Catholic University Journal of Law and Technology

Volume 25 | Issue 2 Article 10

May 2017

Is Your Health Data Really Private? The Need to Update HIPAA Regulations to Incorporate Third-Party and Non-Covered Entities

Latena Hazard
Catholic University of America (Student)

IS YOUR HEALTH DATA REALLY PRIVATE? THE NEED TO UPDATE HIPAA REGULATIONS TO INCORPORATE THIRD-PARTY AND NON-COVERED ENTITIES

By: Latena Hazard

After running 3.5 miles of the Anacostia Riverwalk trail in Maryland, the runner looks down at her smart phone and inputs the information into a health data application. The health data application then creates a diary of her runs, and monitors her daily calorie intake and required water consumption. However, before gaining access to this information, the runner was required to enter personal information, including her name, age, weight, and email address. This information is then stored; however, many consumers fail to ask themselves where and how this information is stored, shared, or tracked. This hypothetical is merely one common situation in which personal health data is retrieved. As mobile applications become easier to access and user-friendly, consumers are downloading applications to their smartphones at an increasing rate and potentially sharing sensitive information with varying unknown parties.[1]

Despite the aforementioned scenario, there are benefits to this type of information sharing, which includes allowing consumers to "manage their own health and wellness, [and] promote healthy living..."[2] In addition, some health applications improve the delivery of health care to patients from their providers.[3] However, the benefits may not outweigh the cost when, for example,

1 Jocelyn Samuels J.D. & Dr. Karen B. DeSalvo, *Examining Oversight of The Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*, U.S. DEP'T OF HEALTH & HUM. SERV. 8 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

2 *Mobile Medical Applications*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm255978.htm (last updated Sept. 22, 2015).

3 U.S. DEP'T OF HEALTH & HUMAN SERVICES FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS, GUIDANCE FOR INDUSTRY & FOOD & DRUG ADMIN. STAFF 6 (2015), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf#page=20.

consumers' personal identifiable information is subject to additional risks.[4] Given that there are roughly 165,000 mobile health apps through which people can readily connect and gain information with the click of a button, it is essential for Congress to update the rules that govern health data management and information sharing.[5]

This need to modernize health care regulations was addressed in March 2016, when Representative Will Hurd (R-TX) drafted a letter to Secretary Burwell[6] addressing the "insufficient guidance" in regards to Health Information Privacy and Accountability Act of 1996 ("HIPAA") and mobile health apps.[7] The lack of guidance in regards to HIPAA and mobile health apps can lead to misunderstanding by users of their privacy rights.[8] With such little guidance the normal consumer may not understand health privacy and security laws like the experts, and can be misinformed about the level of protection their personal information is afforded. Consumers would also benefit from improved communication between covered entities, non-covered entities, and themselves regarding health information technology, and which entities are gathering that information.

Health information technology ("health IT") encompasses technology that shares, stores, and analyzes health data.[9] In 2011, more than 74% of Americans used the Internet, and roughly 59% of these individuals used the Internet to research diseases or treatments, or to read another person's medical or health issues and their experiences on a blog, forum, or website.[10] Yet these conver-

---

4 Personal identifiable information ("PII") "is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII." Margaret Rouse, *Personally Identifiable Information (PII)*, WHATIS.COM, http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information (last updated Jan. 2014).

5 *IMS Health Study: Patient Options Expand as Mobile Healthcare Apps Address Wellness and Chronic Disease Treatment Needs*, IMS HEALTH (Sept. 17, 2015), http://www.imshealth.com/en/about-us/news/ims-health-study:-patient-options-expand-as-mobile-healthcare-apps-address-wellness-and-chronic-disease-treatment-needs.

6 The Honorable Sylvia Mathews Burrell is the Secretary of the Department of Health and Human Services. *See* Alex Rogers, *Senate Confirms Sylvia Burwell As Health and Human Services Secretary*, TIME (June 5, 2014), http://time.com/2827571/senate-confirms-sylvia-burwell-as-health-and-human-services-secretary/.

7 Letter from Members of Congress, Congress of the U.S., to The Honorable Sylvia Mathews Burwell, Secretary of Health and Hum. Serv. (Mar. 9, 2016) (on file with author).

8 Samuels & DeSalvo, *supra* note 1, at 26.

9 *Basics of Health IT*, HEALTHIT.GOV (Jan. 15, 2013), https://www.healthit.gov/patients-families/basics-health-it.

10 Susannah Fox, *The Social Life of Health Information*, PEW RES. CENTER 2 (2011), http://www.pewinternet.org/files/old-media/Files/Reports/2011/PIP_Social_Life_of_Health_Info.pdf.

sations may not have been kept private.[11] Health information is classified by "who creates or receives [the information] and what the information collected consists of."[12] Health Information Technology includes electronic health records ("EHRs"),[13] personal health records ("PHRs"),[14] and e-prescribing.[15] Under HIPAA regulations, any information, whether oral or recorded in any form, that is created or received by a health care provider[16], health plan, public health authority, or health care clearinghouse[17]; and relates to the "physical or mental health or condition of an individual; the provision of health care; or the payment for the provision of health care to an individual"[18] can be considered health information.[19]

Access to health information allows patients to connect with experts when the patient needs it most.[20] There has been an increase in health care providers using health IT to communicate with their patients and improve care.[21]

Since health records are meant to be kept private, the result of accidental or

---

11 *Id.* at 3.

