THE NECESSITY FOR FEDERAL ORGANIZATIONS TO ENSURE PROPER PRIVACY AND SECURITY COMPLIANCE OF MOBILE HEALTH CARE APPLICATIONS

Julia Gonsalves

I. Introduction

In 2007, the first iPhone was released and possessed a series of general applications that were extremely modern for a handheld device.[1] Consumers were able to text on a touch-screen keyboard and have access to a handheld calendar, but originally, Steve Jobs did not envision the iPhone containing third-party applications because he felt that his team would not be able to figure out the major complexities when developing policies with third parties application developers.[2] As technology has evolved over the past decade, with now over 77% of United States adults owning a smart-phone, these once unimaginable third-party applications have become a part of everyday life.[3]

1 *See* Dan Grabham, *History of the iPhone 2007-2017*, T3 (Sept. 8, 2017), *archived at* https://perma.cc/R3PA-PMKM (reflecting on the progression of iPhone technology and how the creation of the iPhone allowed for access to advanced computer-like capabilities with a touch of a button). When first developing the iPhone, Steve Jobs stated that Apple was going to "reinvent the phone," but he did not necessarily convey that to include third-party applications, GPS, or video recording in the first iPhone version. *Id.*

2 *See Jobs' Original Vision for the iPhone: No Third-Party Native Apps*, 9TO5MAC (Oct. 21, 2017), *archived at* https://perma.cc/F5UY-A5KR (positing the "hacking community" would tinker with the Apple Application store, which eventually led to the more advanced development of iPhone software). The iPhone software began to develop kits for third-party application developers to make it possible for certain applications to be sold on the Apple Application store. *Id.*

3 *See* Aaron Smith, *Record Shares of Americans Now Own Smartphones, Have Home Broadband*, PEW RESEARCH CENTER (Jan. 12, 2017), *archived at*

ISSN 1536-7983.

Healthcare-focused mobile-phone applications (mHealth applications) have become one of the most popular types of third-party applications used by clinicians and patients in the United States.[4] Certain mHealth applications have become so advanced that the applications are able to be implemented world-wide, in resource-constrained countries, and have the means to improve health outcomes, deliver healthcare services, enable healthcare-based research and allow clinicians to communicate more efficiently about a specific patients healthcare plans based on individual needs.[5] Woven between all of the common fitness and dietary mHealth applications, there are a variety of mHealth applications that allow for a patient's private health information ("PHI") to be transmitted electronically between clinicians and patients.[6] A

https://perma.cc/HA35-ERS4 (evaluating the use of smartphones between different age groups, and the incline of smartphone usage in older and lower income Americans); *see also* Monica Anderson & Andrew Perrin, *Technology Adoption Climbs Among Older Adults*, PEW RESEARCH CENTER (May 17, 2017), *archived at* https://perma.cc/CK9X-JXVX (noting that "roughly half of older adults who own cellphones have some form of smartphone"); *see also* Deborah Estrin et al., *Diversity in Smartphone Usage*, MOBILESYS, 185-86 (2010) (analyzing the different patterns of usage for communication, browsing, media, productivity, and system smartphone applications).

4 *See* Robert S.H. Istepanian et al., *mHealth: Emerging Mobile Health Systems* (1st ed. 2006) (explaining that mHealth applications are a new source of technology that will be cost-effective and efficient for communicating health information).

5 *See* Richard Pankomera & Darelle van Greunen, *A Model for Implementing Sustainable mHealth Applications in a Resource-constrained Setting: A case of Malawi*, E.J. INFO. SYS. DEV. COUNTRIES (2018) (establishing that mHealth applications are rapidly transforming the delivery of healthcare service across the globe and have assisted with the management of chronic illnesses). The benefits of establishing mHealth applications in under-developing portions of the world include clinicians being able to communicate more effectively and more often with their patients, without having to pay for costs of travel. *Id.*; *see also* David W. Bates et al., *In Search of a Few Good Apps*, 311 [J]AMA 1851, 1851 (2014) (noting that mHealth applications are appealing to patients because applications are inexpensive, and can be used to promote wellness and manage chronic diseases). However, it is difficult for clinicians and consumers to determine which mHealth application is the safest and most effective due to the high volume of applications that have been introduced to the public. *Id.*

6 *See Mobile Medical Applications*, FOOD & DRUG ADMIN. (Sept. 22, 2015), *archived at* https://perma.cc/6KTQ-DVQ4 (providing that mHealth applications can be used for a variety of simple tasks such as allowing patients to monitor their caloric intake or the effects of bottle feeding an infant). Other mHealth applications "aim to help health care professionals improve and facilitate patient care. *Id.* The type of care that can be

variety of federal organizations participate overseeing the development and usage of mHealth applications in order to ensure that PHI is protected is properly transmitted electronically.[7] Specifically, the United States Food and Drug Administration ("FDA")[8], Office of Civil Rights for Health and Human Services ("OCR")[9], and the Federal Trade Commission ("FTC")[10], evaluate and monitor certain mHealth applications purpose, procedure, and policies to ensure that developers comply with the Health Insurance Portability and Accountability Act ("HIPAA") and additional federal laws.[11]

provided when accessing specific patient information may include physicians being able to diagnose and treat radiation injuries, diagnose cancer or heart rhythm abnormalities, or function as the "central command" for a glucose meter for an individual with diabetes. *Id.*

7 *See* Y. Tony Yang & Ross D. Silverman, *Mobile Health Applications: The Patchwork of Legal and Liability Issues Suggests Strategies to Improve Oversight*, 33 EARLY EVIDENCE, FUTURE PROMISE OF CONNECTED HEALTH 2 (2014) (asserting that there are five federal agencies that are likely going to play a role in the regulation of mHealth applications). The five federal agencies include: The National Institute of Standards and Technology, the Federal Communications Commission, the Office for Civil Rights of the Department of Health and Human Services, the Federal Trade Commission, and the Food and Drug Administration. *Id*.; *see, e.g. See Mobile Devices Roundtable*, HEALTHITBUZZ (Apr. 4, 2012), *archived at* https://perma.cc/6YZK-A3TB.

8 *See Mobile Medical Applications*, *supra* note 6 (explaining that the FDA takes a "tailored, risk-based approach" to regulate a small subset of mHealth mobile applications that meet the definition of a medical device, and are intended to be used as an accessory to a regulated medical device *or* transform a mobile platform into a regulated medical device).

9 *See Resources for Mobile Health App Developers*, U.S. DEP'T OF HEALTH & HUM. SERV. (June 16, 2017), *archived at* https://perma.cc/B9E3-SN9Z (recognizing that it is important to build privacy and security protections for technology products to ensure that private health information is appropriately disclosed).

10 *See* HIPAA Journal, *Do Your HIPAA Authorizations Violate the FTC Act?*, U.S. DEP'T OF HEALTH & HUM. SERV. (Oct. 25, 2016), *archived at* https://perma.cc/M5F8-D7EU (affirming that the FTC prevents organizations from "engaging in deceptive practices in or affecting commerce" and evaluates mHealth applications to ensure that patients and consumers are aware of the trade practices occurring with a particular mHealth application).

11 *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1171, 110 Stat. (1996) [hereinafter *HIPAA*] (asserting that HIPAA only applies to health care providers, health plans, and health care clearing houses). A health care clearing house means "a public or private entity that processes or facilitates the

This Note will analyze how the FDA, OCR, and FTC must become more unified in order to ensure that mHealth applications are successful in completing electronic transactions of PHI while simultaneously complying with federal privacy regulations and statutes. Section II of this Note will discuss the evolution of mHealth applications, illustrate how helpful these applications can be for patients and clinicians, and explain the FDA's, OCR's, and FTC's current guidance plans that help regulate mHealth applications. Section III will identify the privacy and security concerns with mHealth applications due to manufacturers being unaware of the federal organization regulations and describe the types of civil penalties that can be imposed on entities that violate federal law. Section IV will examine the how the FDA, OCR, and FTC's guidance plans are not ideal for mHealth application manufacturers and analyze how the federal organizations can create a cohesive team that would only serve to evaluate mHealth applications. Section V will predict there would be less PHI exposure concerns and HIPAA violations for patients and clinicians if the FDA, OCR, and FTC were to create a specialized team to analyze mHealth applications.

