the past, present, or future physical or mental health condition of an individual.[63] It can include a wide variety of data elements including name, address, admission date, birth date, medical record numbers, health plan beneficiary numbers, age over eighty-nine, IP addresses, biometric identifiers, and a variety of other elements.[64] From a data perspective, HIPAA is broad in application, though limited to specific entities, the CE and the BA.[65]

CEs have a primary business relationship with individuals, such as patients, who disclose PHI to CEs for health services or coverage of health services.[66] Under HIPAA, CEs fall into three categories: health plans, which typically involve insurance providers or self-insured entities; healthcare providers, or organizations providing health care to individuals, such as hospitals, clinics, or research institutions; and healthcare clearinghouses, or an organization that processes or facilitates the processing of nonstandard data elements to standard data.[67] BAs, or organizations that perform a supportive role for CEs, perform activities involving the use or disclosure of PHI on behalf of, or to perform services for, a CE.[68] Statutory interpretation clearly illustrates that the categorization of a BA is dependent on the primary organizationˇs classification as a CE.[69] If an organization is not a CE or BA

Associate Agreements), limited PHI sale without authorization, required the expanded use of limited data sets, required data breach notification and reporting requirements, enhanced Office for Civil Rights (OCR) latitude to conduct periodic audits, and expanded fine amount and application to business associates.

[63] 45 C.F.R. í 160.103 (2013).

[64] Id.

[65] See HIPAA Basics, supra note 60.

[66] OFF. NATˇL COORDINATOR FOR HEALTH INFO. TECH., U.S. DEPˇT HEALTH & HUMAN SERVS., GUIDE TO PRIVACY AND SECURITY OF ELECTRONIC HEALTH INFORMATION 15 (Apr. 2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

[67] Id.

[68] 45 C.F.R. íí 164.502(e), 164.504(e), 164.532(d), 164.532(e) (2013); HIPAA Basics, supra note 60.

[69] 45 C.F.R. í 160.103. The statutory language `on behalf of_ a CE illustrates a dependency within HIPAA on CE status. Therefore, if the primary organization receiving health data directly from an individual does not meet the definition of a CE, third parties performing activities on behalf of a CE similarly are not considered a BA, and third parties of a third party are not considered a BA. Ultimately, neither of these organizations, if not following from CE status, would be required to meet HIPAA or HITECH statutory requirements. However, BAs must individually and independently comply with HIPAA under the HITECH updates; somewhat severing a compliance responsibility for CEs of their BAs, though CEs must still hold BAs accountable to compliance with HIPAA via monitoring activities. See Health Insurance Technology for Economic and Clinical Health Act í 17921

and a third party is involved, that third party is also not subject to HIPAA.[70]

2. The HIPAA Privacy Rule

The HIPAA Privacy Rule enforces the privacy concepts of collection, notice, consent, and authorization to use or disclose PHI. HIPAA restricts collection or subsequent use of PHI to the `minimum necessary._[71] To this end, CEs must implement policies and practices to reasonably limit PHI collected, used, or disclosed to only what is necessary for personnel to perform their job duties.[72] Even though a CE may have access to a significant amount of PHI, it may not disclose unrestricted copies of this information to third parties, except at the direction and authorization of the individual or as previously communicated and authorized.[73]

HIPAA provides precise requirements of how an individual must receive notice about a CE˜s privacy practices. Individuals must receive a Notice of Privacy Practices before a CE collects PHI, and be informed that updates to this notice are distributed every three years or within 60 days of material changes.[74] The Notice of Privacy Practices includes an effective date; information about use, such as third party use and data transfer; what type of PHI may be collected; identity of the CE; and information about how to file a complaint.[75] The privacy notice must be provided upon request, posted in an easily accessible location, written clearly and in an easy to read style, provided on demand, and the notice must be complete with respect to CE and BA practices.[76] The individual then consents to the notice by written consent (electronic or in paper form).[77]

(providing the definition of breach and its exceptions).

[70] 45 C.F.R. í 160.103; Health Insurance Technology for Economic and Clinical Health Act í 17921.

[71] 45 C.F.R. í 164.502(b), 164.514(d) (2013).

[72] 45 C.F.R. í 164.502(b), 164.514(d).

[73] 45 C.F.R. í 164.502(b), 164.514(d). The minimum necessary rule does not apply when disclosed to a health care provider for treatment, payment, for operational purposes, or to the individual, pursuant to authorization, for Office for Civil Rights (OCR) complaint investigation, or pursuant to a legal demand; see SUMMARY OF THE HIPAA PRIVACY RULE, U.S. DEP˜T HEALTH & HUMAN SERVS. 4¯11, https://www.hhs.gov/sites/default/files/privacysummary.pdf (last revised May 2003) (explaining the instances when a CE is permitted to use and disclosures protected health information, the authorization requirements a CE must obtain before any use or disclosure of protected health information, and when the minimum necessary requirement is not imposed on a CE).

[74] 45 C.F.R. í 164.520. The three-year distribution depends on material changes not being made. If material changes are made to the notice, the notice must be posted and distributed within 60 days.

[75] 45 C.F.R. í 164.520(b).

[76] Id.

[77] 45 C.F.R. í 164.506, 164.510, 164.512; Standards for Privacy of Individually Identifiable Health Information, U.S. DEP˜T HEALTH & HUMAN SERVS. (July 6, 2001),

Although CEs must adhere to the minimum necessary requirement when handling PHI, CEs may use, transfer, or disclose PHI pursuant to individual authorization.[78] When a CE uses an individual˘s PHI for purposes beyond the scope of necessity outlined in the privacy notice, written consent (authorization) communicating the details of this use is required from the individual.[79]

3. The HIPAA Security Rule

In contrast to the HIPAA Privacy Rule, which relies on standard privacy principles and clear rules, the HIPAA Security Rule applies risk management techniques to manage data confidentiality, integrity and availability for PHI.[80] Risk management techniques typically offer more overall flexibility for an organization to choose a particular solution to comply with the HIPAA Security Rule.[81]

The HIPAA Security Rule organizes implementation specifications into two categories: addressable and required.[82] In contrast with a required

https://aspe.hhs.gov/basic-report/standards-privacy-individually-identifiable-health-information. Individuals can also use electronic signatures. Although the use of electronic signatures is not definitely prescribed under HIPAA, the Electronic Signatures in Global and National Commerce (E-SIGN) would apply to the Notice of Privacy Practices; see Kathy Bakich & Kaye Pestaina, Security and Electronic Signature Standards, Employer˘s Guide to HIPAA Privacy Requirements ò 1030 (Kathryn Bakich & Joanne Hustead eds., 2015), Westlaw (database updated 2016) (explaining that the standard for electronic signatures were never finalized in the security rules).

[78] 45 C.F.R. í 164.506.

[79] 45 C.F.R. í 164.506, 164.508. CEs must receive authorization before collecting data beyond the minimum necessary rule. A hallmark of HIPAA, the minimum necessary rule ensures limitations on abuse of data collection, such as transfer to third parties or gathering of data not pertinent to the administration of treatment or procurement of other health services like insurance. HITECH, which amended and updated HIPAA provisions in 2009 explicitly established that CEs may not sell an individual˘s PHI without additional authorization. See Schick, supra note 62, at 408¯18. HITECH also provided additional enhancements, such as explicit obligations for BAs to follow HIPAA, a co-extensive responsibility to sign a Business Associate Agreement (BAA), and authorization for the Office for Civil Rights to audit CEs and BAs to ensure compliance; see also Howard Anderson, The Essential Guide to HITECH Act, HEALTHCARE INFO SECURITY (Feb. 8, 2010), http://www.healthcareinfosecurity.com/essential-guide-to-hitech-act-a-2053 (summarizing the major data security components of the HITECH Act).

[80] 45 C.F.R. í 160, 164; see generally U.S. Dep˘t Health & Human Servs., 2 HIPAA Security Series 3 (2004), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (explaining how the Security Rule applies to CEs and providing assistance with implementation of the security standards).

[81] U.S. Dep˘t Health & Human Servs., supra note 80, at 8.

[82] 45 C.F.R. í 164.306(d); What is the Difference Between Addressable and Required Implementation Specifications in the Security Rule?, U.S. Dep˘t Health & Human Servs., http://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html (last visited Nov. 8, 2016) [hereinafter Addressable and Required Implementation].

implementation specification, an addressable specification permits a CE or BA to choose how it satisfies the objective of the requirement.[83] Satisfying the objective may include meeting the specification, finding an alternative solution, or not meeting the specification with additional documented substantiation.[84] In all cases, the CE or BA must document its decision.[85] When determining security measures to include, organizations must evaluate the size, complexity, and capabilities of the organization; the technical infrastructure, hardware, and software security capabilities; the costs of security measures; and the probability and criticality of potential risks to electronic PHI (ePHI).[86]

The HIPAA Security Rule, which preceded many modern developments in digital health, requires compliance with a smattering of program-level specifications, yet does not explicitly require many cybersecurity controls. Ultimately, twenty-one specifications of thirty-nine relate purely to security rather than broad IT practices, and of those twenty-one specifications, six describe high-level identity and access management procedures, four relate to higher-level risk management specifications, and three relate to an incident response process.[87] Although these focus areas are important to protect PHI from unauthorized disclosure or change and ensure availability of PHI, only eight specifications in some way describe technical cybersecurity controls, none of them required.[88]

[83] Addressable and Required Implementation, supra note 82.

[84] Id.

[85] Id.

[86] 45 C.F.R. í 164.306(b)(2).