12 Samuels & DeSalvo, *supra* note 1, at 28.

13 Electronic Health Reports is a real-time electronic system that stores patient's health information. EHRs allow doctors to access and keep track of patient health information in or out of the office. It is also used to make it easier for providers to share information about patients. *See What is an electronic health record (EHR)?*, HEALTHIT.GOV (Mar. 16, 2013), https://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-her.

14 Personal Health Records control what kind of information goes into the record. Unlike an EHR the PHR allows for the consumer to keep track of their own data, including blood pressure, exercise, and food consumption. *See What is a personal health record?*, HEALTHIT.GOV (May 2, 2013), https://www.healthit.gov/providers-professionals/faqs/what-personal-health-record.

15 E-prescribing allows a doctor to engage directly with the pharmacist providing a patient with the option of going paperless. *See* Margaret Rouse, *e-prescribing (electronic prescribing)*, SEARCH HEALTH IT (Feb. 2010), http://searchhealthit.techtarget.com/definition/e-prescribing.

16 Health care provider means a provider of services (as defined in section 1861 of the Act, 42 U.S.C. § 1395x(u) (2012)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. § 1395x(s) (2012)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. 45 C.F.R. § 160.103 (2012).

17 *Id.* A clearinghouse is *"*a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and 'value-added' networks and switches, that either processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction or Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity." *Id.*

18 *Id.*

19 Samuels & DeSalvo, *supra* note 1, at 3.

20 Predrag Klasnja, *Healthcare in the pocket: Mapping the space of mobile-phone health interventions*, 45 J. OF BIOMEDICAL INFORMATICS 184, 193 (2012).

21 *Id.* at 185.

unauthorized disclosure may be harmful to the consumer. HIPAA was initiated to combat this disclosure and ensure the protection of consumer health insurance data.[22] HIPAA also establishes requirements for electronic transactions, including those that allow the electronic exchange of health information.[23] HIPAA consists of two rules: the HIPAA security rule and the HIPAA privacy rule.[24] The HIPAA security rule introduced a standard of practice within the health care profession. However, when Congress originally enacted these regulations, many of the technologies we have today were not available. Therefore, in an era where technology is ever revolving Congress should be required to update the rules to ensure that these entities are properly governed.

Furthermore, the Department of Health and Human Services should implement security standards from the National Institute of Standards and Technology Cybersecurity Framework that would create necessary guidelines for "health care organizations and their business associates."[25]

Although the past 20 years of HIPAA have achieved its purpose, with today's technology, its privacy rule is inadequate.[26] Technology is making information more transparent and Congress needs to update these regulations to include the gaps that continue to put users at risk when using health apps. HIPAA should provide a means to ensure that consumers are making a conscious decision whether they'd like to disclose their information.

In a 2013 report entitled "The Internet of Things," the Federal Trade Commission analyzed how data and information sharing has spread.[27] The year the report was published, there were an estimated 25 billion connected devices thus creating the possibility of a security risk capable of harming consumers by enabling unauthorized misuse of and access to personal information, safety, and attacks on systems.[28]

---

22 42 U.S.C. § 300gg (2012).

23 H.R. CHAIKIND ET AL., THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OVERVIEW AND ANALYSES 5 (Susan Boriotti et al. eds., 2004).

24 *A Brief Background on the HIPAA Rules and the HITECH Act*, HIPAA SURVIVAL GUIDE, http://www.hipaasurvivalguide.com/hipaa-rules.php (last visited Feb. 18, 2017).

25 Marianne Kolbasuk McGee, *What's Needed: More HHS Guidance, or New HIPAA Security Rule?*, GOV INFO SECURITY (Sept. 28, 2016), http://www.govinfosecurity.com/whats-needed-more-hhs-guidance-or-new-hipaa-security-rule-a-9426.

26 Samuels & DeSalvo, *supra* note 1, at 4.

27 *See* FTC, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD STAFF REPORT i (2015) (defining the mission of the FTC as "to prevent business practices that are anticompetitive, deceptive, or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without burdening legitimate business practices.").

28 *Id.*

A recent study revealed that 84% of health applications were open to hacks[29] and HIPAA violations.[30] As the number of reports of HIPAA violations increases and personally identifiable information ("PII") thefts occur, the government needs to implement stricter regulations for non-covered entities that are also subject to these thefts and security breaches.[31]

This Note will address the need for Congress to update the HIPAA Security Rule and Privacy ruled to include non-covered entities in order to protect consumer privacy issues. Part I will summarize the background of HIPAA. Part II analyzes the effect HIPAA has on health care applications and manufacturers. Part III describes threats to privacy, data collection and discusses how entities not regulated by HIPAA are collecting and disseminating personal identifiable information and how it is used. Part IV provides a basis for why congress needs to fill the void in coverage and provide continues and updated protection for consumer utilizing mobile health applications not regulated by HIPAA.

I. THE HEALTH INFORMATION PRIVACY AND ACCOUNTABILITY ACT (HIPAA)

A. Background

The Health Information Privacy and Accountability Act ("HIPAA") was enacted in 1996 by the Department of Health and Human Services[32] to create uniformed formats and rules to covered entities regarding electronic health transmissions that were deemed important.[33] A covered entity is defined by the Act as a health plan, health care clearinghouse, or a health care provider that transmits any health information in electronic form about a transaction covered by subchapter C of part 45 of the U.S. Department of Health and Human Services Code of Federal Regulations.[34]

---

29 *See Computer Hacking Law and Definition*, USLEGAL.COM, https://definitions.uslegal.com/c/computer-hacking/ (last visited Feb. 18, 2017) (defining hacking as the gaining of information through an unauthorized access to a data system).