II. History

In 2009, the American Recovery and Reinvestment Act of 2009 was created as a push for the United States to promote economic recovery by creating technological advances in science and health.[12] As

processing of nonstandard data elements of health information into standard data elements." *Id*.

12 *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 177 (2009) (explaining the Act provided an investment for the Secretary of Health and Human Services to allocate money towards different research projects regarding health care treatments and strategies). The Act's goal was to encourage the development and use of electronic health data. *Id*. at 177. The Act designates the National Coordinator for Health Information Technology, who has specific duties such as improving health care quality and ensuring that each patient's health information is secure and protected, as the point person of the Health Information Technology policy and standard committees. *Id*. at 230-31. The HIT policy committee makes recommendations regarding the privacy of health information, promotes security of electronic health records, and utilizes electronic health records for each person in the United States. *Id*. at 234. The HIT standard committee makes recommendations to improve certification criteria for the electronic exchange and use of health information. *Id*. at 237.

a result, there was a massive creation of mHealth applications, which are healthcare related smartphone software programs that target both clinicians and patients.[13] Dr. Kevin Patrick, a professor of preventative medicine at the University of California, San Diego, and two partners were among some of the first mHealth application developers at Santech, Inc. in 2011.[14] Santech, Inc. was a for-profit business that used basic SMS text messages and incentives to encourage participants to eat healthier food, quit smoking, and exercise.[15] Just two short years later, in 2013, approximately 43,700 health or medical applications were available on Apple's iTunes store that initially had a "simple design and do little more than provide information."[16] MHealth application development continued and by March of 2017 the amount of applications were almost quadruple the amount in 2013, totaling at 165,000 mHealth applications that allowed overarching opportunities to enhance medical care for individual patients and had large public health

13 *See Mobile Medical Applications*, *supra* note 6 (defining mHealth, applications as software programs that can run on smartphones or mobile communication devices and help track and regulate different types of health care information "by using attachments, display screens, or sensors"); *see also* Joseph Conn, *No Longer a Novelty, Medical Apps are Increasingly Valuable to Clinicians and Patients*, MOD. HEALTHCARE (Dec. 14, 2013), archived at https://perma.cc/B7ZW-NYUF (announcing that mHealth applications have become so common that patients will likely leave a doctor's office with discharge instructions on how to download mHealth applications to access prescriptions).

14 *See* Susan Buie, *The mHealth Movement: Mobile Apps and the Rise of Portable Care*, THE ATLANTIC (Jan. 29, 2014), *archived at* https://perma.cc/79EX-GE6E (indicating that starting in 2006, Dr. Patrick's studies determined that customized text messages were effective in driving desirable behavior, such as reminding individuals to take medication and exercise regularly).

15 *See id.* (highlighting that Santech, Inc.'s purpose was to encourage patients to participate in healthy habits, and that "the results are positive" overall). Published studies further indicate that text messages provide support for the management of chronic diseases. *Id*. Dr. Patrick expected that the mHealth application market would grow past SMS text reminders and said that the "simplicity and ease of text messaging can be considered baby steps towards increasingly sophisticated care delivery using mobile devices." *Id*.

16 *See* Conn, *supra* note 13 (stating that in 2013, 69% of mHealth applications targeted patients, while 31% of mHealth applications were built for clinicians). There was extreme room for growth in the mHealth application development market because there were not many applications that could track or capture user-entered data, or relate to condition management tools. *Id*.

impact.[17] The development of mHealth applications has been increasingly encouraged.[18] It is anticipated that there will be a compound annual growth rate of 43.6% between 2013 and 2019 of the mHealth application market, thereby reaching a market value of $8.03 billion dollars.[19]

Since their inception, the exponential growth of mHealth applications has created a movement for both consumers and health care providers.[20] Provider-focused mHealth applications allow providers to access PHI during a patient visit, monitor and follow up with patients using GPS technology, and allow clinicians to generate e-questions about a patient's well-being at any time.[21] Additionally, mHealth

17 *See* Catherine J. O'Shea et al., *Mobile Health: An Emerging Technology with Implications for Global Internal Medicine*, 47 INTERNAL MED. J. 616, 616-17 (2017) (asserting that mHealth activity has global barriers because of the availability and affordability of mHealth, as well as lack of education). The use of mHealth activity is greater in high-income countries. *Id*. at 617; s*ee also* Press Release, *A.G. Schneiderman Announces Settlement with Three Mobile Health Application Developers for Misleading Marketing and Privacy Practices*, N.Y. OFF. OF THE ATTY. GEN. (Mar. 23, 2017), *archived at* https://perma.cc/4XGP-QEDS (describing the increasing popularity of mHealth applications in recent years due to consumer access to general medical advice and education).

18 *See Mobile Medical Applications*, *supra* note 6 (offering that mHealth applications are being utilized at an exceedingly fast rate and predicting mHealth application use will continue to grow, as smartphone use increases); *see also Healthcare Mobile App Development and mHealth Apps in 2017*, ADORIASOFT (Apr. 21, 2017), *archived at* https://perma.cc/SSN6-66PV (reporting that the largest market for mHealth applications is currently the United States because of the progressive connection through 3G and 4G networks). By 2022, the global market for mHealth applications is projected to reach $102.43 billion. *Id*.

19 *See Global mHealth Monitoring and Diagnostic Medical Devices to be Fueled By High Incidence of Chronic Diseases: Transparency Market Research*, BUS. WIRE (Apr. 23, 2015), *archived at* https://perma.cc/7QEE-9XA8 (asserting that the mHealth application use and market is growing, which may significantly decrease the amount of health care spending in the United States by $200 billion over the next 25 years); *see also Healthcare Mobile App Development and mHealth Apps in 2017*, *supra* note 18 (predicting that by 2018, 50% of the 3.4 billion smartphone users will have downloaded some type of mHealth application).

20 *See Mobile Health Apps*, ATHENAHEALTH (2017), *archived at* https://perma.cc/T7UR-BYE2 (explaining the "eHealth" movement includes patients and providers using computers and mobile phones to access health care information).

21 *See Clinicians and Mobile Health*, ATHENAHEALTH (2018), *archived at* http://perma.cc/G2SV-ERUD (reporting that in 2014, 83% of physicians said that they used some type of mobile healthcare to provide patient care and view documents, but

application developers have created patient portals that grant providers the ability to electronically provide test results, prescription refills, and medical records directly to a patient's phone.[22] Remarkably, patient portals have allowed for providers to connect to remote devices in patient's bodies to survey patients' health; for example, patients who have cardiovascular implantable electronic devices.[23] By contrast, patient-focused mHealth applications have allowed patients to: 1) manage chronic diseases and disorders, such as blood pressure and mental health;[24] 2) maintain healthcare and fitness by keeping track of their daily caloric intake;[25] 3) take medication and keep track of the dosages;[26] and 4) store personal health care information about medical conditions and share records with their doctors.[27]

---

only one-third of clinicians had electronic health records integrated with the mobile health care tools).

22 *See Mobile Health Apps*, *supra* note 20 (describing how patient portals make it easier for clinicians to provide PHI to patients); *see also Clinicians & Mobile Health*, *supra* note 21 (noting that mHealth applications allow providers to directly communicate with patients by texting or sending secure emails). By using mHealth applications, providers can stay directly in touch with high-risk patients. *Id*.

23 *See* O'Shea et al., *supra* note 17, at 616-17 (highlighting that providers have the ability to detect heart failure in a patient early by observing a patient's thoracic impendence and left atrial pressure).

24 *See* David Mohr, *Highlight: A Therapist in One's Pocket: mHealth to Improve Access to Mental Health Care*, NAT'L INST. OF MENTAL HEALTH (2017), *archived at* https://perma.cc/8QYQ-GWDJ (noting a large disparity between the demand for and the delivery of medical and therapy services because of the cost, patient's inability to access mental health services, and resistance to seeing a mental health professional).