[87] For example, HIPAA devotes eight specifications to disaster recovery and business continuity; four specifications to physical security; three specifications to documentation requirements; two specifications to media management; one specification to asset management; and one specification to human resources controls. Although these controls support cybersecurity considerations, they are not typically used to protect an organization and individuals from cyberattack and are instead information technology functions, broadly construed in a typical IT organization. It should be noted that the HITECH Act did introduce compulsory data breach notification requirements. While not discussed here, data breach notification provides a significant opportunity both for improved oversight and for affected individuals to protect themselves; see 45 C.F.R. í 164.400-164.414. Incorporating addressable security specifications, such as encryption using an acceptable key strength and protocol, may reduce a CE or BA˜s obligations for notification, as well; see Breach Notification Rule, U.S. DEP˜T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Sept. 14, 2016).

[88] The remaining specifications fall into the categories of: session management (1), patch management (1), network management (1), event management (1), integrity (2), and encryption (2). These specifications do not consider a substantial amount of cybersecurity controls necessary to protect data. Although this Author aims to illustrate the insufficiency of cybersecurity controls against the backdrop of an increasingly complex regulatory scheme rather than propose changes to HIPAA legislation, it is worth noting that compliance with HIPAA alone would not likely protect PHI from hackers or other entities seeking to damage an organization or individual. It is worth revisiting the sufficiency of the Security Rule at some

In an effort to evolve cybersecurity maturity for CEs and BAs, the OCR has mapped applicable National Institute of Standards and Technology (NIST) specifications to the HIPAA Security Rule, a so-called `crosswalk._[89] Unfortunately, this mapping and other NIST guidance do not establish mandatory requirements for CEs or BAs, and many still mistakenly believe that HIPAA compliance sufficiently protects against cybersecurity risk.[90]

4. OCR Audit Protocol and Oversight

In 2011 and 2012, the OCR developed, pursuant to new HITECH responsibilities, an audit framework transitioning HIPAA specifications into an audit control set and worked with 115 CEs to test the audit process.[91] In 2015, the OCR selected and initiated its first candidate pool for audits, notifying CEs in July of 2016, with planned (at the time of writing) notification of BAs in the fall of 2016.[92] The audit protocol matched HIPAA statutory requirements and was written similarly to the HIPAA privacy, security, and data breach notification rules.[93]

Overall, HIPAA coupled with OCR oversight has set a standard for organizational privacy and security.[94] However, the limited application via

point in the near future. See Niam Yaraghi, Hackers, Phishers, and Disappearing Thumb Drives: Lessons Learned from Major Health Care Data Breaches, BROOKINGS CTR. FOR TECH. INNOVATION 2 (May 2016), https://www.brookings.edu/wp-content/uploads/2016/07/Patient-Privacy504v3.pdf. The use of `addressable_ and `required_ within the HIPAA Security rule was included for purposes of organizational flexibility, enabling organizations to select an appropriate security requirement based on individual circumstances. Unfortunately, organizations have often interpreted `addressable_ as optional. See ADDRESSABLE AND REQUIRED IMPLEMENTATION, supra note 82; Kerry Shackelford, Top 5 HIPAA Compliance Gaps to Avoid, LINFORD & CO LLP BLOG (July 15, 2013), http://linfordco.com/blog/top-5-hipaa-compliance-gaps-to-avoid/.

[89] See generally U.S. DEP˘T HEALTH & HUMAN SERVS., HIPAA SECURITY RULE CROSSWALK TO NIST CYBERSECURITY FRAMEWORK (Feb. 22, 2016), http://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf (describing the mappings between the HIPAA Security Rule and NIST specifications).

[90] Id. NIST offers helpful mappings between cybersecurity categories and relevant standards (including International Standards Organization, or ISO, a popular standard; COBIT, a popular audit standard; NIST standards; and other control sets. NIST has also created additional documents for assistance in complying with HIPAA); see NAT˘L INST. OF STANDARDS & TECH., AN INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) SECURITY RULE (2008), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf.

[91] HIPAA Privacy, Security, and Breach Notification Audit Program, U.S. DEP˘T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/ (last visited Oct. 7, 2016).

[92] Id.

[93] Id.; Audit Protocol ̄Updates April 2016, U.S. DEP˘T HEALTH & HUMAN SERVS. http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/ (last visited Oct. 13, 2016).

[94] HIPAA Enforcement, U.S. DEP˘T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipa

narrow statutory entity definitions and lack of comprehensive required technical security controls illustrate a need for more comprehensive regulation of the digital health marketplace.

B. Federal Food, Drug, and Cosmetic Act

In contrast to the clear application of HIPAA to limited organizational entities, the FDA establishes comprehensive medical device process requirements to ensure safety in the health marketplace for devices subject to the FDCA.[95] The FDCA establishes a compliance framework for products considered medical devices under the statute.

1. Applicability

Under the FDCA, a device is defined as:

> An instrument, apparatus, implement, machine, contrivance, implant . . . including any component, part, or accessory, which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease . . . or intended to affect the structure or function of the body.[96]

Coupled with case law interpretation, the FDCA defines medical devices broadly, including a large variety of devices within the digital health sector.[97] Whether a device is considered a medical device depends on multiple factors.[98] Not remarkably, then, medical device manufacturers or sellers must

a/for-professionals/compliance-enforcement/ (last visited Oct. 13, 2016).

[95] See What does FDA Regulate?, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194879.htm (last updated Mar. 4, 2016) (explaining that the scope of the FDA˜s regulatory authority includes jurisdiction over medical devices such as tongue depressors, heart pacemakers, dental devices, surgical implants, and prosthetics).

[96] 21 U.S.C. í 321(h) (2009); U.S. v. Undetermined No. of Unlabeled Cases, 21 F.3d 1026, 1028 (10th Cir. 1994); JAMES T. O˜REILLY & KATHARINE A. VAN TASSEL, FOOD AND DRUG ADMINISTRATION í 18.2 (4th ed. 2016) (explaining that the definition of device now includes computer software and diagnosis aids, but the device must serve a diagnostic or therapeutic purposes, `regardless of whether medical treatment will follow_).

[97] O˜REILLY & VAN TASSEL, supra note 96; see also Adam Candeub, Digital Medicine, the FDA, and the First Amendment, 49 GA. L. REV. 933, 937¯38 (2015) (noting the complexities and impact of broad FDA regulation of medical devices, including the chilling of innovation. While this Author does not aim to redraw FDA determinations of in-scope medical devices according to the FDCA here, the lack of suitable alternatives for regulation of digital health applications, such as partial regulation under HIPAA or general, non-specific regulation under the FTC does not effectively manage very real patient safety and data privacy concerns); see generally Gary E. Gamerman, Intended Use and Medical Devices: Distinguishing Nonmedical `Devices_ from Medical `Devices_ under 21 U.S.C. í 32(H), 61 GEO. WASH. L. REV. 806 (1993) (explaining medical device definitions until 1993).

[98] U.S. v. An Article of Device, 731 F.2d 1253, 1261 (7th Cir. 1984) (explaining that although the intention of manufacturer in labeling is not dispositive, it may give some

satisfy FDA requirements under the FDCA, in contrast with CEs under HIPAA.[99]

Although previously unclear,[100] the FDA recognizes a category of digital health medical devices involving modern technology: mHealth, IT, wearable devices, telehealth, telemedicine, and personalized medicine.[101] Digital health medical devices span panels, which are groupings created by the FDA to create specific requirements and provide informed oversight by medical specialization.[102]

2. Classification

The FDA classifies devices as Class I, II, or III, and this classification determines medical device controls, including exemptions.[103] From Class I to III, medical devices are organized from requiring least regulatory oversight to most, with Class I devices requiring only compliance with general controls in the FDCA.[104] Classes II and III require a showing of `performance standards_ beyond general controls, and the FDA classifies new medical devices as Class III by default.[105] How the device is used and its connection

indication of the device˘s use and that the intention of the seller or manufacturer is just one of many factors determining status as a medical device).

[99] See infra Part III (adding further discussion on proposed responsibilities for digital health cybersecurity); Compare O˘REILLY & VAN TASSEL, supra note 96 (explaining the definition of medical device), with supra Part II, Health Insurance Portability and Accountability Act, Classification and Applicability (describing parties that largely comply with HIPAA regulation). Covered Entities, frequently health care providers or recipients of devices, must comply with HIPAA regulations. In contrast, the FDCA regulates manufacturers and sellers of medical devices. In some circumstances, a Covered Entity may also be a medical device manufacturer. This may mandate co-compliance with divergent requirements. When organizations are not subject to both regulations, they may be held to comparatively different security schemes, despite reasonably similar risk to individuals.

[100] See Alex Krouse, IPads, IPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices, 9 IND. HEALTH L. REV. 731, 751¯52 (2012) (`[M]ethods of defining when software must be regulated as a medical device creates difficulties with new mHealth companies developing mobile applications. The three FDA software guidance documents still leave considerable questions as to whether an application requires regulation and if so, what regulation is necessary._).

[101] Device Classification Panels, U.S. FOOD & DRUG ADMIN. (Jun. 24, 2014), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051530.htm [hereinafter Device Classification Panels]; see also Digital Health, supra note 18.

[102] 21 C.F.R. íí 868.1¯892.6500 (2016); see Device Classification Panels, supra note 101 (identifying the medical device classification panels).

[103] Classify Your Medical Device, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ (last updated July 29, 2014) [hereinafter Classify Your Medical Device].

[104] Paul M. Coltoff et al., Regulation of Medical Devices, 28 C.J.S. Drugs and Narcotics í 26 (2016).