30 Bill Sidiki, *8 out of 10 mobile health apps open to HIPAA violations, hacking, and data theft*, HEALTHCARE IT NEWS (Jan. 13, 2016), http://www.healthcareitnews.com/news/8-out-10-mobile-health-apps-open-hipaa-violations-hacking-data-theft.

31 Samuels & DeSalvo, *supra* note 1, at 34.

32 *See About HHS*, HHS.GOV, http://www.hhs.gov/about/index.html (last visited Feb. 18, 2017) (explaining how the Department of Health and Human Services enhances and protects the health and well-being of Americans by providing effective health and human services and fostering advances in medicine, public health, and social services).

33 Steven Fleisher, *Background and History of HIPAA, in* A GUIDE TO HIPAA SECURITY AND THE LAW 6 (Stephen W. Wu ed., 2007).

34 *Covered Entities and Business Associates*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/covered-entities/ (last visited Feb. 18, 2017); *see generally* 45 C.F.R. §

These rules required the development of specific areas of regulation, including standards for electronic transactions, privacy of individually identifiable health information,[35] national employer identification, security, national provider identification, and proposed enforcement rule.[36] The proposed enforcement rule provides compliance and investigation provisions.[37] It is the "[U.S.] legislation that provides data privacy[38] and security provisions for safeguarding medical information."[39] The relevant part of HIPAA is Title II.[40] Title II "directs the U.S. Department of Health and Human Services to establish national standards for processing electronic healthcare transactions."[41] The Act also provides a federal standard of care for Protected Health Information[42] for pro-

---

160.103.

35 *See* 45 C.F.R. § 160.103 (quoting "Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:
(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.").

36 Steven Fleisher, *supra* note 33, at 7.

37 *The HIPAA Enforcement Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html (last visited Mar. 2, 2017); *see generally* 45 C.F.R. §§ 160(C-E).

38 Heather L. Buchta, *Privacy and Mobile Apps: What We Can Learn from Recent FTC Enforcement*, 26 WESTLAW J. SOFTWARE L. 1, 2 (2013) (explaining the difference data privacy and data security as privacy being the use and collection of data and data security is how that data is stored and maintained).

39 Margaret Rouse, *What is HIPAA*, SEARCHDATAMANAGEMENT, http://searchdatamanagement.techtarget.com/definition/HIPAA (last updated Apr. 2015).

40 *Id.*

41 *Id.*

42 *See* 45 C.F.R. § 160.103 (2012).

> Protected health information means individually identifiable health information:
> (1) Except as provided in paragraph (2) of this definition, that is:
> (i) Transmitted by electronic media;
> (ii) Maintained in electronic media; or
> (iii) Transmitted or maintained in any other form or medium.
> (2) *Protected health information* excludes individually identifiable health information in:
> (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
> (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
> (iii) Employment records held by a covered entity in its role as employer.

Id.

viders, health insurance plans, and employers.[43]

In 2016, the HHS launched Phase 2 of the HIPAA Audit Program.[44] The Program was established to ensure the standards set by the HIPAA Privacy, Security and Breach Notification Rules are met.[45] The Phase 2 Audit reviews the policies and procedures followed by covered entities and their business associates, in order to ensure they meet the standards set by the Privacy, Security, and Breach Notification Rules.[46]

B. What is a mobile health app?

A mobile application is information accessed through the use of software designed to run on smartphones.[47] A mobile medical application ("mobile medical app") can be defined as "medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device."[48] To be classified as a regulated medical device, one must base it off the intended use of the mobile app.[49] Intended use is determined by how the manufacturer labels the product or device.[50]

C. Security v. Privacy

On September 22, 2016, Yahoo revealed that they had been hacked.[51] The information was stolen from roughly 500 million user accounts[52] and included personal data from users dating back to 2014.[53] Roughly 89% of healthcare experts use their phones for work purposes thereby escalating the security

---

43 *Id.*

44 *OCR Launches Phase 2 of HIPAA Audit Program*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html?language=es (last visited Feb. 18, 2017).

45 *Id.*

46 *Id.*

47 Jamie L. Flaherty, Note, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM. L.J., 416, 418 (2014).

48 *Mobile Medical Applications*, *supra* note 2.

49 *Id.*

50 U.S. DEP'T OF HEALTH & HUMAN SERV., FDA, THE 501(K) PROGRAM: EVALUATING SUBSTANTIAL EQUIVALENCE IN PREMARKET NOTIFICATIONS: GUIDANCE FOR INDUSTRY FOOD AND DRUG ADMINISTRATION STAFF 16 (2014).

51 Seth Fiegerman, *Yahoo says 500 Million accounts stolen*, CNN MONEY (Sept. 23, 2016), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/.

52 Matt Ford, *Yahoo's Half-Billion Hack*, THE ATLANTIC (Sept. 22, 2016), http://www.theatlantic.com/news/archive/2016/09/yahoo-data-stolen-hack/501290/.

53 Fiegerman, *supra* note 51.

threat by increasing privacy issue not previously imagined.[54] This breach is one of the largest cyber breaches that included private identifiable information attached to user email accounts.[55] Unfortunately, the HIPAA Security Rule is not designed to regulate email and doesn't require HIPAA compliance or encryption.[56]

HIPAA is divided into two main rules – the Privacy Rule and the Security Rule that helps to regulate these issues.[57] The privacy rule applies to covered entities and business associates.[58] The HIPAA Privacy Rule covers any form of protected health information (PHI) unlike the HIPAA Security Rule which only covers electronic protected health information (ePHI).[59] In addition, the privacy rule identifies that public health authorities need to have access to PHI in order to carry out the public mission.[60] In order for this to work the privacy rule allows CEs to disclose protected information, without authority, to legally protected authorities in order to prevent injury or disease.[61]

The HIPAA Security Rule was passed in 2004 by Health and Human Services' Office for Civil Rights (OCR) to ensure that covered entities protect "the confidentiality, integrity, and availability of [electronic Protected Health Information]."[62] Therefore, confidential information should not be available or disclosed to unauthorized personnel,[63] and entities must prevent any unauthor-

---

54 Securing Health Data in a BYOD World (2014), https://www.cleardata.com/wp-content/uploads/2014/12/SET-MKTG-Securing-PHI-in-a-BYOD-World.pdf.