25 *See* Zubin J. Eapen et al., *An Evaluation of Mobile Health Application Tools*, 2 JMIR MHEALTH UHEALTH 19, 21 (2014) (observing that a study of mHealth applications found those available on iTunes, fitness, and wellness applications were the most popular). Fitness and training applications are intended to improve physical fitness and provide consumers with training and gym plans. *Id*.

26 *See* Brad E. Dicianno et al., *iMHere: A Novel mHealth System for Supporting Self-Care in Management of Complex and Chronic Conditions*, 2 JMIR MHEALTH UHEALTH 10, 17 (2013) (affirming that clinicians can use a portal to make a treatment plan and remind patients to take medication).

27 *See Healthcare Mobile App Development and mHealth Apps in 2017*, *supra* note 18 (providing an overview of the types of mHealth applications currently available to consumers); *see also* Eric Wicklund, *mHealth Study Ties App to Improved Outcomes for Pregnant Women*, MHEALTH INTELLIGENCE (Aug. 1, 2017), *archived at* https://perma.cc/GC3G-74AM (explaining that pregnant women who used the mHealth

A. The Food and Drug Administration

Beginning in February of 2001, the United States Food and Drug Administration was designated as the federal body in charge of regulating mHealth applications because, among a variety of tasks, the FDA is responsible for regulating equipment or software intended to diagnose or treat diseases or other health conditions.[28] The FDA developed a guidance plan in September of 2013 that provided non-binding recommendations to individuals who were developing mHealth applications and informed manufacturers that the FDA would only be regulating mHealth applications that are categorized as "medical devices"[29] under the definition provided by the Federal Food, Drug, and Cosmetic Act.[30] An mHealth application is defined as a medical device

app called WYhealth Due Date Plus were 76% more likely to schedule prenatal visits before delivery). This particular mHealth app also connects women to clinical information regarding specific pregnancy symptoms. *Id*. Also, WYhealth positively affected the outcomes in population health programs and "points to the value of a digital health program in a rural area like Wyoming where physicians are scarce and patients are likely to face access issues." *Id*.

28 *See* BAKUL PATEL, MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF, U.S. FOOD & DRUG ADMIN. 6 (Feb. 9, 2015) (providing the history of FDA regulation of these medical devices). The FDA decided to regulate mHealth applications that fell within the definition of a "medical device" because of certain risks that could be posed to the public. *Id*. Also, the FDA affirms that Congress has appointed the FDA to review device applications to ensure safety and effectiveness. *Id.*; *see also mHealth Laws and Regulations*, CTR. FOR CONNECTED HEALTH POL'Y (2017), *archived at* https://perma.cc/DT5Y-79GS (setting forth the FDA's role in regulating mHealth applications).

29 *See What We Do*, U.S. FOOD & DRUG ADMIN. (Apr. 4, 2017), *archived at* https://perma.cc/4CU3-KT4C (summarizing the FDA's overall mission as protecting public health and increasing safety and efficiency regarding "human and veterinary drugs, biological products, and medical devices."); *see also* PATEL, *supra* note 28, at 9 (asserting the FDA is using the guidance document to clarify which mHealth applications will be regulated by the FDA). The FDA does not regulate mHealth applications that fall outside of the definition of "medical devices" under section 201(h) of the Federal Food, Drug, and Cosmetic Act. *Id*. Also, the FDA asserts discretion to monitor certain mHealth applications if the applications pose a lower risk to the public, even though the applications are within the definition of a "medical device." *Id*. The FDA will only regulate mHealth applications that are considered "medical devices" and "whose functionality could pose a risk to a patient's safety." *Id.*

30 *See* Federal Food, Drug, and Cosmetic Act, 21 U.S.C § 321 (2018) [hereinafter *FD&C Act*] (creating the FDA's power to regulate the safety of food, drugs, and

if it is "intended to be used as an accessory to a regulated medical device," or "transforms a mobile platform into a regulated medical device."[31] The FDA updated the 2013 guidance plan in 2015 to specify and delineate the subset of mHealth applications that are subject to FDA regulatory oversight.[32] The broad categories of mHealth applications are under the watch of the FDA include: 1) having a purpose of controlling devices for use in active patient monitoring or analyzing medical device data;[33] 2) the display of screens or sensors that have specific medical functions similar to currently regulated medical devices;[34] and 3) having a patient-specific analysis and provide patients

cosmetics). In 1931 the term "device" meant "instruments, apparatus, and contrivances, including their components, parts, and accessories, intended 1) for the use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man or other animals; or 2) to affect the structure or any function of the body of man or other animals." *Id.*; *see also* 21st Century Cures Act, Pub L. No. 114-225, 130 Stat. 1033 (2016) (redefining the term "device" to exclude certain software functions); *see also 21st Century Cures Act*, U.S. FOOD AND DRUG ADMIN. (Sept. 14, 2017), *archived at* https://perma.cc/8L57-G5N9 (stating the purpose of the 21st Century Cures Act is to help accelerate medical product development and work closely with the FDA to incorporate the perspectives of patients into the decision-making process of medical products).

31 *See Mobile Medical Applications*, *supra* note 6 (providing the FDA definition of mHealth applications that are a "medical device" and, therefore, subject to FDA regulation).

32 *See* PATEL, *supra* note 28, at 13 (describing the FDA's limited approach to regulating mHealth applications as focusing on those able to transform a mobile platform into a "regulated medical device by using attachments, display screens, sensors," or other such methods). The FDA may regulate mHealth applications that are considered to be an accessory to a device that is used to gather medical information. *Id*. The FDA may regulate mHealth applications that analyze or interpret data that is electronically collected or manually entered. *Id*.

33 *See* PATEL, *supra* note 28, at 15 (noting the FDA can regulate mHealth applications that monitor a patient for heart rate variability from a signal produced by an electrocardiography because certain display attachments transform the mobile platform).

34 *See* PATEL, *supra* note 28, at 6 n.3 (asserting the FDA can regulate mHealth applications that are considered to be an accessory to a device that is used to gather medical information and mHealth applications that analyze or interpret data that is electronically collected or manually entered).

with specific diagnosis or treatment recommendations due to the access of PHI.[35]

The FDA recommendations do not specify broad categories of mHealth applications that can be used safely by a patient without active oversight by a medical professional or are not intended to provide specific treatment recommendations.[36] Additionally, the FDA guidance plan also generally provides for mHealth applications that the FDA intends to exercise enforcement discretion over, meaning that the FDA may not regulate mHealth applications that are considered medical devices if the application provides for a low-risk against patients.[37] Manufacturers of mHealth applications must be aware if their product needs to comply with FDA regulations and must disclose that the mHealth application is not regulated by the FDA.[38] If the mHealth application is considered a medical device, then developers, as a third-party business associate, must comply with the HIPAA and other necessary federal statutes, and notify consumers that the mHealth application complies with FDA standards.[39]

---

35 *See* PATEL, *supra* note 28, at 15 (describing that the mHealth applications that the FDA intends to regulate are those that are able to transform a mobile platform into a "regulated medical device by using attachments, display screens, sensor, or other such methods).

36 *See* PATEL, *supra* note 28, at 20-2 (providing a non-exhaustive list of examples of mHealth applications that the FDA will not regulate because the applications are not defined as a "medical device").

37 *See* PATEL, *supra* note 28, at 16-18 (providing examples of mHealth application manufacturers that subject to FDA regulations).

38 *See* PATEL, *supra* note 28, at 10 (demonstrating that manufacturers of mHealth applications must be aware that the FDA has regulation authority when a mHealth application has hardware attachments for a mobile platform or creates a software system that provides users access to the medication device function through a website subscription or software as a service); *see also A.G. Schneiderman Announces Settlement with Three Mobile Health Application Developers for Misleading Marketing and Privacy Practices*, *supra* note 17 (reporting the New York Attorney General settlement with three mHealth application manufacturers requires these manufacturers to amend statements making clarifying for consumers that these specific mHealth application products are not regulated by the FDA).