[105] Id.; Clinical Reference Lab., Inc. v. Sullivan, 791 F. Supp. 1499 (D. Kan. 1992),

to sustaining human life (in comparison to diagnostic or therapeutic uses) determines its final classification.[106]

3. Medical Device Market Obligations

If any organization expects to successfully market a medical device in the United States, the organization must maintain a quality system, a procedural capability that identifies potential safety issues.[107] Class II and III devices and Class I devices automated with computer software require implementation of design controls and process controls within such a quality system.[108] Organizations also must evaluate and document suppliers on the basis of their ability to meet quality controls, including notification to a supplier when its product or service no longer meets quality controls.[109]

When an organization prepares to submit a device to the FDA for approval, organizations may choose to pursue a Q-Submission process.[110] Organizations can use this process to formally receive FDA feedback before submitting a medical device for review in 510(k) or Pre-Market Approval (PMA) submission.[111] Q-Submission processes enable an organization to share information about its device(s) to varying degrees, from an informal meeting like an Informational Meeting, or a more formal Pre-Submission.[112] A Pre-Submission notification submission is required when a device is submitted for the first time or when an organization has changed or modified

aff˜d in part, rev˜d in part on other grounds sub nom; U.S. v. Undetermined No. of Unlabeled Cases, 21 F.3d 1026 (10th Cir. 1994) in 28 C.J.S. Drugs and Narcotics í 26 (2016); see í í 807.81¯807.100, infra note 114 (explaining that because Class III devices pose substantial safety risk to individuals, a PMA is submitted, requiring approval from the FDA).

[106] Classify Your Medical Device, supra note 103.

[107] 21 C.F.R. í 820.5 (2016) (adding that a quality program involves management responsibility for: organizational structure, policies and procedures, and training and awareness; additionally, organizations must provide adequate resources and ensure management review and planning of the Quality Management System (`QMS_)); see 21 C.F.R. í í 820.20, 820.22, 820.25 (2016) (elaborating on quality system requirements regarding management responsibilities, quality audits, and personnel).

[108] 21 C.F.R. í í 820.30, 820.70, 820.80, 820.90 (2016) (explaining that process controls include Standard Operating Procedures (`SOPs_) and compliance with specified reference codes or standards. Devices must also be inspected, tested, or verified prior to acceptance. If a device is found to be nonconforming, the organization must identify and document the nonconformance, and maintain procedures for rework).

[109] 21 C.F.R. í 820.50 (2016).

[110] U.S. Food & Drug Admin., Requests for Feedback on Medical Device Submissions: The Pre-Submission Program and Meetings with Food and Drug Administration Staff 9 (Feb. 18, 2014), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm311176.pdf.

[111] Id. at 11.

[112] Id. at 5; Kimberly Piermatteo, The Pre-Submission Program and Meetings with FDA Staff, U.S. Food & Drug Admin. 6, http://www.fda.gov/downloads/Training/CDRHLearn/UCM461721.pdf (last visited Oct. 9, 2016).

a device to the extent it is not substantially similar.[113]

After any preliminary processes, the FDA requires a 510(k) or PMA submission for all substantially similar or new Class I, II, or III devices marketed for sale.[114] The PMA and 510(k) provide notification from an organization to the FDA of an offering for sale and include supporting documentation about the device, such as comparable technology similarities or differences, whether an organization has conducted a reasonable search of causes for known problems with devices, and clinical trial results.[115] This information enables effective FDA investigation and classification.[116]

[113] 21 C.F.R. í í 807.81(a)(1), 807.81(a)(3), 807.87 (2007).

[114] 21 C.F.R. í í 807.81¯807.100 (2016); Premarket Approval (PMA), U.S. Food & Drug Admin., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/ucm2007514.htm (last updated July 8, 2016); see 21 C.F.R. í 814.1 (2014) (describing the scope of premarket approval of medical devices); Premarket Notification 510(k), U.S. Food & Drug Admin., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYour Device/PremarketSubmissions/PremarketNotification510k/ (last updated Sept. 16, 2015) (explaining that an organization importing a device from an organization that has already filled out the 510(k) does not need to resubmit a 510(k). For Class II devices, if an exemption applies, the FDA may not require a 510(k). For devices with Classes III, a Pre-Marketing Approval (`PMA_) generally is required). But see Laura Hagen, Coding for Health: Cybersecurity in Medical Devices, 28 Health Law. 25, 26¯28 (2016) (explaining that the 510(k) and PMA processes apply to Class II and Class III devices, respectively; Class I devices typically only require registration, not premarket submission).

[115] Classify Your Medical Device, supra note 103; Hagen, supra note 114 (explaining substantially similar Class II devices proposed for sale submit a 510(k); substantially similar devices meeting Class III submit a PMA; and all non-substantially similar, Class II and III new devices submit a PMA. Class I devices are subject to FDCA general controls but do not have additional special controls, while Class II devices are subject to FDCA performance standards); PMA Approvals, U.S. Food & Drug Admin., http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/PMAApprovals/default.htm (last updated Jan. 26, 2016) (explaining that the FDA provides 510(k) clearances after review of disclosed changes to a medical device that is still substantially similar to a previously approved device. For PMAs, the FDA must approve, question, or reject an application within 180 days, while the FDA has 30 or 90 days to clear, question, or reject a 510(k)); Jason Smith & Stephen Barrett, What are 510(k) Clearance and Premarket Approval?, Device Watch (Apr. 12, 2008), http://www.devicewatch.org/reg/510k.shtml; see Premarket Approval, supra note 114 (giving an overview of premarket approval); see Tamsen Valoir & Linda J. Paradiso, Patent Strategy for Medical Devices, 23 Intell. Prop. & Tech. L. J. 8, 8 (2011), http://www.boulwarevaloir.com/fda-paper.pdf (discussing the basics of the FDA and issues in designing patent strategies that adhere to FDA rules).

[116] 510(k) Clearances, U.S. Food & Drug Admin., http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/510kClearances/ (last updated Jan. 26, 2016); Premarket Notification Class III Certification and Summary, U.S. Food & Drug Admin., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/ucm142662.htm (last updated May 19, 2015) (indicating the alternative to a 501(k) is the Investigational Device Exception, where organizations submit documentation to register a device for a clinical study, in comparison to offering a device for sale); see 21 C.F.R. í 812.1 (2016) (identifying the scope of the investigational device exemptions); Device Advice: Investigational Device Exception (IDE), U.S. Food & Drug Admin., http://www.fda.gov/MedicalDevices/Device

Although Class I devices must meet the FDCA standards, they receive neither clearance nor approval through a formal process and only require registration of the organization and the device.[117] Medical mobile applications, a significant proportion of the future digital health marketplace, may require even less scrutiny: the FDA has communicated that many medical mobile applications will not be subject to regulatory requirements, including premarket submissions or quality measures, at this time.[118] If the FDA determines it will regulate a type of device, then an organization˜s obligations do not end after the FDA˜s review and approval of an application.[119] Organizations must report adverse effects for cleared devices, such as safety issues and recalls.[120] This information enables the FDA to effectively share such information with consumers.[121] Organizations selling medical devices must report issues using a Medwatch form, including individual adverse events, device-related deaths, device-related serious injuries, malfunctions, or reportable events requiring remedial action to prevent unreasonable risk of substantial harm to the public health.[122] The FDA then posts safety communications, recalls, bans, and emergency situations for the general public on its Website and via email updates.[123]

4. Reports and Cybersecurity Guidance

Passed in 2012, the Food and Drug Administration Safety and Innovation Act (FDASIA) required the FDA, the National Coordinator for Health Information Technology (ONC), and the Federal Communications

RegulationandGuidance/HowtoMarketYourDevice/InvestigationalDeviceExemptionIDE/ (last updated Sept. 4, 2015).

[117] An Overview of the US FDA Regulatory Process for Medical Devices, EMERGO GROUP (May 5, 2011), http://www.slideshare.net/emergogroup/us-fda-medical-device-regulatory-approval-process.

[118] Examples of Mobile Apps for which the FDA Will Exercise Enforcement Discretion, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368744.htm (last updated Aug. 1, 2016) [hereinafter Examples of Mobile Apps] (explaining that the FDA communicated that health apps involving highly sensitive or confidential information, such as a health condition or individual health data, do not constitute enough risk to the public to merit FDA scrutiny).

[119] 21 C.F.R. í 803.10 (2016); Medical Device Safety, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/Safety/default.htm (last updated Dec. 16, 2016) [hereinafter Medical Device Safety].

[120] 21 C.F.R. í 803.10.

[121] Id.

[122] Id.

[123] See infra Part II, Federal Food, Drug, and Cosmetic Act, Scope of Application and accompanying notes. (explaining generally the quality controls imposed on organizations to ensure consumer safety); Medical Device Safety, supra note 119. The FDA posts communications on its Website and sends email communications to those who register to receive them. See, e.g., Medical Device Safety, supra note 119 (referencing specific safety communications and linking to an email notification sign-up page).

Commission to create a report on a proposed strategy for a risk-based framework involving mobile applications.[124] The 2014 FDASIA Health IT Report recognized four significant conclusions with respect to health information technology that apply to the digital health cybersecurity landscape and shape expectations regarding the FDA˘s involvement in cybersecurity management: 1) that existing FDA functionality is effective, within a culture of safety and quality, including voluntary and non-punitive reporting; 2) health IT should use recognized standards; 3) agency roles should be clarified and avoid overlap; and 4) the FDA will not regulate general, non-health-specific use of IT infrastructure or devices.[125] Further, the FDASIA report clearly illustrated a continuing focus for regulatory agencies on security principles, not applicable technical standards.[126]

In 2014, the FDA began issuing pre- and post-release cybersecurity

[124] Food and Drug Administration Safety and Innovation Act, Pub. L. No. 112-144, í 618, 126 Stat. 993, 1063 (2012).