55 Fiegerman, *supra* note 51.

56 *See generally* Art Gross, *6 things organizations are doing that are not HIPAA compliant*, HIPAA SECURE NOW: BLOG (May 24, 2014), http://www.hipaasecurenow.com/index.php/6-things-organizations-are-doing-that-are-not-hipaa-compliant/.

57 Flaherty, *supra* note 47, at 424.

58 *Id. See also Health Information Privacy*, *supra* note 34. A covered entity ("CE") is a health care provider, health plan, and a health care clearinghouse. A health care clearing house includes "entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa." *Id.* A non-covered entity ("NCEs") is an entity not subject to HIPAA. Business associates are those entities that assist health care providers and health care plans carry out other functions. The privacy rule allows covered entities to disclose protected information to these associates, but only after receiving confirmation that these associates will not abuse the protected information. *Id.*

59 *HIPAA 'Protected Health Information': What Does PHI Include? HIPAA 'Protected Health Information': What Does PHI Include?*, HIPAA.COM, https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/ (last visited Nov. 27, 2016).

60 45 C.F.R. § 164.512 (2003).

61 *Id.*

62 *Summary of the HIPAA Security Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/ (last visited Mar. 2, 2017).

63 45 C.F.R. § 164.306 (2013).

ized alteration and destruction of information,[64] and finally information must be available when demanded.[65] Healthcare information is collected by a multitude of venues that are not covered by HIPAA, although, some of these organizations are covered by the FTC Act.[66] The Security Rule allows individuals to access identifiable health information held by covered entities.[67] These rights include ensuring requested information is obtained in a timely fashion and in the specific format requested.[68]

With the initiation of HIPAA, HHS was required to adopt "safeguards" and "security standards."[69] It ensured that clearinghouses adopted policies that would isolate their activities from the organization when processing information.[70] This was "intended to prevent unauthorized access to health information by other divisions or affiliates outside the clearinghouse."[71] However, in situations where HIPAA does not apply, the rights of the individual are unknown. Since HIPAA does not regulate these entities, if a non-covered entity gains access to a consumer's PHI, they may be able to share that information with third parties even though this is not governed by law.[72]

The HIPAA Privacy Rule was revised in 2002 and requires "appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization."[73] In addition, the rule authorizes "patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections."[74]

Not all medical apps are regulated by HIPAA. The criteria includes, the type of entity[75] that uses the app, the data[76] the app generates, stores, and shares, and

---

64 *Summary of the HIPAA Security Rule*, *supra* note 62.

65 45 C.F.R. §164.306 (2013); *see also Summary of the HIPAA Security Rule*, *supra* note 62.

66 Greg Slabodkin, *FTC Steps Up Protection of Consumer Health*, HEALTH DATA MGMT. (Mar. 23, 2016), http://www.healthdatamanagement.com/news/ftc-steps-up-privacy-security-protection-of-consumer-health-data (providing that the FTC Act prohibits unfair and deceptive practices and allows the FTC to bring enforcement actions against companies that do not maintain appropriate data security practices).

67 U.S. DEP'T OF HEALTH & HUMAN SERV., EXAMINING OVERSIGHT OF PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 5 (2016).

68 *Id.*

69 Frangoise Gilbert, *HIPAA Privacy and Security*, *in* A GUIDE TO HIPAA SECURITY AND THE LAW 10 (Stephen S. Wu ed., 2007).

70 *Id.*

71 *Id.*

72 U.S. DEP'T. OF HEALTH & HUM. SERV., *supra* note 67, at 22.

73 *The HIPAA Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es (last visited Feb. 17, 2017).

74 *Id.*

75 Iryna Pototska, *What HIPAA Requirements Apply to Medical App Devices*, YALANTIS, https://yalantis.com/blog/what-hipaa-requirements-apply-to-medical-app-development/

the software[77] that powers the app.[78]

In 2009, the Office for Civil Rights enacted the Health Information Technology for Economic and Clinical Health (HITECH) in order to "strengthen the privacy and security" portions of HIPAA regulations.[79] The HITECH program authorized the Office of the National Coordinator (ONC) to "manage and set standards for the stimulus program."[80]

In addition, the HIPPA omnibus rule was passed to amend the HIPAA Privacy, Security and Enforcement Rules to implement statutory amendments under the HITECH Act and to strengthen privacy and security protections for health information.[81]

Traditionally, health care was provided in person and paid through health insurance.[82] The traditional means of insuring privacy was through HIPAA, state regulated privacy laws, and the Federal Trade Commission Act.[83] HIPAA regulations are enforced by implementing the Privacy, Security, and Breach Notification Rules and the Office of Civil Rights and at times the Department of Justice.[84] There has been "a dramatic advancement in adoption and use of health IT, in the seven years since the HITECH Act was enacted."[85]

(last visited Feb. 27, 2017) (providing that if an app is designed to facilitate doctor-patient interactions, it must comply with HIPAA regulations. This is determined by knowing if the covered entity or non-covered entity is originally governed by HIPAA regulations before the app is developed).