39 *See* HIPAA Journal, *supra* note 10 (providing individuals with specific rights to their health information and requiring health providers must follow certain rules when disclosing patient's private health information); *see also To Whom Does the Privacy Rule Apply and Whom Will it Affect*?, U.S. DEP'T OF HEALTH & HUM. SERVS. (Feb. 2, 2007*), archived at* https://perma.cc/JZZ6-XSMT (requiring the following entities

B. Office of Civil Rights for Health and Human Services

In addition to the FDA's efforts towards regulating mHealth applications, the Civil Rights Health and Human Services Office ("OCR") continues to aim to protect patient's fundamental rights when it comes to electronically transmitting private health information.[40] After HIPAA's original enactment in 1996, Congress began to make amendments to HIPAA once recognizing that electronic technology could negatively impact the privacy of healthcare information.[41] Beginning in the early 2000's, Congress incorporated the Privacy Rule[42] and Security Rule[43] into the HIPAA provisions, which furthered the

to comply with HIPAA: "health plans, health care clearinghouses, and health care providers who electronically transmit any health information"). Additionally, the privacy rule protects individual's identifiable health care information that is in the possession of a third party who acts on behalf of covered entities. *Id*.

40 See *About Us*, OFF. OF CIV. RTS. (Sept. 6, 2015), *archived at* https://perma.cc/VNT4-ACGH (describing OCR's efforts to protect PHI by educating health care and social service workers about safety confidentiality laws).

41 *See* Health Information Technology for Economic and Clinical Act, 111 Pub. L. No. 111-5, 123 Stat. 227 (2009) [hereinafter *HITECH Act*] (explaining that the HITECH Act was included in the American Recovery and Reinvestment Act of 2009 to promote the use of electronic health records to improve quality, safety, and efficiency of public health care); *see also HIPAA for Professionals*, OFF. OF CIV. RTS. (June 16, 2017), *archived at* https://perma.cc/2GGMQ8H6 (setting forth the belief that HIPAA needs to keep up with technology advancements to ensure that patient's PHI is protected); *see also Meaningful Use Definition & Objectives*, HEALTHIT (Feb. 6, 2015), *archived at* https://perma.cc/AKB6-E3RB (articulating the goal of utilizing electronic health records is to provide better clinical outcomes, increase efficiency of public health, and improve population health outcomes). The purpose of HITECH Act was to promote and expand the usage of technology regarding electronic health care records. *Id*.

42 *See* Definitions, 45 C.F.R. § 160.103 (indicating that the Privacy Rule standards apply to health care covered entities that have access to patient private health information); *see also Summary of the HIPAA Privacy Rule*, OFF. OF CIV. RTS. (Jul. 26, 2013), *archived at* https://perma.cc/RQ3U-7ETJ (proposing the goal of the Privacy Rule is to assure that individual's health information is properly protected while "health plans, health care providers, and business associates are able to promote a high quality of healthcare").

43 *See* The Security Rule, 45 C.F.R. §§ 160, 164 (2003) (asserting that the Security Rule was established because Health and Human services needed to take into "account the technical capabilities of record systems used to maintain health information" and ensures for a technical safeguard against the integrity and confidentiality of PHI that

requirements of privacy protections for individually identifiable health information.[44]

In accordance with the Privacy and Security Rules of HIPAA, the OCR created effective guidelines for mHealth application developers to ensure that PHI is secure when using smartphones.[45] Deven McGraw, the OCR Deputy Director for Health Information Privacy, stated that if a developer is creating a mHealth application that "involves the use or disclosure of identifiable information" and or is a business associate that works on behalf of an entity that is covered by HIPAA, then the mHealth application must comply with HIPAA standards.[46] Congress furthered the desire in wanting to protect PHI and put into effect the Enforcement Final Rule of 2006, which gives the Office of Civil Rights the power to issue financial penalties or corrective action plans to work with entities that fail to comply with HIPAA.[47]

could be compromised); *see also Summary of the HIPAA Security Rule*, OFF. OF CIV. RTS. (Jul. 26, 2013), *archived at* https://perma.cc/FQL7-8MZL (explaining that the Security Rule requires measures to be taken to protect the integrity, confidentiality, and availability of electronic PHI that is held or transmitted by covered entities). The HITECH Act "expanded the responsibilities of business associates under the HIPAA Security Rule." *Id.*

44 *See* The Enforcement Rule, 45 C.F.R. § 160.400 (2006) (designating that HIPAA does not specify how to protect privacy or transmit health records efficiently or effectively). However, HIPAA authorizes the Secretary of Health and Human Services to adopt administrative standards that will allow for electronic PHI to be transmitted in accordance with HIPAA's Privacy Rule. *Id.*; *see also HIPAA for Professionals*, *supra* note 41 (stating the Administrative Simplification provisions require the Department of Health and Human Services to "adopt national standards for electronic health care transactions" and security).

45 *See* Rajindra Adhikari & Deborah Richards, *Security and Privacy Issues Related to the Use of Mobile Health Apps*, UNIV. OF SYDNEY AUSTL., 1, 3 (2014) (indicating that the OCR suggests that the guidelines for mHealth app developers 1) know the risk; 2) take the steps; and 3) protect and secure health information).

46 *See* Rajiv Leventhal, *OCR Releases HIPAA Guidance For mHealth App Use*, HEALTHCARE INFORMATICS (Feb. 19, 2016), *archived at* https://perma.cc/5LZ2-MM4N (discussing when developers must comply with HIPAA's Privacy Rules).

47 *See* 45 C.F.R. § 160.400 (asserting that imposing civil money penalties on covered entities or business associates for HIPAA violations will be mandated by the Secretary of Public Welfare).

C. The Federal Trade Commission

The Federal Trade Commission ("FTC") has joined the FDA and OCR in overseeing mHealth applications by having the essential role of regulating mHealth applications that have made potentially false claims about their effectiveness to consumers.[48] The FTC works with HIPAA-covered entities to ensure that patients receive full authorization, in plain language, for the release of any electronic-PHI ("ePHI").[49] The FTC has required that a HIPAA-covered entity must have valid a business associate agreement that provides for the terms and disclosure provisions when transmitting electronic PHI.[50]

---

48 *See* Definitions, 16 C.F.R. § 318.2 (2017) (defining the FTC's process of informing patients when their electronic personal health record (PHR) was accessed without authorization). A person's PHR is defined as "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." *Id*.; *see also* Federal Trade Commission Act, 15 U.S.C. § 45 (1914) (defining the FTC's primary purpose as protecting consumers from deceptive acts or practices, and false or misleading claims).

49 *See* FTC v. Medical Billers Network, Inc., 543 F. Supp. 2d 283, 318 (S.D.N.Y. 2008) (holding that the defendants violated section 5 of the FTC Act because the defendant misrepresented conditions to the third-party purchasers); *see also Do Your HIPAA Authorizations Violate the FTC Act*?, *supra* note 10 (affirming position that the FTC prevents organizations from "engaging in deceptive practices in or affecting commerce"). It is possible for a covered entity under HIPAA to comply with the HIPAA regulations and still violate the FTC Act. *Id*. In order for patients to give full consent as to the disclosure of their health information, patients must be informed as to what of their PHI will be released, why their information is going to be shared, and what will happen to their PHI after information has been shared. *Id.; see also Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM'N (Apr. 2016), *archived at* http://perma.cc/CUM7-VEYQ (recommending several best practices for manufacturers developing mHealth applications in order to comply with the FTC Act).

50 *See* 45 C.F.R. § 160.103 (2017) (providing that "business associates" includes Health Information Organization, E-prescribing Gateway, or another person that provides data transmission services with respect to protected health information to a covered entity). An example of a business associate for a HIPAA-covered entity would be "a person that offers a personal health record to one or more individuals on behalf of the covered entity." *Id.* at § 160.103(4)(ii)(3)(ii); *see also Business Associate Contracts*, U.S. DEP'T OF HUM. HEALTH (June 16, 2017), *archived at* https://perma.cc/ZS98-ESLC (providing examples of business associate provisions where the organization's goal is to ensure that all parties comply with HIPAA and breach notification requirements); *see also Do Your HIPAA Authorizations Violate the FTC Act*?, *supra* note49 10 (stating that a business associate cannot get authorization

Specifically in regards to mHealth applications, the FTC has noted that third parties have previously transmitted sensitive health information carelessly and declared jurisdiction over claims that are focused against the developer's statements of the applications effectiveness.[51] To ensure that manufacturers of mHealth application comply both with the FTC and HIPAA regulations, the FTC produced a similar guidance document in conjunction with the OCR and FDA, as well as the Department of Health and Human Services' Office of National Coordinator for Health Information Technology ("ONC"), which offers non-binding recommendations as to how manufacturers should implement data security.[52] The FTC also developed a Mobile Health Apps Interactive Tool that allows mHealth application developers to ask series of questions that help determine what federal laws the applications must comply with.[53] Ultimately, the goal of the FTC is to ensure manufacturers of mHealth applications do not forgo regulations and do not disclose patient information that is protected.[54]

from a patient or health plan member if the business associate agreement does not permit release a patient's ePHI).