[125] U.S. Food & Drug Admin., Federal Commc˘ns Comm˘n, Off..Nat˘l Coordinator for Health Info. Tech., FDASIA Health IT Report 3, 9 (Apr. 2014), http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsand Tobacco/CDRH/CDRHReports/UCM391521.pdf [hereinafter FDASIA White Paper] (explaining that The Office of the National Coordinator for Health Information Technology (ONC), an office within the U.S. Department of Health and Human Services (HHS), is positioned in this report as focusing on privacy, security, and health Information Technology (IT) infrastructure. Although the ONC has developed eight documents in collaboration with the broader HHS and the OCR, these documents focus on healthcare providers, not on supply-side requirements for the digital health marketplace, and reiterated HIPAA requirements); see Health IT Privacy and Security Resources, Off. Nat˘l Coordinator for Health Info. Tech., https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources (last updated Feb. 12, 2016) (identifying resources to better integrate HIPAA and other federal health information privacy into practice); Your Mobile Device and Health Information Privacy and Security, Off. Nat˘l Coordinator for Health Info. Tech., https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security (last updated Mar. 21, 2014).

[126] FDASIA White Paper, supra note 125. Government agencies have not attempted to implement specific security requirements in law because appropriate standards could change frequently. However, although technology may change; frameworks, processes, practices, and standards may not change as frequently. Frameworks offer a strong foundation without articulating specific technical solutions. See, e.g., ISO/IEC 27001¯Information security management, Int˘l Org. for Standardization, http://www.iso.org/iso/iso27001 (last visited Oct. 9, 2016) (providing requirements for an information security management system); What is COBIT 5?, Info. Sys. Audit and Control Ass˘n, http://www.isaca.org/COBIT/Pages/default.aspx (last visited Oct. 9, 2016) (describing a model used most often for IT audit purposes); Guidance, Committee Sponsoring Orgs. Treadway Comm˘n, http://www.coso.org/guidance.htm (last visited Oct. 9, 2016); Understanding and Leveraging the CSF, HITRUST Alliance, https://hitrustalliance.net/understanding-leveraging-csf/ (last visited Oct. 9, 2016) (explaining the value of using the HITRUST model for information security in the health care industry); Cybersecurity Framework, Nat˘l Inst. Standards and Tech., https://www.nist.gov/cyberframework/ (last visited Oct. 9, 2016) (explaining why the new NIST cybersecurity framework was created and is useful for organizations) [hereinafter Cybersecurity Framework].

guidelines and issued device vulnerability notices to assist device manufacturers in producing and managing devices less likely to adversely impact consumers.[127] The 2014 Pre-Release Cybersecurity Guidelines addressed incorporating cybersecurity considerations in the design and development of medical devices as part of `software validation and risk analysis . . . [in] 21 CFR 820.30(g)._[128] The FDA recommended incorporating asset identification, threat analysis, and vulnerability reviews into an organizationˇs device development process, including risk assessment and analysis, to determine residual risk and apply mitigation strategies.[129] Such processes should take into consideration the intended use and implementation of a device, such as home use.[130] Moreover, medical device manufacturers are encouraged to specify `cybersecurity safeguards_ in premarket submission processes, such as `hazard analysis_ and `design considerations_ for a medical device, and risks like device cybersecurity controls considered or implemented.[131]

The premarket cybersecurity safeguards recommending asset identification, threat analysis, and vulnerability reviews, reflect a level of standardization in cybersecurity practice.[132] These standards incorporate best practice cybersecurity capabilities, such as access and identity management´ the capability that bars unauthorized users from accessing a system, code validation and management, cybersecurity incident response capabilities, and business continuity´ continuing function of devices even when compromised.[133] These standards have been established by the International Electrotechnical Commission (IEC), the `worldˇs leading

[127] See generally U.S. Food & Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices 1 (2014), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf [hereinafter Cybersecurity White Paper].

[128] Id. at 3.

[129] Id. at 4.

[130] Id. (`Manufacturers should also carefully consider the balance between cybersecurity safeguards and the usability of the device in its intended environment of use (e.g home use vs. health care facility use)._

[131] Id. at 4¯5.

[132] See, e.g., Michael Muckin & Scott C. Fitch, A Threat-Driven Approach to Cyber Security, Lockheed Martin 5, http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/Threat-Driven%20Approach%20whitepaper.pdf (last visited Sept. 15, 2016) (advocating a threats-assets-controls relational model, which shifts focus from vulnerability analysis to threat analysis); Christopher J. Alberts et al., Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0, Carnegie Mellon University (June 1999), https://resources.sei.cmu.edu/asset_files/TechnicalReport/1999_005_001_16769.pdf (describing a security risk management approach involving asset management, vulnerability analysis, and threat identification originating as early as 1999).

[133] Id.

organization_ for electrical technologies.[134]

The FDA˘s Guidance for Industry¯Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software explicitly allocated responsibility for new cybersecurity activities under existing FDCA laws governing technology validation processes.[135] The Guidance further explained that manufacturers should work with vendors to timely receive cybersecurity updates, such as patches, and develop a `cybersecurity maintenance plan._[136]

In January 2016, the FDA distributed the Postmarket Management of Cybersecurity in Medical Devices for comment purposes.[137] This guidance document reiterated the responsibility of manufacturers to include cybersecurity considerations throughout product development and to continuously monitor for device vulnerabilities throughout each device˘s lifecycle.[138] Specifically, the FDA recommends following the NIST Framework for Improving Critical Infrastructure Cybersecurity, a risk management framework, and also sharing identified cybersecurity risks and security incident data via the National Health Information Sharing & Analysis Center.[139]

[134] About the IEC Vision & Mission, Int˘l Electrotechnical Comm˘n (2016), http://www.iec.ch/about/.

[135]· U.S. Food & Drug Admin., Guidance for Industry´ Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (May 28, 2015), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm [hereinafter Guidance for Industry].

[136] *Id.* (The FDA specified that such patches would not be required because `most software patches . . . reduce the risk of developing a problem associated with a cybersecurity vulnerability and not to address a risk to health posed by the device . . . If the software patch affects the safety or effectiveness of a medical device, you should report the correction to FDA._ Although in most cases, a patch is used to neutralize a vulnerability, it is important to remember that vulnerabilities always pose some risk to a device that is used for health purposes. For example, a patch closes a vulnerability that allows an unverified user to change data in transit between the medical device and the receiver, for example a data analysis application. If data is changed, the data in the analysis is incorrect, and decisions for treatment negatively affecting patient safety could be made); *see, e.g.*, Patricia AH Williams & Andrew J. Woodward, *Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem*, 8 Med Devices (Auckl) 305 (2015) (noting that, most, if not all patches will have some bearing on safety of medical devices).

[137] U.S. Food & Drug Admin., Postmarket Management of Cybersecurity in Medical Devices 1 (Jan. 22, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf [hereinafter Postmarket Management].

[138] *Id.* at 4.

[139] *Id.* at 6; Nat˘l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity 1 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf; Promoting Private Sector Cybersecurity Information Sharing, Executive Order 13691, 80 Fed. Reg. 9349 (Feb. 13, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf; Cybersecurity Information Sharing Act of 2015, Pub. L. 114¯113, 129 Stat. 2242 (2015); U.S. Dep˘t of

The FDA also recommends monitoring for cybersecurity vulnerabilities, assessing potential vulnerability impact, and developing mitigation strategies, including deploying patches or remediating code to neutralize vulnerabilities.[140] These recommendations represent industry standard vulnerability management practices, and very thoroughly explain the relationship between vulnerabilities and essential clinical performance.[141] Although the Postmarket Guidelines do not establish binding rules for manufacturers, the details expressed a relatively comprehensive understanding of vulnerability management practices, which significantly affect the ability of a manufacturer to manage medical device risk.[142]

5. Scope of Application

In 2015, the FDA directly communicated its intention to regulate only mobile applications classified as `medical devices_ where their function(s) could pose a risk to patient safety, though it began communicating its overall reluctance to regulate mobile health applications in 2014.[143] In January of 2016, the FDA first reiterated and solidified its intention to minimize its involvement in mobile application regulation, in particular general wellness products.[144] This recent, non-binding direction effectively focuses attention

Homeland Security, Cybersecurity Sharing Act of 2015 Final Guidance Documents ¯ Notice of Availability (June 15, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-06-15/pdf/2016-13742.pdf. The ISACs were created in response to Executive Order 13691 on information sharing, included in the Cybersecurity Information Sharing Act of 2015.

[140] Postmarket Management, supra note 137, at 11¯12.

[141] See generally Murugiah Souppaya & Karen Scarfone, Nat˘l Inst. of Standards & Tech., Guide to Enterprise Patch Management Technologies, 3rd ed. (2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf (explaining the industry standards for enterprise patch management technologies); Tom Palmaers, Implementing a Vulnerability Management Program, SANS Inst. (2013), https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180. Although the FDA Postmarket Guidance does not specify the level of detail explained via NIST and SANS, the conceptual vulnerability management language references these types of programs; and additional detail is introduced to assist manufacturers in considering medical device risk, such as vulnerability scoring and health impact rankings; Postmarket Management, supra note 137, at 13¯15.