76 *Id.* (providing that data includes Protected Health Information which incorporates personal data, fingerprints, and voiceprints).

77 *Id.* (stating software standards include audit controls, integrity, and access controls. Audit controls ensures that a medical app developer implements hardware, software, and procedural mechanisms that record and examine activities containing or using EPHI).

78 *Id.*

79 Press Release, HHS Press Office, New rule protects Patient privacy, secures health information, (Jan. 17, 2013), (on file with HHS) (explaining that the Act was signed into law as part of the American Recovery and Reinvestment Act of 2009 economic stimulus bill).

80 Margaret Rouse, *HITECH Act*, SEARCHDATAMANAGEMENT, http://searchhealthit.techtarget.com/definition/HITECH-Act (last visited April 20, 2017).

81 Margaret Rouse, *HIPAA omnibus rule (Health Insurance Portability and Accountability Act of 1996 omnibus rule)*, SEARCHDATAMANAGEMENT, http://searchhealthit.techtarget.com/definition/HIPAA-omnibus-rule-Health-Insurance-Portability-and-Accountability-Act-of-1996-omnibus-rule (last visited April 20, 2017). HIPAA omnibus rule was enacted by the U.S. Dep't. of Health and Human Services' Office of Civil Rights to modify the HIPPA Privacy, Security and Enforcement Rules to implement statutory amendments under the HITECH Act.

82 U.S. DEP'T. OF HEALTH & HUM. SERV., supra note 67, at 3.

83 *Id.*

84 *Id.* at 12.

85 *Testimony before the Committee on Oversight and Government Reform, Subcommittees on Information Technology and Health Care, Benefits, and Administrative Rules*, 114th Cong. (2016) (Statement of Karen B. DeSalvo, M.D., M.P.H, M.Sc., Nat'l Coordinator for

Breaking free of these traditional measures has provided convenience, unfortunately, as consumers become increasingly active and share personal data online, organizations not regulated by HIPAA or HITECH are using, collecting, and sharing consumer data that may be inappropriate and put consumers at risk.

D. The Effect of HIPAA on Health Apps

HIPAA does not apply to all medical apps, but it does affect research that uses, creates, or discloses PHI.[86] For example, if a non-covered entity designs an application and a consumer buys that application, the data collected by that specific device is not covered under HIPAA.[87]

Digitizing health information has many potential benefits including reducing costs and increasing medical accuracy.[88] One key example of digitized health information is an electronic health record ("EHR").[89] An EHR is a digital version of a patient's paper medical record or chart. EHRs make information available instantly and securely to authorized users.[90] They can contain the medical and treatment history of a patient, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results.[91] These records can also give a provider access to evidence-based tools for making decisions about a patient's care and can automate certain workflows. [92]

There are multiple benefits of mobile health apps, including the ability for providers to improve and care, patient engagement, communication, and decrease health costs.[93] An example of a mobile health app is the Radiation Emergency Medical Management (REMM) app which provides health care providers with medical assistance and guidance with diagnosing and treating radiation injuries.[94] Mobile health apps and privacy are regulated by the Food

---

Health Info. Technology).

86 According to the U.S. Dep't of Health & Human Services there are "18 classes of personal information that constitute PHI" including name, date of birth, phone numbers and social security numbers. Iryna Potoska, *What HIPPA Requirements Apply to Medical App Development*, YALANTIS, https://yalantis.com/blog/what-hipaa-requirements-apply-to-medical-app-development/ (last visited Nov. 26, 2011).

87 *Id.*

88 Devon Herrick et al., Health Information Technology: Benefits and Problems, NAT'L CTR. FOR POL. ANALYSIS 1 (Apr. 2010), http://www.ncpa.org/pdfs/st327.pdf.

89 *Id.*

90 *Id.*

91 *What is an Electronic Health Record (EHR)?*, *supra* note 13.

92 *Id.*

93 *See MHealth: Mobile Technology Poised To Enable A New Era In Healthcare*, EY, http://www.ey.com/Publication/vwLUAssets/mHealth/ (last visited Feb. 17, 2017).

94 *Mobile Medical Applications*, *supra* note 2.

and Drug Administration, Federal Trade Commission, and HIPAA.

The increase in smartphones and mobile apps has changed the way consumers communicate and has increased competition to produce more useful apps. Smartphones have become consumers' "life line" as they are not only for personal use, but work, family, finances, and now health.[95]

Although this has made access to medical information more convenient and there are benefits to health apps, these same apps may pose a threat to privacy and security.[96] Few consumers read through terms of service or privacy policies before clicking "I Agree" to access the features of the app.[97] Allowing a consumer to automatically agree increases the chances that they are not fully aware of who is receiving that data.[98] This lack of awareness is why mobile health apps may also be regulated by the Federal Trade Commission Act and the Food and Drug Administration.[99]

E. Food and Drug Administration ("FDA")

In a 2011 press release, the director of the Food and Drug Administration's Center for Devices and Radiological Health, Jeffrey Shoran, M.D., J.D., stated: "[t]he use of mobile medical apps on smart phones and tablets is revolutionizing health care delivery."[100] The FDA began regulating this revolution in 1989 when they generated a "policy statement on how to determine if a computer or software product was a device and how the FDA intended to regulate."[101] However, recognizing that technology was changing and diversifying the "Draft Software Policy" was withdrawn in 2005.[102]

In addition, the FDA defines and regulates devices and their manufacturers and has stated "certain mobile medical apps can pose potential risks to public health."[103] The FDA has also stated that if "stand-alone software is used as to analyze medical device data; it is regulated as an accessory to a medical device or as medical device software."[104] According to FDA data, "by 2018, 50 per-

95 Cory Fox, *Personal Smartphones: A Ticking HIPAA/HITECH Time Bomb?*, JD SUPRA (Apr. 10, 2013), http://www.jdsupra.com/legalnews/personal-smartphones-a-ticking-hipaahi-00665/.