51 *See mHealth Laws and Regulations*, *supra* note 28 (noting that there can be an overlap of the FDA, FTC, and Federal Communications Commission ("FCC") when regulating mHealth apps); *see also* Yang & Silverman, *supra* note 7, at 4 (predicting that if electronic health care information is not regulated properly by the FTC, then consumers may begin to lose trust in the mobile marketplace).

52 *See FTC Releases New Guidance for Developers of Mobile Health Apps*, FED. TRADE COMM'N (Apr. 5, 2016), *archived at* https://perma.cc/3LNK-Y3FN (clarifying that the FTC guidance tool allows mHealth application developers to comply with the FTC Act, by building privacy and security into their apps).

53 *See Mobile Health Apps Interactive Tool*, FED. TRADE COMM'N (Apr. 2016), *archived at* https://perma.cc/3AY9-8ZPQ (providing ten questions to mHealth app developers to help determine what federal laws the mHealth app needs to comply with). The questionnaire looks to what the mHealth application is intended for, if there are minimal risks for consumers when using the app, and if the mHealth app is being developed on behalf of a covered entity under HIPAA. *Id*.

54 *See FTC Releases New Guidance for Developers of Mobile Health Apps*, *supra* note 52 (focusing on FTC requirements that mHealth app developers must consider and suggest that developers should have a strong encryption security to protect patient data); *see also* Ali Sunyaev et al., *Availability and Quality of Mobile Health App Privacy Policies*, OXFORD ACAD. (Aug. 21 2014), *archived at* https://perma.cc/4C5X-RW8B (pointing out the FTC encourages application developers to provide privacy policies and disclosures requesting consent to collecting formation).

III. Facts

MHealth applications have been acknowledged for their ability to allow patients to play an interactive role in their own health and for physicians to relay health information to patients within seconds.[55] Cell phones have the capacity to store an incredible amount of personal identifiable data, making it possible to have "several interrelated privacy consequences."[56] Because of the risk of exposing sensitive patient information can be so destructive, both physicians and patients are concerned about privacy, security, and licensure of mHealth applications.[57]

Congress has continuously had the interest of keeping PHI confidential and has acknowledged that there are substantial risks in carelessly transmitting data by way of different technologies.[58]

---

55 *See mHealth: New Horizons for Health Through Mobile Technologies*, WORLD HEALTH ORG. (2011), *archived at* https://perma.cc/MYX9-M9TA (highlighting the different types of mHealth applications that allow patients to monitor their own health through their own choices). The World Health Organization has developed the initiative with the goal of getting mHealth applications into lower income countries. *Id*. Developed countries possess the highest rate of programs enabling the accessibility to electronic medical records, which is most likely due to widespread internet access. *Id*.

56 *See* Riley v. California, 134 S. Ct. 2473, 2478-79 (2014) (describing that there is a substantial privacy interest when digital data is involved because cellular phones can store millions of text messages, pictures, and videos all in one place). Also, cell phones collect user information over the years they are used, and privacy interests are further complicated when this information is stored on a remote server. *Id*. at 2479.

57 *See* Tobias Dehling et al., *Availability and Quality of Mobile Health App Privacy Policies*, 22 J. OF THE AM. MED. INFO. ASSOC. e32 (Apr. 1, 2015) (analyzing the available privacy policies of mHealth applications and the characteristics of mHealth privacy policy applications); *see also* David Lee Scher, *The Big Problem With Mobile Health Apps*, MEDSCAPE (Mar. 4, 2015), *archived at* https://perma.cc/72NUG6Y6 (declaring that physicians have trust issues with mHealth applications because the FDA does not regulate a vast majority of the applications that target doctors). *Id*. The privacy and security are "magnified" when using mHealth applications because it is required that mHealth application developers and physicians both comply with HIPAA. *Id*. It is the developer's responsibility to comply with HIPAA as to how PHI is handled, while it is hospitals and physician's responsibility to ensure that there are strong passwords protecting actual access to PHI. *Id.*

58 *See The Enforcement Rule*, *supra* note 44 (relating to the compliance and investigation of third parties who may have breached HIPAA).

Generally, the Enforcement Rule of 2006 allows the Secretary of Health and Human Services to take into account several factors and impose civil or criminal penalties on third parties who do not comply with HIPAA.[59] The monetary penalties that can be sanctioned onto a covered entity or business associate can vary in amount based on if the violation occurred due to willful neglect, was not corrected within a certain amount of time, or by not exercising reasonable diligence to determine if HIPAA requirements applied.[60] Additionally, broadly in accordance with the Security Rule, the OCR has held individuals and entities directly liable if HIPAA requirements are not complied with.[61] The Office of Civil Rights has been able to utilize the Enforcement and Security portions of HIPAA to impose the Privacy Rule against both individuals and entities, as since of March 6, 2018, the OCR had received over 173,436 HIPAA complaints and imposed civil money penalty in 53 cases resulting in a total amount of $75,229,182.00.[62]

To prevent the potential penalties against mHealth application developers, Security Rule poses a mandatory requirement that a full risk assessment be done of mHealth application security to ensure that the

59 *See The Enforcement Rule*, *supra* note 44, § 160.408 (noting that the Secretary of Health and Human Services may take into account factors such as the number of individuals affected by the violation, if the violation caused an individual to suffer physical or financial harm, and if the violation caused harm to an individual's reputation when imposing penalties on violating parties).

60 *See* 45 C.F.R. § 160.404 (asserting that the Secretary of Health and Human Services may impose civil monetary penalties on covered entities or business associates that "did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associated violated such provision").

61 *See* 45 C.F.R. §§ 160, 164 (2013) (eliminating the direct liability additions that were added to HIPAA and HITECH to further protect PHI). The additions to HIPAA and HITECH ensured that there would be no sale of PHI without individual authorization, expanded individuals' rights to receive electronic copies of their health information, modify individual authorization, and increased the penalty structure provided by the HITECH act of entities that did not comply with HIPAA. *Id*.

62 *See Enforcement Highlights*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Mar. 6, 2018), *archived at* https://perma.cc/JA7G-JWJ9 (highlighting that the OCR has investigated and resolved over 25,797 cases, which have required changes in privacy practices and corrective actions to HIPAA covered entities and their business associates).

security features actually work.[63] The OCR launched a platform for mHealth application developers who were concerned about HIPAA privacy protection as a way to improve health outcomes and answer any questions that developers may have when complying with the HIPAA Security Rule.[64] Additionally, OCR released a series of fact sheets to help mHealth application developers understand the permitted disclosures and the uses of patient's PHI under HIPAA.[65]

Although one would assume a majority of mHealth applications would have privacy policies attached to the product due to the amount of resources and guides available to developers, it has been discovered that many mHealth applications do not have clear privacy policies or any privacy policies at all.[66] For instance, in 2014, professors from Germany and Massachusetts conducted a study to evaluate mHealth application privacy policies that were provided by the iOS and the Android application stores, and found that only 30.5% of mHealth applications contained privacy policies.[67] For the 30.5% of privacy

63 *See Mobile Data Security and HIPAA Compliance*, HIPPA JOURNAL (2015), *archived at* https://perma.cc/HAH9-GJ77 (describing that it is possible to create multiple security defenses by having all of the standard defense measures). Nevertheless, a risk assessment is necessary to make sure that PHI is not accessed without individual authorization. *Id.* It also expanded individuals' rights to receive electronic copies of their health information, modify individual authorization, and increased the penalty structure provided by the HITECH act of entities that did not comply with HIPAA. *Id*.