[142] Postmarket Management, supra note 137; see Cybersecurity White Paper, supra note 127 (illustrating the agency awareness of security risks potentially affecting the medical device community).

[143] U.S. Food & Drug Admin., Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff 8 (Feb. 9, 2015), http://www.fda.gov/downloads/MedicalDevices/. . ./UCM263366.pdf [hereinafter Mobile Medical]; Examples of Mobile Apps, supra note 118; see Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff- Availability, 78 Fed. Reg 59038 (Sept. 25, 2013) (LEXIS) (illustrating the FDA˘s intent to apply regulatory requirements to only a small subset of mobile apps).

[144] U.S. Food & Drug Admin., General Wellness: Policy for Low Risk Devices Guidance for Industry and Food and Drug Administration Staff 2 (July 26, 2016),

on implanted and physically invasive connected devices and Classes II and III, which the FDA deems not `low risk,_ and it neglects Class I devices.[145]

In the FDA˜s Mobile Medical Apps Guidance, issued in February 2015, the FDA gave specific examples of mobile medical apps where the FDA may exercise enforcement and reiterated the FDA˜s sole focus on patient safety.[146] These examples include medical devices providing technology to monitor patients, conduct data analysis, or for controlling the medical device via a mobile application (Type A, see Table 1); mobile applications connecting to sensors, displays, or attachments of existing medical devices (Type B, see Table 1); and mobile apps that perform the functions of existing diagnostic or therapeutic software, most likely Class II and Class III devices.[147] Reinforcing the FDA˜s focus on patient safety, the FDA also listed mobile apps for which the FDA will exercise enforcement discretion, or choose not to regulate.[148] The FDA will not actively regulate the majority of these apps that may be vulnerable to information loss, including apps that help patients manage disease, track health information, provide remote medical care, provide access to health information, or transfer data from a medical device (Types C-E, see Table 1).[149] In short, the FDA has demonstrated it will regulate direct physical safety, not data loss or disclosure.

The FDA has the ability, via statute and practice, to manage and monitor Class II and Class III medical devices.[150] However, the lack of clear direction of organizational and technical cybersecurity requirements coupled with a reluctance to regulate Class I devices and a significant proportion of mobile applications does not position the FDA to effectively manage cybersecurity risk in the digital health marketplace.

Part III: Proposed Regulatory Landscape

The existing statutory framework regulating the digital health marketplace is not sufficient to reduce and manage cybersecurity risk. FDA guidelines do not effectively manage a market heavily driven by compliance-oriented activities, and entities required to follow HIPAA only covers a subsection of

http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm429674.pdf [hereinafter General Wellness].

[145] Id.

[146] Mobile Medical, supra note 143, at 13.

[147] Id. at 15.

[148] Id.

[149] Id. at 15¯18.

[150] Overview of Medical Devices and Their Regulatory Pathways Medical Devices: The Basics, U.S. Food & Drug Admin., http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHTransparency/ucm203018.htm (last updated Nov. 27, 2015).

organizations involved in creating digital health products and services.[151] Unlike internal confidential data loss affecting an organization only, parties affected by insufficient cybersecurity controls can be patients or consumers, often individuals in a compromised health position.[152] Many patients assume, given the FDA˜s involvement in device safety matters and HIPAA˜s coverage of PHI, that health safety and confidentiality meet existing industry best practices.[153] Others may not be able to effectively advocate their interests, either because of health status or comparatively less bargaining power.[154]

Because the market cannot effectively guarantee this protection and patients often expect a basic level of safety for digital health products, a regulatory framework provides the best option for managing cybersecurity risk. However, achieving a level of specificity in the law that actually reduces risk requires knowledge and regulation of technology as it actually works.[155] Although computer systems collect, compile, process, transfer, display, or store data, specific implementations may use different variations of security controls to meet a security principle, for example, methods for managing password resets.[156] Frameworks should balance specificity with flexibility to

[151] Heather Landi, Medical Device Cybersecurity Needs Enforceable Regulations, Not Just Suggestions, HEALTHCARE INFORMATICS (Feb. 17, 2016), http://www.healthcare-informatics.com/news-item/medical-device-cybersecurity-needs-enforceable-regulations-not-just-suggestions-icit-says; Derek Mohammed et al., Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector, 5 INT˜L J. BUS. & SOC. RESEARCH 55, 57 (2015), http://www.saintleo.edu/media/975946/cybersecurity_challenges_and_compliance_issues.pdf.

[152] Following from the recognition that for the digital health marketplace, participants using devices and apps often have a particular health condition, some very serious in nature. See Mohammed et al., supra note 151, at 56.

[153] See Pam Dixon, What˜s a Consumer to Do? Consumer Perceptions and Expectations of Privacy Online, Testimony Before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, WORLD PRIVACY FORUM 3 (Oct. 13, 2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10PamDixonConsumerExpectationTestimonyfsshort.pdf (testifying on how consumers often do not have the information or opportunity to evaluate the status and treatment of their information, and disconnect exists between what consumers believe organizations do to protect information and what organizations actually do).

[154] See McGraw et al., infra note 173 (illustrating that large business associates, with great bargaining power, can more easily dictate the terms of their security compliance).

[155] In my experience, this challenge has borne out in HIPAA compliance schemes. It is my opinion that because encryption is an `addressable_ requirement under HIPAA, many organizations do not encrypt data and when they do, employ poor encryption practices simply to meet the requirement. Poor practices do not significantly improve an organization˜s ability to protect individual˜s PHI. Similarly, high-level general FDA guidelines will not likely establish the structure necessary to measurably reduce cybersecurity for medical devices.

[156] Mathew J. Schwartz, 5 Ways to Solve the Password Reset Dilemma, DARKREADING (Aug. 14, 2012), http://www.darkreading.com/attacks-and-breaches/5-ways-to-solve-the-password-reset-problem/d/d-id/1105781.

ensure adequate adherence without stifling cybersecurity innovation.

Although a framework could improve cybersecurity for the digital health marketplace, no clear and comprehensive regulatory responsibility currently exists. Overlapping administrative agency responsibilities between the FDA, OCR, the ONC, and the FTC results in a lack of clear cybersecurity direction and accountability for digital health providers.[157] Both part of HHS, the OCR monitors HIPAA compliance for CEs and BAs while the FDA evaluates FDCA compliance for medical devices.[158] Meanwhile, the ONC, also part of HHS, creates high-level standards for cybersecurity and privacy and the FTC establishes rules and holds organizations accountable for unfair or deceptive trade practices under Section 5 of the FTC Act, increasingly for privacy and cybersecurity concerns.[159] This m¶lange of guidance exists, yet no clear stance has emerged that provides a level of specificity, leaving organizations with few options aside from inventing rules inconsistently and independently.[160]

Of these four regulatory bodies, the OCR and the FDA have mature regulatory frameworks with specific health and medical device industry expertise.[161]

[157] David Raths, Digital Health Dilemma: Regulators Struggle to Keep Pace with Health-Care Technology Innovation, Gov˘t Tech. (Jan. 13, 2015), http://www.govtech.com/health/Digital-Health-Dilemma-Regulators-Struggle-to-Keep-Pace-with-Health-Care-Technology-Innovation.html.

[158] See Part II.

[159] See, e.g., Iltifat Husain, FTC, Not the FDA, Tells the Digital Health World They Need Peer Reviewed Data to Back Up Their Claims, iMedicalApps (Jan. 7, 2016), http://www.imedicalapps.com/2016/01/ftc-fda-digital-health (describing the FTC˘s role in ensuring that claims are truthful and non-deceptive while also discussing the FTC˘s growing role in reviewing health products).

[160] Jonah Comstock, Time to Reform HIPAA and FDA Regs for Digital Health Era?, Healthcare IT News (July 13, 2016, 5:01 PM), http://www.healthcareitnews.com/news/time-reform-hipaa-and-fda-regs-digital-health-era; Ed Miserta, mHealth Panel: Make Progress, Not Excuses, Clinical Leader (Aug. 30, 2016), http://www.clinicalleader.com/doc/mhealth-panel-make-progress-not-excuses-0001.

[161] See Part II; HIPAA and the FDCA are typically considered potential regulatory frameworks for managing cybersecurity in the digital health marketplace due to their relatively mature frameworks (HIPAA with its focus on PHI and the FDCA with its focus on medical devices). Further, the OCR and the FDA have been regulating HIPAA and FDCA for, respectively, 20 and 110 years. The OCR has significantly moved the needle toward increased enforcement and activity for privacy and security. On the 20th anniversary of HIPAA, the OCR described how HIPAA has revolutionized the very nature of healthcare and noted the changing nature of health technology, especially mobile health. U.S. Dep˘t Health & Human Servs., U.S. Dep˘t of Labor & U.S. Dep˘t of Treasury, HIPAA at 20: A Bipartisan Achievement, HHS Blog (Aug. 19 2016), https://www.hhs.gov/blog/2016/08/19/hipaa-20-bipartisan-achievement.html. The FDA has also increased its reach as new technologies emerged. See Colin Zick et al., Regulation Electronic Health Records and Clinical Decision Support, Foley Hoag, LLP (Jan. 2014), http://www.foleyhoag.com/-/media/files/foley%20hoag/speaking%20engagements/2014/zick_ehra_fda_onc_regulation_of_health_it.ashx?la=en (describing FDA proposed regulation and workgroup implemented in order to address then-

B. The Office for Civil Rights: Steady Executor

HHS˘ OCR provides oversight for HIPAA compliance, which includes management of the HIPAA Security Rule.[162] Although the HHS and OCR have worked with the FTC to create guidance for digital health cybersecurity topics, such as a Mobile Health Apps Interactive Tool,[163] the OCR has preferred to focus on its HIPAA obligations.[164] Absent broad omnibus privacy or cybersecurity legislation, the OCR has created a strong enforcement structure and fairly clear guidance for privacy and security requirements applicable to PHI within the United States, at least illustrating its broad reach.[165]

For CEs and BAs subject to HIPAA, HIPAA does require some level of cybersecurity compliance, albeit somewhat limited to highly flexible, general, and presumably avoidable security specifications.[166] Despite less

emerging categories software). Software has been subject to FDA regulation since the 1980s, even though Congress did not expressly direct the FDA to manage software. The FDA regulates both devices AND accessories to medical devices. The FTC also regulates mobile medical applications and drafted guidance in 2013 updating in 2015. See MOBILE MEDICAL, supra note 143 (issuing updated guidance on mobile medical applications).