96 U.S. DEP'T. HEALTH AND HUM. SERV., *supra* note 67, at 3.

97 Flaherty, *supra* note 47, at 421-23.

98 *Id.*

99 *Id.*

100 Press Release, U.S. Food & Drug Admin., *FDA Outlines Oversight of Mobile Medical Applications* (July 19, 2011), (on file with author).

101 U.S. FOOD & DRUG ADMIN., *supra* note 3, at 6.

102 *Id.*

103 *Id.*

104 *Id.*

cent of 3.4 billion smartphone and tablet users will have downloaded mobile health applications."[105]

On February 9, 2015, the FDA released an update to their "Guidance for Industry and Food and Drug Administration Staff."[106] In these provisions the FDA defines mobile medical applications[107] and mobile applications.[108] The FDA[109] applies a risk-based analysis when an agency uses a medical app in order to ensure safety and effectiveness and regulates moderate or high-risk mobile apps.[110] If a medical device is not considered high-risk it may not be subject to FDA regulation.[111] The FDA may "exercise enforcement discretion" when it applies to low risk medical devices, therefore, applications that access and display personal information may not be regulated.[112]

The FDA does regulate mobile applications that:

> "[h]elp patients/users self-manage their disease or condition without providing specific treatment suggestions; [p]rovide patients with simple tools to organize and track their health information; [p]rovide easy access to information related to health condition or treatments; [a]utomate simple tasks for health care providers; [and] [e]nable patients or providers to interact with Personal Health Records ("PHR") or [E]lectronic [H]ealth [R]ecords ("HER") systems."[113]

Furthermore, an analysis of free and paid applications showed that most unencrypted data was sent to advertisers, including personal information.[114] Finally, the FDA does not regulate mobile medical applications that "function as an electronic health record or a personal health record system."[115]

Although there are multiple guidelines to ensure consumer privacy, it is not

---

105 *Mobile Medical Applications*, *supra* note 2.

106 U.S. FOOD & DRUG ADMIN., *supra* note 3, at 4.

107 A "mobile medical app" is a mobile app that meets the definition of device in section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and either is intended: to be used as an accessory to a regulated medical device; or to transform a mobile platform into a regulated medical device. *Id.* at 7.

108 A mobile application or "mobile app" is defined as a software application that can be executed (run) on a mobile platform (i.e., a handheld commercial off-the shelf computing platform, with or without wireless connectivity), or a web-based software application that is tailored to a mobile platform but is executed on a server. *Id.*

109 The Food and Drug Administration "recognizes the extensive variety of actual and potential functions of mobile apps, the pace of innovation, and the potential benefits and risks to public health represented by these apps." *Id.* at 4.

110 *Mobile Medical Applications*, *supra* note 2.

111 *See id.*

112 *See id.* A mobile app is determined as a device by its intended use. Intended use may be shown by "labeling claims, advertising materials, or oral or written statements by manufacturers or their representatives." U.S. DEP'T OF HEALTH & HUMAN SERV.'S FOOD & DRUG ADMIN., *supra* note 3, at 8.

113 *See Mobile Medical Applications*, *supra* note 2.

114 *Healthcare On-The-Go: Pros and Cons of Mobile Health Apps*, SUPPLEMENTAL HEALTH CARE BLOG (Aug. 27, 2013), http://blog.supplementalhealthcare.com/patient-care-forum/healthcare-on-go-pros-and-cons-of-mobile-health-apps.

115 *See Mobile Medical Applications*, *supra* note 2.

enough. Additionally, the increase in the amount of corporations investing in mobile health apps[116] is driving the need for additional regulations. Applications that may be regulated by the FDA include "[a]pps that display medical device data to allow patient monitoring and apps that use a mobile platform reader."[117]

In 2016, the FDA drafted guidance on sharing medical device data with patients. The FDA released this guidance to "clarify that manufacturers may share patient-specific information recorded, stored, processed, retrieved, and derived from medical devices with a patient."[118] The FDA also regulates mobile medical app manufacturers. According to FDA guidelines, mobile medical apps are "software programs that run-on smartphones and other mobile communication devices."[119]

II. DATA COLLECTION

A. Data

Roughly 63 percent of global population and 91 percent of American adults use or own smartphones, and roughly the same percentage download applications to their smartphone.[120] In 2015, nearly "one and a half billion smartphone

---

116 *See generally* Flaherty, *supra* note 47, at 432-37 (discussing how the rise in industrial compilation of smartphone user's information, particularly with respect to health-related apps, instigated an increase in regulation by the Federal Communications Commission, the Federal Trade Commission, the Office for Civil Rights of the Department of Health and Human Services, and the National Institute of Standards and Technology).

117 *Id.* at 423.

118 U.S. DEP'T OF HEALTH & HUMAN SERV.'S FOOD & DRUG ADMIN., DISSEMINATION OF PATIENT-SPECIFIC INFORMATION FROM DEVICES BY DEVICE MANUFACTURERS 4 (June 10, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm505756.pdf.

119 *See Mobile Medical Applications*, *supra* note 2.