64 *See Resources for Mobile Health App Developers*, U.S. DEP'T OF HEALTH & HUM. SERVS. (June 16, 2017) (explaining that the OCR platform was launched because many mHealth application developers were not familiar with how HIPAA's provisions applied to their products).

65 *See* Marianne Kolbasuk McGee, *New HIPAA Guidance for Mobile Apps*, HEALTH INFO. EXCH., INFO. SEC. MEDIA GROUP, CORP. (Feb. 15, 2016), *archived at* https://perma.cc/3YZU-FE8S (noting that the OCR HIPAA guidance plan for mHealth application developers allows developers to ask a series of questions based on the application that they are developing). There are a number of scenarios that are produced by the OCR and the answer may determine if the developer needs to comply with HIPAA. *Id*.

66 *See* Dehling et al., *supra* note 57, at e28 (describing that mHealth applications available on the iOS and the Android application store have poor availability rates for privacy policies, and when privacy policies are available, they are extremely difficult to understand).

67 *See* Dehling et al., *supra* note 57, at e32 (commenting that mHealth applications are currently sold and downloaded at a high rate, even though privacy policies are either "absent, opaque, or irrelevant"). It is suggested that consumers download

policies that were available, many did not focus on the application at all and were not informative to consumers.[68] While the mHealth application manufacturers ignore developing privacy policies, "concerns about information privacy may inhibit physicians' and patients information sharing."[69]

Although there have been clear efforts made by federal agencies to lessen the amount of PHI exposure, there have still been major breaches and violations committed by mHealth application manufacturers.[70] A major discovery occurred in 2015 when it was found that there were 1.2 million healthcare records exposed.[71] Of that number, 270,671 of those record exposures subject to HIPAA breaches involving mobile devices.[72] To deal with the number of mHealth application breaches, the FDA first issued a guidance documents in 2013 and then a revised copy 2015 as to the types of mHealth applications the FDA would regulate.[73] However, since that first initiation by the FDA to avoid mHealth application breaches, the FDA still has discretion as to what mHealth applications the FDA will

mHealth applications for a short-term benefit even though there could be a potential exposure to harm in the long term or have a complete misunderstanding of the applications access to personal privacy. *Id*. at e32.

68 *See* Dehling et al., *supra* note 57, at e32 (asserting that privacy policies lack relevant information to consumers leaving them "blissfully ignorant" of potential risks).

69 *See* 45 C.F.R. § 160.408 (designating the factors that are considered when the Secretary of Health and Human Services determines that a civil money penalty should be imposed on an entity that violated HIPAA).

70 *See Mobile Data Security and HIPAA Compliance*, *supra* note 63 (asserting that there are so many HIPAA violations occurring on mobile devices because mHealth devices do not have the proper security, have access to public WiFi, and have unaddressed security issues).

71 *See Mobile Data Security and HIPAA Compliance*, *supra* note 6363 (demonstrating the many ways covered entities can compromise health care records during an average day). Also, noting how many health care data breaches involved mobile devices. *Id*.

72 *See Mobile Data Security and HIPAA Compliance*, *supra* note 6363 (estimating that 81% of physicians use their smartphone to access professional data and that 38% of healthcare providers use a system to send secure text messages). These figures reflect data that was collected between January 1 and July 31 of 2015. *Id.*

73 *See* PATEL, *supra* note 28, at 4 (recording that the document was issued on February 9, 2015); *see also* Sarah Jean Kilker, *Effectiveness of Federal Regulation of Mobile Medical Applications*, 93 WASH. L. REV. 1341, 1349 (2016) (asserting that the FDA's discretion between what mHealth applications are regulated and unregulated can be unclear).

directly oversee.[74] The FDA's discretion in regulating mHealth is expanded by the language in 21 C.F.R. § 801.4, which observes that mHealth application developers can label applications as medical devices even if the product is not a medical device.[75]

The FTC has attempted to make it a goal to ensure that mHealth applications are being truthful as to the applications ability in utilizing PHI to establish against "unfair or deceptive" trade practices."[76] In 2011, the FTC filed a complaint against two different acne applications on the grounds that the applications claimed that they could treat acne by colored lights emitted from other mobile devices.[77] Additionally, state government officials have filed complaints against mHealth applications because developers have made deceptive statements about their applications being regulated by the FDA, and needed to modify their privacy policies to better protect consumers.[78] After New York Attorney

74 *See* PATEL, *supra* note 28 (indicating that the only change that was made to the document is due to the 21st Century Cures Act, which amended the definition of "device" in the FD & C Act to exclude certain software functions, including some described in the guidance document).

75 *See* Meaning of Intended Uses, 21 C.F.R. § 801.4 (2016) (indicating "[T]he totality of the evidence establishes that a manufacturer objectively intends that a device introduced into interstate commerce by him is to be used for conditions, purposes, or uses other than ones for which it has been approved, cleared, granted marketing authorization, or is exempt from premarket notification requirements (if any), he is required, in accordance with section 502(f) of the Federal FD & C Act, or, as applicable, duly promulgated regulations exempting the device from the requirements of section 502(f)(1), to provide for such device adequate labeling that accords with such other intended uses.").

76 *See* Federal Trade Commission Act, *supra* note 48 (explaining that that FTC has the power to prevent persons and entities from using unfair methods, or unfair or deceptive acts or practices in or affecting commerce); *see also* Children's Online Privacy Protection Act of 1996, 15 U.S.C. § 6501-06 (1996) (indicating that there may be certain circumstances where the FTC can impose special privacy rules on a company if information concerning a child under 13 years old is transmitted).

77 *See "Acne Cure" Mobile App Marketers Will drop Baseless Claims Under FTC Settlements*, FTC (Sept. 8, 2011), *archived at* https://perma.cc/7R7N-VB63 (describing that the FTC charged the acne treatment claims because the mHealth applications were substantiated and provided false study results to the British Journal of Dermatology).

78 *See* Press Release, N.Y. OFF. OF THE ATTY. GEN., *supra* note 17 (describing how a settlement was eventually reached after a year-long investigation of mHealth applications and required that the mHealth application developers modify their privacy policies to better protect consumers).

General Eric Schneiderman filed three claims against mHealth applications that falsely advertised the application capabilities, developers are now required to receive affirmative consent to their privacy policies and disclose that the applications will collect and share information that could be personally identifying.[79] As a way to ensure that mHealth applications do not continue to practice unfair and deceptive trade methods, states have enacted statutes and regulations in accordance with the FDA and FTC for mHealth applications that are releasing PHI, while legislatures work to make HIPAA more inclusive of technology that contain PHI.[80]

IV. Analysis

The OCR, FTC, and FDA continue to define HIPAA compliant measures for mHealth applications.[81] Though the organizations have produced multiple guidance documents and have many Internet resources readily available, it is difficult to determine how closely and

79 *See* Press Release, N.Y. OFF. OF THE ATTY. GEN., *supra* note 17 (explaining that A.G. Schneiderman filed claims against two mHealth application developers because developers claimed that their applications could accurately measure heart rate after exercise using only a smartphone camera and sensors). The third claim was against a developer that claimed a mHealth application could transform a smartphone into a fetal heart monitor, despite the fact that the application was not FDA-approved. *Id*.