[162] See Part II, Health Insurance Portability and Accountability Act.

[163] Mobile Health Apps Interactive Tool, FED. TRADE COMM˘N (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[164] See Part II, Health Insurance Portability and Accountability Act. The OCR has focused the majority of its time in creating and audit process, auditing, and investigating 24,331 cases with settlements totaling $39,989,200. Enforcement Highlights, U.S. DEPT. HEALTH & HUMAN SERVS, (Nov. 30, 2016), http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[165] Daniel J. Solove, HIPAA Might and Flawed: Regulation Has Wide-Reaching Impact on the Healthcare Industry, 84 J. OF AHIMA 30¯31 (2013), http://bok.ahima.org/doc?oid=106326#.V8lXWfkrLIU. The OCR˘s use of `Final Omnibus Rule_ is a bit of a misnomer. Omnibus is used to reference broadly applicable privacy laws internationally, such as Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada or the Global Data Protection Regulation (GDPR) in the European Union. Sectoral and Omnibus Privacy and Data Protection Laws, NYMITY (2015), https://www.nymity.com/~/media/Nymity/Files/Privacy%20Maps/NYMITY_World_Map.ashx.

[166] See Part II, The HIPAA Security Rule; Historically, the OCR has not prosecuted HIPAA Security Rule violations except where a violation has already caused a data breach or where a complaint has been filed; see, e.g., Data Breach Results in $4.8 Million HIPAA Settlements, U.S. DEP˘T. HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/new-york-and-Presbyterian-hospital/index.html (last visited Dec. 12, 2016) (listing two listed settlements, both of which closed lawsuits brought upon by HHS receiving a notice of a data breach within each organization); see also Matthew A. Fisher, First Ever OCR Settlement of Enforcement Action against HIPAA Business Associate Due to PHI Breach ¯ $650,000 Monetary Resolution Payment, POYNERSPRUILL LLP (July 13, 2016), http://www.poynerspruill.com/publications/Pages/FirstOCRSettlementofEnforcementActionagainstHIPAABusinessAssociateDuetoPHIBreach.aspx (describing an OCR settlement with a Business Associate, which closed an action brought after the reported theft of the Business Associate employee˘s PHI-filled yet unencrypted - and noncompliant - phone); see also OCR Penalizes Physician Practice for HIPAA Privacy and Security Rule Violations, HIPAA.COM (Apr. 18, 2012),

restrictive cybersecurity requirements in the HIPAA statute, the HIPAA regulatory structure, in particular the OCR˜s enforcement activity, has evolved over eighteen years to become comparatively stronger than pre-HITECH HIPAA OCR activity.[167]

Unfortunately, the existing roles within HIPAA significantly limit the OCR˜s ability to fully regulate the digital health marketplace.[168] CEs only include health plans, healthcare providers, and healthcare clearinghouses, a limited set of organizations with very specific purposes.[169] Manufacturers and developers of digital health products, therefore, would likely not be considered CEs unless their services are provided directly to consumers and the services are reimbursable by insurance.[170] The BA role may include some manufacturers and developers if providing digital health solutions through a CE, but collectively CE and BA roles alone do not encompass direct-to-consumer digital health technologies, leaving a large portion of the digital health marketplace regulated only by catch-all FTC enforcement.[171]

Further, the HIPAA model cannot sufficiently regulate digital health cybersecurity because it exhibits a pull, demand-side compliance model.[172]

https://www.hipaa.com/ocr-penalizes-physician-practice-for-hipaa-privacy-and-security-rule-violations/ (describing an HHS resolution with a Physician Practice following its HIPAA violations).

[167] See HIPAA enforcement actions, supra note 166 (representing a fraction of HIPAA enforcement actions which ultimately serve to strengthen the OCR˜s regulatory scheme); see generally Part II, Health Insurance Portability and Accountability Act and accompanying notes (describing CE and BA roles and statutory requirements).

[168] EXAMINING OVERSIGHT, supra note 11, at 15.

[169] See Part II, HIPAA Classification and Applicability.

[170] Id.

[171] Id. Although the BA role is comparatively large and has been applied in a variety of business contexts, the BA role depends on its relationship with a Covered Entity. Because a Covered Entity is fairly narrow in application, BA applicability also leaves out significant portions of the Digital Health marketplace. Although the Federal Trade Commission does enforce unfair and deceptive trade practices, the FTC Act gives power to the FTC to regulate data security practices, but does not directly create statutory requirements for organizations to meet on the front end. See Kathryn F. Russo, FTC v. Wyndham Worldwide Corporation et al. and the FTC˜s Authority to Regulate Companies˜ Data Security Practices, 23 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 164, 166¯68 (2014) (describing the Wyndham case outcome substantiating the FTC˜s ability to bring actions under the FTC Act for data security practices amounting to unfair or deceptive trade practices). The FTC does have rulemaking authority as specifically allocated according to statute, such as the Health Breach Notification Rule, incorporated into the American Recovery and Reinvestment Act of 2009; see 16 C.F.R. Part 318.

[172] This Article does not address whether privacy should be included in consumer protection statutes because Congress has already enshrined that decision in substantial legislation, including HIPAA. That said, the regulatory structure of HIPAA does not require pre-market approval or validation before a process or device is released to the public; this structure relies on voluntary compliance. Otherwise, this structure carries substantial potential penalties if an entity does not comply, additionally in which case either the OCR audits the entity or someone files a complaint; see Part II, Health Insurance Portability and

Essentially, the HIPAA model depends on purchasers demanding compliance of products that are currently on the market in comparison to the FDA˘s barrier for entry: CEs purchasing products or services from a BA and individual consumers purchasing products or services from a CE must have the requisite bargaining power and knowledge to ensure CE or BA compliance prior to purchase.[173] If CEs or BAs do not choose to fully comply with HIPAA, consumers or CEs accept the risk or file a complaint with the OCR.[174] In contrast, for BAs who have less bargaining power, CEs may demand more stringent requirements than HIPAA compliance requires,[175] potentially resulting in additional barriers to market or lack of good faith and fair dealing when BAs agree to terms they cannot meet.[176] HIPAA˘s lack of preemptory power, wide variation of bargaining power between parties, and `after the fact_ compliance management is a poor fit for mass-produced or developed digital health products and services with fewer opportunities for significant change after development or manufacture.[177] When a manufacturer has developed a product or service offering before selling to a

Accountability Act. In contrast, approval-based compliance with continuing obligations provides a better fit both to ensure compliance before market entry in order to safeguard safety in the digital health marketplace and ultimately instill consumer confidence; see Part III, The U.S. Food and Drug Administration: Reluctant Leader.

[173] Deven McGraw et al., Business Associate Compliance With HIPAA: Findings From a Survey of Covered Entities and Business Associates, MANATT, https://www.manatt.com/getattachment/0b19cc2d-ed14-458b-a4bc-7b4436437c4f/attachment.aspx;
Although HITECH updates made clear BAs˘ independent HIPAA compliance, somewhat removing complete reliance on a pull model, Congress presupposes that the OCR knows of a particular organization and holds it accountable. While the OCR could use various measures to ascertain BAs, such as registration of Business Associate Agreements or annual disclosures of BAs, Congress has not yet required such actions of Covered Entities; compare Part II, HIPAA with Part II, FDCA (particularly note substantial activities required of organizations seeking to market products in the United States).

[174] How to File a Health Information Privacy or Security Complaint, U.S. DEP˘T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html (last visited Aug. 10, 2016) (explaining that despite a complaint process, complaints filed after product development cannot prevent data exposure or potential physical injuries, simply because enforcement action occurs after development and product release).

[175] See McGraw et al., supra note 173 (noting how variability in compliance terms can create market issues: in particular, with unpredictable expectations some organizations may face a significant barrier to entry in the market, reducing competition).

[176] Id. (describing that some BAs may agree to terms without fully understanding obligations, and some CEs may not have the requisite resources to conduct risk assessments on all BAs to ensure compliance).

[177] See Part II, HIPAA Security Rule and accompanying notes (noting that HIPAA works more effectively for organizations that manage ongoing HIPAA compliance, such as health care providers) (explaining that such organizations can plan additions and changes to privacy and security programs, and HIPAA requirements heavily reference privacy and security business processes (explaining that for medical devices, substantial issues identified after the fact can involve recalls, costing significant amounts of money)).