120 *Mobile Fact Sheet*, PEW RESEARCH CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ (noting that 77% of Americans own smartphones); Jacob Poushter, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, PEW RESEARCH CTR. 18 (Feb. 22, 2016), http://www.pewglobal.org/files/2016/02/pew_research_center_global_technology_report_final_february_22__2016.pdf (analyzing the percentage increase in global smartphone ownership since 2013); Maeve Duggan, *Cell Phone Activities 2013*, PEW RESEARCH CTR. (Sept. 13, 2013), http://pewinternet.org/Reports/2013/Cell-Activities.aspx (recognizing that 50% of cell phone owners in the United States use their phone to download apps); *See also* Alex Krause, *iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices*, 9 IND. HEALTH L. REV. 731, 732 n.3 (2012) (citation omitted) (defining "smartphone" as "[a] cellular telephone and handheld computer with built-in applications and Internet access. Smartphones provide digital voice service as well as text

users had at least one mobile health app on their phone."[121] Many of these consumers trust that their information will remain private.[122]

Furthermore, a study conducted by BMC Medicine revealed that roughly "89 percent of apps transmitted information to online services."[123] In addition, that 66 percent of apps sending identifying information over the internet did not use encryption and 20 percent had no privacy policy."[124] These applications collected health data. Health data includes:

> (1) archetypal personal data provided by the user, such as name and address; (2) fitness and health-related data provided by the user, such as height, weight, and fitness activities; (3) information collected by the app during use; (4) information shared through the app's social media component; (4) information measured by sensors on the mobile device, such as heart rate; (5) information provided by the mobile device itself, such as geolocations; (6) aggregated data from the above; (7) behavior tracking[125] data prepared by third party analytics firms; and (8) user data collected by advertisers during use.[126]

B. mHealth Technology

Another method of data collection is through mHealth technology.[127] mHealth technology allows consumers to monitor their daily activities and record data outside of doctors' visits.[128] mHealth technology includes wearable

---

messaging, e-mail, web browsing, still and video cameras, MP3 player, video viewing and often video calling. In addition to their built-in functions, smartphones can run myriad applications, turning the once single-minded cellphone into a mobile computer.").

121 Vera Gruessner, *Too Many Apps Lack Strong Mobile Health Security Features*, MHEALTH INTELLIGENCE (Oct. 12, 2015), http://mhealthintelligence.com/news/too-many-apps-lack-strong-mobile-health-security-features.

122 *See* Flaherty, *supra* note 47, at 432 (quoting William Enck et al., *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, 32 ACM TRANSACTIONS ON COMPUTER SYS., no. 2, June 2014, at 5:1, 5:2).

123 Kit Huckvale et al., *Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment*, BMC MEDICINE 6 (2015), http://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-015-0444-y.

124 *Id.* at 1.

125 Advertising and marketing agencies use behavior tracking to tailor advertisements for specific users. "Behavior tracking" is a set of online techniques used to collect and interpret the fitness app user activity as they use apps, visit websites, and engage in other Internet activity. *See* Lori Deschene, *What is Behavioral Targeting?*, CBS MONEY WATCH, http://www.cbsnews.com/news/what-is-behavioral-targeting/ (last updated June 17, 2008).

126 William A. Tanenbaum & Lourdes M. Turrecha, *Are Fitness Apps Fit for Privacy Protection?*, HEALTHCARE INFORMATICS (Sept. 28, 2016), http://www.healthcare-informatics.com/article/mobile/are-fitness-apps-fit-privacy-protection.

127 U.S. DEPT. HEALTH AND HUMAN SERVICES, *supra* note 67, at 29-30 (discussing the absence of clear guidance surrounding the privacy and security of health information accumulated, disseminated, and utilized by entities that are not currently subject to HIPAA).

128 *Mobile Technology Poised to Enable a New Era in Healthcare*, ERNST & YOUNG 47 (2012), http://www.ictliteracy.info/rf.pdf/mHealth%20Report_Final.pdf.

sensors, tablets, smartphones, and software applications.[129] These applications allow data to be stored locally or with a vendor.[130] Therefore, when an app is sold directly to a consumer and not offered by a HIPAA covered entity or a business associate these vendors will not fall under HIPAA. This means that these entities can share information with third party vendors, including advertisers.[131] For example, an application sold directly from an app store and downloaded strictly by the consumer to manage their own health data is not regulated by HIPAA.[132]

Even though there is "not a single comprehensive law regulating the collection of personal data"[133] when a privacy interest is recognized, there are at least two branches of informational privacy law in the United States, traditional privacy law and data protection law.[134] Traditional information privacy concerns an individual's claim to prevent the disclosure of sensitive or confidential information. It also addresses issues that allow "individuals to prevent others from knowing, discovering, or disclosing sensitive and confidential information pertaining to the private life of the individual."[135] Data protection is necessary if a network contains sensitive information or PII. This protection "focuses on an individual's claim to control, use, or disclose *PII (or, increasingly, information that is not identifiable to a person but might identify a device they typically use) whether or not that information is confidential or sensi-*

---

129 The House Energy and Commerce Committee regulates health information technology. *See also PA Rep. Costello Highlights Importance of 21st Century Technology to Deliver #CuresNow*, THE ENERGY AND COMMERCE COMM. (Oct. 28, 2016), https://energycommerce.house.gov/news-center/news/pa-rep-costello-highlights-importance-21st-century-technology-deliver-curesnow (citing Ryan Costello, *Utilizing technology to improve healthcare*, DAILY LOCAL (Oct. 24, 2016), http://www.dailylocal.com/opinion/20161024/utilizing-technology-to-improve-healthcare (articulating opinions of the U.S. Representative and Energy and Commerce Committee member).