80 *See Mobile Data Security and HIPAA Compliance*, *supra* note 63 (acknowledging that health care providers and HIPAA-covered entities have embraced the mobile technological changes, but must implement a number of controls to protect PHI that is accessed through a device, stored on it, or transmitted by it). It is important that HIPAA-covered entities increase security control to avoid cybercriminals and have protected internet networks. *Id.*

81 *See Mobile Devices Roundtable*, *supra* note 7 (identifying all of the federal organizations that work together to ensure that mHealth applications comply by federal statutes). The FDA specifically is responsible for overseeing the safety and effectiveness of mobile medical applications that present a potential risk to patients if they do not work as intended. *Id*. The FTC has brought enforcement actions challenging the privacy and data of security practices, and educates consumers about protecting their privacy. *Id*. The OCR enforces the HIPAA Privacy Rule that limits how a covered entity may use or disclose the protected health information, and the HIPAA security Rule to ensure privacy, integrity, and availability of electronic protected health information through standards for administrative, physical, and technical safeguards. *Id*.

efficiently members of the FDA, FTC, and the OCR work together to monitor mHealth applications that may not be secured.[82]

The guidance plans developed by the FDA and FTC have numerous guidelines as to how mHealth application manufacturers that fall within the definition of a medical device should ensure patient privacy.[83] However, the guidance plans only make non-binding recommendations as to how a manufacturer should develop an application and does not assert clear line of what *must* be done.[84] The FDA guidance plan fails to provide specific requirements to determine if a mHealth application is considered a medical device, which ultimately puts the responsibility on the manufacturers to determine which guidelines and federal requirements are applicable.[85] Additionally, neither the FDA nor FTC guidance plans explain or demonstrate how the two organizations directly have intertwined resources to ensure how all necessary mHealth applications are regulated.[86]

The FDA created a list of medical applications and HIPAA covered entities that it intends to have authority over to exercise enforcement discretion over.[87] Some examples of mHealth applications that the FDA will not enforce requirements are applications that enable

82 *See mHealth Laws and Regulations*, *supra* note 28 (stating the FDA, FTC, and FCC all share jurisdiction over some part of the federal regulation of mHealth).

83 *See* PATEL, *supra* note 28, at 13 (describing the scope of mHealth applications that the FDA will have jurisdiction over because the applications falls within the definition of a medical device or if the application is intended to be used as an accessory to a regulated medical device or to be a mobile platform to a regulated medical device).

84 *See* PATEL, *supra* note 28, at 5 (noting that some topics within the guidance plans are only recommendations "unless specific regulatory or statutory requirements are cited").

85 *See* PATEL, *supra* note 28, at 13 (asserting that if a "mobile medical application, on its own, falls within a medical device classification, its manufacturer is subject to the requirements associated with that classification"). The FDA has a regulatory approach on a subset of mobile applications that can also be an extension of a mHealth application. *Id.* The extensions of a mHealth applications may be required if there is a display of patient-specific data or if there are specific display screens that are similar to regulated medical devices. *Id.*

86 *See* PATEL, *supra* note 28, at 20-22 (indicating how the FDA will regulate mHealth applications and provides a list of mHealth applications that will not be regulated by the FDA because they are not considered medical devices).

87 *See* PATEL, *supra* note 28, at 15-18 (discussing various mHealth applications under the FD & C Act).

patients or providers to interact with Personal Health Record or applications that are intended to transfer, store, convert format, and display medical device data in its original format.[88] The FDA has the ability to use discretion and not regulate mHealth applications that use a patient's diagnosis to provide a clinician with the best practice treatment guidelines for common illnesses.[89] The FDA will evaluate the privacy and security risks that are posed to consumers, and have divided mHealth applications into Class I, Class II, and Class III risk categories.[90] Examples of different types of mHealth applications are provided for each category but the guidance document fails to make explicit how manufacturers should determine what risk class their mHealth application belongs in.[91]

The FDA guidance document also fails to provide a clear set of steps to help manufacturers determine if their mHealth application is a medical device.[92] However, the lack of transparency of the FDA guidance plan can be balanced by the FTC guidance plan.[93] Unlike the FDA guidance plan, the FTC guidance plan sets out a series of questions

88 *See* PATEL, *supra* note 28, at 9 (demonstrating the types of mHealth applications that the FDA will not intend to enforce requirements under the FD & C Act). The FDA acknowledges that some mHealth applications within the list that the FDA intends to use enforcement discretion on may eventually fall within the definition of a medical device. *Id*. at 16. The FDA mostly focuses on how the FDA will not regulate applications that are intended to supplement professional clinical care or coach users through. *Id*. at 16.

89 *See* PATEL, *supra* note 28, at 17 (explaining that the FDA will use discretion against applications that are able to access specific patient documents and help patients communicate with physicians about their specific illnesses).

90 *See* PATEL, *supra* note 28, at 19 (designating the three classes of mHealth applications as Class I, Class II, and Class III). Class III is the highest risk class, and manufacturers need to meet premarket submission requirements before being put out on the market. *Id*. at 40. However, Class I applications have the lowest amount of risk for consumers and are exempt from premarket submission requirements are subject to the least regulatory control. *Id.*

91 *See* PATEL, *supra* note 28, at 19 (setting forth the requirements that each class of mHealth applications must meet before being presented to the market).

92 *See* PATEL, *supra* note 28, at 27- 28 (presenting examples of the FDA's regulatory oversight of mHealth applications). The risk for each mHealth application is the manufacturer being able to determine if their specific application falls within the meaning of one of the examples provided. *Id*.

93 *See Mobile Health App Developers: FTC Best Practices*, *supra* note 49 (reaffirming that the guidance plan provides ways to comply with regulations).

and tips that a mHealth application developer should address when creating the applications.[94] The FDA suggests to mHealth application developers that data accessed from the application should be limited and that the data accessed is absolutely necessary to achieve the purpose of the application. [95] Additionally, the FTC provides a list of federal statutes, including health care, financial, and security laws that should be considered by mHealth application developers who are unsure of the applicable laws.[96]

As discussed in a research project completed by the team of Tobias Dehling, the FTC has paid little attention "to the information security and privacy policies and practices of mHealth application vendors."[97] The results of that project indicated that mHealth application developers often fail to provide application privacy policies transparent to uses, and are not focused on the application itself.[98] Dehling's project is a prime example of applications developers competing without benefiting from protection from harm that may be destructive.[99] The project further demonstrates that even though the FTC wishes to encourage transparency, consumers are concerned because sensitive and private data is being transmitted through applications that have privacy policies that are absent or irrelevant.[100]

---

94 *See Mobile Health App Developers: FTC Best Practices*, *supra* note 49 (presenting a series of questions, divided up into a number of subcategories focusing on how mHealth application developers should determine which statutory requirements they must follow).

95 *See Mobile Health App Developers: FTC Best Practices*, *supra* note 49 (providing eight suggestions to application envelopes, focusing on mHealth applications, to ensure that the proper security is implemented to protect consumers and companies).

96 *See Mobile Health App Developers: FTC Best Practices*, *supra* note 49 (setting out a variety of federal and state laws that may apply to mHealth applications depending on an application's specific features).

97 *See* Sunyaev, *supra* note 54 (noting the important of privacy policies and consent).

98 *See* Sunyaev, *supra* note 54 (providing results that privacy policies have poor availability rates, there is a lack of privacy policy availability, and the policy scope is lacking).

99 *See* Sunyaev, *supra* note 54 (explaining that mHealth application developers fail to address information privacy and do not have the ability to access quality privacy policies).

100 *See* Sunyaev, *supra* note 54 (stating that while there are no privacy policies corresponding to mHealth applications, mHealth applications are still purchased by consumers).

By the FTC not taking a higher role in regulating mHealth application privacy policies consumers are becoming misinformed, and are only looking at the short term benefit of the mHealth application use compared to the long term risk of having PHI exposed.[101]

Between the FDA and the FTC not having strict requirements for mHealth application manufacturers when it comes to protecting patient PHI, it makes it difficult for the Health and Human Services Office for Civil Rights to complete their job.[102] The Office of Civil Rights believes that HIPAA must keep up with technology in order to continue to protect PHI.[103] A series of changes regarding HIPAA were made starting in the year 2000, and the FDA and FTC do seem to suggest that mHealth applications look at the HIPAA Privacy or Security Rules for guidance, but there seems to be a lack of cohesiveness between all of the federal entities.[104] For example, the FTC provides a small quiz through their interactive tool to help developers decide if their mHealth application needs to HIPPA to protect privacy or security rules in their interactive tool and brings developers right to the HHS website for the definition of HIPAA.[105] However, although the FTC provides definitions throughout

---

101 *See* Sunyaev, *supra* note 54 (surmising that consumers may be "blissfully ignorant" and more likely to use a mHealth application if its privacy policies are unclear). One reason that privacy policies are kept vague may be because specific privacy policies would make physician-patient interactions more tense because patients would be forced to share their information. *Id*.