CE, the likelihood of consumer injury increases.[178]

In addition to concerns regarding the breadth of HIPAA regulatory effects and the ability for HIPAA to meaningfully prevent consumer injury, the digital health marketplace also requires more robust and comprehensive cybersecurity specifications to sufficiently manage cybersecurity risk.[179] HIPAA privacy and security specifications fit the roles of CEs and BAs as traditionally understood, rather than as product manufacturers or service providers.[180] Focusing on general IT functions, high level organizational process, and risk management techniques, rather than product development and service requirements or validation procedures does not effectively direct the specificity often needed in the development process.[181]

While the OCR provides active HIPAA enforcement, HIPAA limits applicability to specified entities, leaving a significant gap of uncovered entities.[182] In the rare circumstance that Congress would expand definitions of HIPAA entities, the HIPAA compliance model does not effectively manage consumer risk for entities manufacturing and developing products.[183] Absent significant statutory revision, it is unlikely that OCR oversight could effectively manage broad digital health cybersecurity risk.

A. The U.S. Food and Drug Administration: Reluctant Leader

The FDA has signaled its reluctance to manage cybersecurity in a variety of ways, including statements that the ONC manages privacy and cybersecurity standards for health IT and that the FDA will not regulate

[178] See Part II (following the logical conclusion of demand-side compliance, the best case occurs when and if CEs have bargaining power to demand HIPAA compliance of BAs; the worst case when and if the OCR holds BAs accountable) (nothing how in both circumstances, compliance expectations are communicated after, rather than before a BA creates an unsecure product causing consumer injury).

[179] See Part II, HIPAA Security Rule and accompanying notes; see Raths, supra note 157.

[180] See Raths, supra note 157 (describing how the HIPAA Privacy Rule does not match a fast-moving, digital health marketplace with increasingly mobile connectivity and how, similarly, security specifications could include standard product development measures, such as code scanning prior to release, effective code merging and management, standard authentication procedures and identity validation); see Part III.

[181] Raths, supra note 157.

[182] See Part II, HIPAA Classification and accompanying notes.

[183] See Part II and accompanying notes. Because Covered Entities (CE) and Business Associates (BA) are highly specific roles under HIPAA, requiring a variety of conditions to be in place before HIPAA applies, relying only on HIPAA to regulate the digital health marketplace would not effectively manage cybersecurity risk across the digital health market, as many organizations are not required to be compliant with HIPAA. If Congress expanded these definitions, the lack of comprehensive cybersecurity requirements would still not effectively manage cybersecurity risk, due to the gaps in required cybersecurity activities for CE and BA.

general health apps.[184] Despite this, the FDA has the regulatory structure, function, and focus to effectively regulate the digital health marketplace with some involvement from OCR, FTC, and ONC partners.[185]

The FDA first must officially include the digital health products and services in its definition of medical device. This change will require compliance with standard quality measures included in a quality system under the FDCA.[186] Today, the FDA does not recognize many potential Class I devices, like mobile health applications, as medical devices.[187] With an ever-increasing focus on IoT technologies, non-invasive sensor-based care, and health data loss, the FDA cannot avoid acting in the best interests of consumers.[188] Similar to the extension of the FDCA˘s interpretation of `contrivance_ to include computer software in 1989, the FDA should embrace its responsibility for regulating other computer-based applications.[189] Many benefits to the consumer will naturally extend from FDCA regulatory controls, including required inclusion of a quality management system, policy development and standard operating procedures, accountability, and employee training.[190] These general controls map well to a standardized cybersecurity program.

To fully realize the benefits of an FDA-managed model for the digital health marketplace, the FDA will need to adjust its use of the 510(k) and PMA processes as they apply to digital health products. At least initially, the FDA should consider requiring all Class I and II digital health devices to submit a 510(k).[191] The 510(k) provides a level of additional confidence in products via required disclosures, and the FDA holds discretion over required information disclosed via this process.[192] The FDA could easily incorporate

[184] See FDASIA WHITE PAPER, supra note 125; see also GENERAL WELLNESS, supra note 144.

[185] See Part II, FDCA, and accompanying notes (explaining that although Class I medical devices receive no oversight and health mobile apps do not require compliance with the FDCA, the framework for pre-market disclosures, quality management programs, and post-market obligations matches most product development lifecycles).

[186] See Part II, FDCA, Applicability, and accompanying notes.

[187] See GENERAL WELLNESS, supra note 144.

[188] See Glaser, supra note 9.

[189] John F. Murray, Jr., CDRH Regulated Software, REG. AFF. PROF˘L SOC˘Y 6 (Oct. 2011), http://sterlingmedicaldevices.com/wp-content/uploads/2011/11/jmurray-fdapresentation-softwarerapsindianapolisoctober2011.pdf.

[190] See Part II, FDCA, Medical Device Market Obligations and accompanying notes.

[191] This author notes that a 501(k) is not without cost: in 2014, the average fees were $2,585 for small businesses and $5,170 for large businesses. See Alexander Gaffney, Regulatory Explainer: Why and how is FDA Regulating Mobile Apps? REG. AFF. PROF˘L SOC˘Y (Apr. 15, 2014), http://www.raps.org/focus-online/news/news-article-view/article/4889/. It is recommended that with introduction of Class I devices, average fees could be reduced with comparatively less scrutiny (than Class II devices) and investment of FDA time.

[192] 21 C.F.R. í 807.92 (2016).

a requirement for organizations to disclose details of their cybersecurity risk management programs, including information about the secure development lifecycle included within a quality program and plans for continuing vulnerability management, such as an ability to remotely patch devices or provide hot fixes, or deploy new releases (See Table 3 for examples of Cybersecurity risk management domains typically addressed in security frameworks).[193] This activity would enable the FDA to hold a significant number of organizations accountable to what otherwise is rendered optional.[194]

Class III devices should also require serious inquiry into cybersecurity controls. Although Class III devices do require rigorous testing activities and comprehensive disclosures under the FDCA, these disclosures do not directly include cybersecurity practices.[195] Absent Congressional intervention, the FDA can interpret PMA content requirements under the FDCA to require detailed specification of cybersecurity controls and testing procedures. For example, an organization should disclose device-specific controls and quality process-based controls within the Product Description portion of the PMA.[196] Further, the FDCA requires organizations to disclose deviation both from FDCA performance standards and voluntary standards.[197] The FDA could require organizations to disclose why they chose not to incorporate the NIST security framework, standards, or other applicable standards.[198] Allowing an organization to disclose its cybersecurity approach enables flexibility in choosing which standards are applied while simultaneously ensuring that standards are applied. Although some have proposed the creation of a government-led task force to determine cybersecurity standards; existing

[193] 10 Security Domains, AHIMA HIM BODY OF KNOWLEDGE, http://library.ahima.org/doc?oid=107038#.WBEystUrLIU (last visited Oct. 26, 2016); ISO 27001 Domains, Control Objectives, and Controls, DAN VASILE INFOSEC ADVENTURES & MORE BLOG (Nov. 11, 2011), https://www.pentest.ro/iso-27001-domains-control-objectives-and-controls/; CYBERSECURITY FRAMEWORK (EXCEL), NAT. INST. OF STANDARDS AND TECH., https://www.nist.gov/document-3764 (last visited Oct. 26, 2016).

[194] See Part II, FDA Reports and Cybersecurity Guidance and accompanying notes; See generally James Scott & Drew Spaniel, Assessing the FDA˘s Cybersecurity Guidelines for Medical Manufacturers Why Subtle :Suggestions˜ May Not Be Enough, INST. FOR CRITICAL INFRASTRUCTURE TECH. (Feb. 2016), http://icitech.org/wp-content/uploads/2016/02/ICIT-Blog-FDA-Cyber-Security-Guidelines2.pdf.

[195] 21 C.F.R. í 814.20 (2016). Although Class III devices require submission of clinical trial data as part of the PMA process, a significantly onerous requirement, Class III devices are not required to provide details of security testing, such as code scans, vulnerability scans, or penetration testing results.

[196] 21 C.F.R. íí 814.20(b)(3)¯(4) (2016).

[197] 21 C.F.R. í 814.20(b)(5) (2016).

[198] See Cybersecurity Framework, supra note 126 (describing how many frameworks can be used for cybersecurity purposes, although NIST provides very comprehensive and specific standards for technology).

standards, existing agencies, standard FDA submission procedures, and a willingness to regulate can solve existing digital health marketplace cybersecurity challenges so long as the FDA assumes the responsibility to develop cybersecurity technical competency.[199]

The FDA should also ensure organizations marketing Class II and III devices continuously evaluate marketed devices for potential cybersecurity issues. Organizations with approved or cleared Class II and III devices already have a responsibility to disclose potential safety issues for devices when devices are: 1) designed to be implanted for more than a year, 2) sustain life, or 3) where failure would reasonably have serious adverse health consequences.[200] Based on this direction, the FDA can distinguish between quality activities including routine cybersecurity management, such as upgrades and updates, and emergency fixes or patches resulting from identified vulnerabilities.[201] Information sharing between private organizations and governmental agencies such as the Information Sharing and Analysis Center (ISAC) and the Information Sharing and Analysis Organization (ISAO), will likely include the National Health Information Sharing and Analysis Center (NHISAC) ISAC and the Health Information Trust Alliance (HITRUST) for the health market.[202] These organizations can provide resources for organizations to effectively monitor threats, manage vulnerabilities, and respond to incidents as part of an ongoing quality

[199] See Hagen, supra note 114, 31¯33 (explaining how incorporating the `Least Burdensome Approach_ likely means permitting organizations to exhibit some flexibility in incorporating appropriate standards, yet reviewing the sufficiency of these standards and design prior to market release).

[200] 21 C.F.R. í 822.4 (2016).