102 *See About Us*, *supra* note 40 (indicating that the OCR protects health and information rights by patient safety confidentiality laws and investigating civil rights, health information privacy, and patient safety confidentiality complaints to take corrective action).

103 *See HIPAA for Professionals*, supra note 41 (stating that Congress recognized the changes in technology and, therefore, tailored HIPAA provisions to cover technological developments). Starting in December 2000, the Department of Health and Human Services conducted a series of tests to ensure that covered entities correctly processed electronic transactions using PHI. *Id.*

104 *See HIPAA for Professionals, supra* note 41 (outlining the details of the Department of Health and Humans Services's Security Rule that was published in February 2003). The Security Rule sets national standards for protecting confidentiality, integrity, and availability of electronic protected health information. *Id*. As of April 20, 2005, compliance with the Security Rule was mandatory. *Id*.

105 *See Mobile Health App Developers: FTC Best Practices, supra* note 49 (setting forth a series of questions for mHealth application developers). Answers to these questions provide developers with tips to determine if an application qualifies as a covered entity under HIPAA. *Id.*

the quiz, one wrong answer may lead the developer down a path to not follow any of the necessary federal laws.[106] Moreover, the FDA does not provide any suggestions in their 2015 guidance document to mHealth application developers about what federal laws should be considered.[107] Between the lack of clarification from all of the federal organizations and the results of Tobias Dehling's study compared to the Security Rule, it is possible that not all mHealth application developers comply with ensuring that PHI is kept confidential.[108] Additionally, it is possible that because mHealth application developers do not actually provide privacy policies that the integrity and availability of protected electronic PHI is low.[109]

The overall goal of mHealth applications is to help provide additional care to those who have the desire to not only improve their health, but also want to communicate more efficiently with their physicians.[110] The idea of mHealth applications is extremely successful due to the overwhelming amount available to consumers, but due to the FDA and FTC lack of asserting which mHealth applications are covered, consumer engagement continues to be a concern.[111] It is possible that there are many existing mHealth applications that are not governed by effective privacy policies, indicating that the FDA, FTC, and HHS are

106 *See* PATEL, *supra* note 28, at 7 (defining protected health information, medical device, and mobile medical apps to help developers determine if their mHealth application must comply with HIPPA).

107 *See* PATEL, *supra* note 28, at 19 (providing the regulatory requirements for the general controls that must be followed by mHealth application developers in order to have the application be for sale on the market).

108 *See* Dehling, *supra* note 57, at e30 (demonstrating that 66.1% of privacy polices did not specifically address the mHealth application itself).

109 *See HIPAA for Professionals*, *supra* note 41 (defining the role of the Department of Health and Human Services as ensuring that covered entities are complying with HIPAA's requirements to ensure confidentiality and integrity).

110 *See Mobile Medical Applications*, *supra* note 6, at 1-2 (articulating the purpose of a mHealth application and defining what consumers can use the mHealth applications for).

111 *See Mobile Medical Applications*, *supra* note 6, at 1 (predicting that by 2018, 50% of the 3.4 billion smartphone users will have downloaded some type of mHealth app, with the global market for mHealth applications reaching $102.43 billion by 2022); *see also* O'Shea, supra note 17, at 618 (opining that mHealth applications are not governed by effective policies).

not communicating as well as they should be.[112] The gaps between the regulatory bodies do not provide for correct evaluations to be made of mHealth applications available because of the lack of privacy policies that go unregulated by the FTC.[113] This lack of communication is ultimately leading to mHealth applications remaining invalidated, and thus potentially not useful or even harmful.[114]

As mHealth applications remain to be invalidated, this creates a "potential minefield" of HIPAA violations.[115] Because guidance controls from the FTC and FDA are inadequate, devices can be compromised and lead to PHI being leaked very easily.[116] The biggest concerns are against those who are considered cybercriminals and look to steal electronic health information from healthcare networks.[117] It is possible for anyone with a computer to develop a mHealth application and then go through the steps of complying with HIPAA, and the FTC

112 *See* O'Shea, *supra* note 17, at 618 (pointing out there is no regulatory body that evaluates how effective a mHealth application is); *see also mHealth Laws and Regulations*, *supra* note 28 (recounting instances where the FTC and FDA have collaborated in jurisdictions where the two organizations overlap). It was only in 2012 that the FDA received the approval to move forward with taking steps to regulate mHealth applications. *Id*.

113 *See* Dehling, *supra* note 57, at e30 (demonstrating that 66.1% of privacy polices did not specifically address the mHealth application itself); *see mHealth Laws and Regulations*, *supra* note 28 (defining the FTC responsibilities as making sure that consumers are protected from unfair or deceptive acts, or practices that lead to false or misleading claims). The FTC ensures that mHealth applications run effectively by avoiding legal liability. *Id*.

114 *See* O'Shea, *supra* note 17, at 618 (highlighting a Mobile Application Rating Scale that is used to measure the quality of health-related mobile applications). The goal of the rating scale is to engage consumers regarding the functionality and information quality provided by the application. *Id*. However, these programs do not measure an application's efficacy or patient outcomes. *Id*.

115 *See Mobile Data Security and HIPAA Compliance*, *supra* note 63 (noting that even though mHealth applications are convenient to use, they can present users with risks). There are hundreds or thousands of mobile devices that access healthcare networks making these same networks easy to hack. *Id*. at 3.

116 *See Mobile Data Security and HIPAA Compliance*, *supra* note 63 (describing mobile data security and HIPAA compliance as two of the biggest concerns for Compliance officers and health IT professionals). Even though a mobile device may be secure, users of the device may still violate HIPAA rules or company policies. *Id*.

117 *See Mobile Data Security and HIPAA Compliance*, *supra* note 63, at 2 (stating that there is considerable potential for theft or loss when cybercriminals go into a healthcare network to access electronic health information).

and FDA requirements.[118] An increased risk occurs when there is an often lack of robust security controls.[119]

The FDA and FTC should work more closely with the OCR to determine which mHealth applications are actually transmitting PHI in the regular course of business and conduct a more in-depth analysis of those mHealth applications that walk the fine line of being a medical device.[120] Additionally, it would be helpful if the FDA, FTC, and OCR communicated more directly with HIPAA covered entities and business associates to train and educate others as to the security of the mobile devices connecting to their health care network.[121] The communication between the FDA, FTC, and OCR needs to be stronger in order to lessen the amount of private healthcare information accessed through mHealth applications.

V. Conclusion

MHealth applications have become a worldwide phenomenon based on the incredible amount of information that can be accessed by consumers and physicians. However, in order to ensure that patient's private health care information is consistently protected, the Food and Drug Administration, Health and Human Services Office of Civil Rights, and Federal Trade Commission need to implement a regulatory

118 *See* PATEL, *supra* note 28, at 9 (defining "mobile medical app manufacturer"). There are a series of federal rules that must be followed to be a mobile medical application manufacturer. *Id*. at 9-10. Ultimately, the definition focuses on someone who creates, designs, develops, labels, re-labels, remanufactures, modifies or creates a mobile medical application software system from multiple components. *Id*.

119 *See Mobile Data Security and HIPAA Compliance*, *supra* note 63 (calling for robust mobile data security and HIPAA compliance). Organizations and entities that are required to comply with HIPAA through the FDA, FTC, and OCR must do so or there can be hefty fines imposed upon them. *Id*.

120 *See Mobile Data Security and HIPAA Compliance*, *supra* note 63 (setting forth that if covered entities allow the transmission of electronic PHI over an open network, then they violate HIPAA). To avoid a HIPAA violation, the electronic PHI that is being transmitted should be encrypted. *Id*.

121 *See Mobile Data Security and HIPAA Compliance*, *supra* note 63 (offering HIPAA compliance tips which include conducting risk assessments as to mobile security, training the staff to recognize a security breach and report the issue, tracking data as to where healthcare data is being transmitted, and implementing information access controls to avoid all devices accessing PHI).

system that is consistent when evaluating privacy, security, and HIPAA standards. The lack of regulations that have been lost in between the cracks has created the ability for private health care information to be compromised. Though Congress and state legislatures have attempted to create a statutory scheme that prevents personal health data from being stolen or leaked, it is clear that the methods currently in place are ineffective and the schema in place now is outdated.