[201] See Part II, FDA Medical Device Market Obligations and accompanying notes (describing how class II and III devices require postmarket surveillance); see Guidance for Industry, supra note 135. The FDA has previously specified that patches would not be required because `most software patches . . . reduce the risk of developing a problem associated with a cybersecurity vulnerability and not to address a risk to health posed by the device . . . If the software patch affects the safety or effectiveness of a medical device, you should report the correction to FDA._ Although in most cases, a patch is used to neutralize a vulnerability, it is important to remember that vulnerabilities always pose some risk to a device that is used for health purposes. For example, a patch closes a vulnerability that allows an unverified user to change data in transit between the medical device and the receiver, for example a data analysis application. If data is changed, the data in the analysis is incorrect, and decisions for treatment negatively affecting patient safety could be made; see, e.g., Patricia A.H. Williams & Andrew J. Woodward, Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem, 8 Med. Devices (Auck.) 305 (2015). Ultimately, most, if not all patches will have some bearing on safety of medical devices.

[202] See 21 C.F.R. í 822.4; Exec. Order No. 13636, 80 Fed. Reg. 11739 (Feb. 19, 2013); About Us, Nat˘l Health-ISAC (2016), https://nhisac.org/about-nhisac/; Who We Serve, Health Info. Trust Alliance (2016), https://hitrustalliance.net/ (explaining how class I devices in the digital health marketplace will require ongoing quality measures specific to the function of such devices (e.g. an application is fundamentally different than surgical gloves in that it requires continuous maintenance), not just a standard manufacturing quality process).

management system for Class I devices and pursuant to FDCA post-market surveillance requirements for Class II and III devices.[203]

The FDA will also need to more actively regulate behavior of organizations when information arises regarding organizational non-compliance with the FDCA, as the FDA has interpreted those regulatory requirements. The OCR has taken significant steps to hold HIPAA entities accountable, and the FDA may also need to more rigorously evaluate organizations marketing Class I devices given the comparatively flexible regulatory responsibilities for these devices.[204] Despite less potential for physical injury, Class I devices, like mobile apps, also likely involve processing, transfer, and storage of highly sensitive health information, making them more likely to be a conduit for healthcare fraud.[205] In particular, the FDA can leverage its previous experience prosecuting for violations to the quality system regulation to enforce effective cybersecurity quality measures if the FDA learns of data breaches, failure to patch or remediate devices with known vulnerabilities affecting individual safety or sensitive personal information.[206] Alternatively, the FDA could operate a modified audit process, similar to recent OCR audits, involving self-disclosure or third party certification.[207] While this might require additional budgetary allocation, coupling strong process with strong enforcement would likely preserve maximum flexibility for organizations while creating the necessary stringency to improve cybersecurity for consumers.

CONCLUSION

Although the OCR could provide some level of oversight for the digital health marketplace, the FDA provides the most comprehensive regulatory

[203] 21 C.F.R. í 822.4; NAT˘L HEALTH-ISAC, supra note 202; HEALTH INFO. TRUST ALLIANCE, supra note 202.

[204] Compare Part II, HIPAA OCR Audit Protocol and Oversight and accompanying notes, with Part II, FDA and accompanying notes. In addition, the FDA and OCR may need to coordinate activities and choose when meeting certain requirements will suffice. For example, if a Class II or III device is also regulated by HIPAA, security requirements implemented and validated by the FDA should sufficiently meet the HIPAA Security Rule as well, without additional showing to the OCR.

[205] Jim Finkle, Exclusive: The FBI Warns Healthcare Sector Vulnerable to Cyber Attacks, REUTERS (Apr. 23, 2014), http://www.reuters.com/article/us-cybersecurityhealthcare-fbi-exclusiv-idUSBREA3M1Q920140423.

[206] See, e.g., Federal Judge Approves Consent Decree with Maquet Holding B.V. & Co, U.S. FOOD & DRUG ADMIN. (Feb. 4, 2015), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm432925.htm; FDA Enters Consent Decree with Medtronic, Inc.,U.S. FOOD & DRUG ADMIN. (Apr. 27, 2015), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm444690.htm; Chuck Soder, FDA Identifies More Problems at Invacare Corp., MODERN HEALTHCARE (Jan. 25, 2016), http://www.modernhealthcare.com/article/20160125/NEWS/301259997.

[207] See Part II, HIPAA OCR Audit Protocol and Oversight and accompanying notes.

framework for digital health products and services and is well placed to solve the digital health cybersecurity dilemma. In particular, a broader definition of `medical device_ and compulsory procedures under the FDCA, coupled with FDA oversight and enhanced enforcement will enable the FDA to manage products and services for a wide variety of health market participants.

A corresponding set of cybersecurity requirements, compiled by leveraging an established NIST cybersecurity framework, increases predictability for consumers, healthcare providers, and digital health organizations. The inclusion of such cybersecurity requirements in FDA quality management requirements and 510(k) and PMA processes ensures that products and services cannot enter or remain in the market without implementing minimum cybersecurity controls. Overall, the FDA provides the structure necessary to effectively incorporate a cybersecurity framework and ensure compliance for the digital health marketplace.

Tables and Figures

Table 1: Digital Health Device Type

Reference	Device Type	Device Example
Type A	Implanted Devices (not network-aware, network-aware, application compatible, data storage); includes monitoring devices	Pacemaker
Type B	Non-Implanted Bio Devices (device only, data storage, network-aware)	X-ray Machine
Type C	Wearables (device only, network-aware, data storage)	Heart Rate Monitor
Type D	Mobile App (app only, remote data storage ¯ remote, local data storage)	Remote Clinic App
Type E	Web Application (application only, data storage)	Diagnostic Questionnaire
Type F	General Administrative IT	Patient Intake Software

Table 2: Digital Health Device Type with Cybersecurity Risks

Reference	Device Type	Inherent Risk	Risk Description
Type A (Class II-III)	Implanted Devices (including monitoring devices)	Critical	Network-enabled devices are open to malware or viruses impeding or changing function. Unauthorized users can also launch attacks altering data, commands, or configurations remotely. Loss of personal could also result via remote data storage capabilities.
Type B (Class II-III)	Non-Implanted Bio Devices	High	Network-enabled non-implanted devices are open to malware, viruses, or attacks, many of which would likely result in device inoperability, which could cause patient safety hazards. Loss of personal information could also result remote via data storage capabilities if healthcare providers store medical record numbers or other identifying information in the device.
Type C (Class I-II)	Wearables	Medium	Network-enabled wearables are open to malware, viruses, or attacks that could result in device inoperability. Attacks could alter data reliability, causing unnecessary concern or treatment. Wearables also pose significant concern for loss of personal information due to the connectivity with mobile devices.
Type E (Class I-III)	Mobile App	Medium	Network-enabled mobile devices are open to malware, viruses, or attacks that could result in device inoperability and personal information loss. Thick client mobile apps often function offline, which means that significant data volumes can be stored on a mobile device.
Type D (Class I)	Web Application	Low	Web Applications are subject to well-known threats and vulnerabilities, in particular identity and encryption concerns, leading primarily to organizational risk (e.g. site defacing), personal information loss, and potential malware/virus infection from an organization to a consumer˜s computer.
Type F (Class I)	General Administrative IT	Medium	Administrative software can process and store significant volumes of personal information for employees and patients, which can be subject to personal information loss, data integrity issues (such as deletion, addition, or change of critical patient information) resulting in incorrect patient treatment. Ransomware and other data availability attacks could cause patient data to be unavailable during critical treatments.

Table 3: Cybersecurity Domains

Cybersecurity Domain	Quality Management Example
Organizational Responsibility	Designate and document a management-level individual responsible for cybersecurity; implement policies and procedures; train employees.
Risk Governance	Review, document, and record risk decisions when non-compliant with internal policies and procedures.
Encryption	Document and use processes for determining when encryption will be used and acceptable methods, protocols, and key management approaches.
Identity and Access Management	Document and use processes for determining specific identity and access technology selections appropriate to technology (e.g. biometric scanning, two-factor authentication).
Secure Development Program	Document and use process for designing architectures and systems securely and taking into account privacy principles; develop a repository of technology-specific requirements for enterprise technologies used.
Threat and Vulnerability Management	Document and use a process for gathering threat intel to anticipate potential vulnerabilities or data exposure. Document a process for identifying vulnerabilities and appropriate remediation timeframes.
Asset Management	Implement an asset management system and include information about technologies used internally, implemented in systems or products, third party status, and configuration information.
Third Party Management	Document and use third parties providing equipment, infrastructure, or services. Routinely assess third parties are following organization processes and procedures and ensure compliance through standard contractual provisions.
Integrity Monitoring	Document and use processes and technologies for ensuring data and device function integrity, such as file integrity monitoring or similar technologies.
Incident Response and Data Breach Notification	Document, test, and use routine processes and procedures for detecting potential incidents, such as intrusion prevention or detection systems, internal forensic procedures, information sharing models, playbooks and processes, incident response team and draft notification language.
Network Management	Document and implement secure network technologies and include appropriate use of firewalls, firewall management systems, DMZ, data loss prevention tools, and network segmentation.
Business Continuity and Disaster Recovery	Document, test, and use processes for determining system priority and expected uptime/downtime requirements. Document, test, and use processes for managing disaster situations, including appropriate recovery procedures, emergency operation, and storage of disaster recovery plans.
Retention, Archive, Deletion	Document, test, and use appropriate retention requirements according to data stored; archive and delete data securely. Ensure ability to ensure data can be deleted in all systems as appropriate.