130 A vendor would be considered a third party. Third parties are considered entities not controlled by an organization or by a common control or ownership. *See, e.g.*, *The A7 Revolution*, ANDAMAN7, http://www.andaman7.com/en/a7-revolution (last visited Feb. 18, 2017) (detailing how healthcare professionals and patients, through the Andaman7 healthcare app, may collaborate through a peer-to-platform).

131 *See* U.S. DEPT. HEALTH AND HUMAN SERVICES, *supra* note 67, at 29-30.

132 *Id.* at 9.

133 Arti Sangar, *Data Privacy Protection: A Serious Business for Companies*, INT'L LAW NEWS (Fall 2012), http://www.americanbar.org/publications/international_law_news/2012/fall/data_privacy_protection_serious_business_companies.html.

134 1-1 DATA PRIVACY, PROTECTION, AND SECURITY LAW § 1.02 (2015).

135 *Id.* (citing 9 R.T. Nimmer, Information Law 8:2 (2014 Supp.)). *See* Hallstein v. City of Hermosa Beach, 87 Fed. Appx. 17 (9th Cir. 2003) (unpublished) (holding there is no reasonable expectation of privacy in a license plate when the information is voluntarily exposed to the public).

tive in nature."[136] However, mHealth technology may be subject to the FTC Act, as in *FTC v. New Consumer Solutions LLC*, where the FTC settled with two marketers for deceptively claiming their mobile applications could detect melanoma.[137]

In *Busse v. Motorola*, the court determined that there are four ways to claim an action for invasion of privacy: (1) intrusion upon the seclusion of another, (2) appropriation of another's name or likeness, (2) public disclosure of private facts, and (4) publicity placing another in a false light.[138] In addition, the court stated that the intrusion must be purposeful.[139] Most providers agree that mHealth Technology "can improve outcomes, reduced health care cost, and time saved."[140]

C. Federal Trade Commission ACT

The mission of the Federal Trade Commission ("FTC") is to prevent deceptive business practices that are unfair to the consumer and to increase informed consumer choices.[141] The FTC also initiates policy that promotes privacy and data security. Thus, another way privacy and data is regulated is through the Federal Trade Commission Act.[142] The FTC enforces statutes and rules that protect consumer data and impose obligations upon businesses.[143] This applies to anyone involved in the buying and selling of goods.[144] A person or company is involved in unfair acts or practices when the act "causes or is likely to

136 *Id.*

137 FTC v. New Consumer Solutions LLC, et al., No.15-cv-01614 (N.D. Ill. Apr. 30, 2015).

138 Busse v. Motorola, Inc., 813 N.E. 2d 1013, 1017 (Ill. App. Ct. 1st Dist. 2004).

139 *Id.* (''One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.'') (citing Restatement (Second) of Torts § 652B, at 378 (1977)).

140 U.S. DEPT. HEALTH AND HUMAN SERVICES, *supra* note 67.

141 *About the FTC*, FTC, http://www.ftc.gov/about-ftc (last visited Nov. 27, 2016).

142 15 U.S.C. § 41. The FTC Act allows the Commission to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress and the public. *See also Federal Trade Commission Act*, FTC, https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act (last visited Feb. 18, 2017).

143 15 U.S.C. § 45(a); 15 U.S.C. §§ 6801-6809; 15 U.S.C. § 1681; 15 U.S.C. §§ 6501-6506; *See also* 16 C.F.R. Part 312.

144 15 U.S.C. § 45(a).

cause substantial injury to consumers, cannot be reasonably avoided by consumers, and is not outweighed by countervailing benefits to consumers or to competition."[145]

Companies are in danger of violating the FTC ACT if they provide misleading statements or omissions to consumers including statements and omissions regarding privacy or data security.[146] An example of this is found in the final FTC order from *FTC v. Payments MD, LLC*.[147] The FTC charged Payments MD with violating consumers' privacy by collecting personal medical information without their consent. The complaint stated that Payments MD and CEO Michael C. Hughes used personal consumer data without their consent and altered the signup process for a health billing site to include permission to collect sensitive health information for an electronic health record portal site.[148] The FTC ruled that the company's practices violated Section 5.5 of the FTC Act by creating a situation to consumers that was unreasonably avoidable and did not benefit the consumer or competition.[149] Consequentially, PaymentsMD was required to provide how the information they collect could possibly be shared with a third party and was required to get consumer consent before obtaining health information from a third party.[150]

The FTC's authority extends to both HIPAA and non-HIPAA covered entities;[151] however this authority "does not apply to nonprofit entities or practices that are in the business of insurance to the extent that such business is regulated by state law."[152] Therefore, since state laws vary, it would be difficult to determine if these businesses would be required to report security infringements.[153]

The FTC also has authority to enforce data security in health care. An ex-

---

145 *Id.*

146 *Opportunities and Challenges in Advancing Health Information Technology Before the Sub. Comm. On Info. Tech. and Health, Benefits, and Admin. Rules of the H. Comm. On Oversight and Gov. Reform*, 155th Cong. 2-4 (2016) (statement of Jennifer Rich, Director of the Bureau of Consumer Protection at the FTC).

147 Press Release, FTC, FTC Approves Final Order in PaymentsMD Privacy Case (Feb. 6, 2015) (on file with FTC).

148 *Id.*

149 *Supra* note 146.

150 Press Release, FTC, Medical Billing Provider and its Former CEO Settle FTC Charges That They Misled Consumers About Collection of Personal Health Data (Dec. 3, 2014) (on file with the FTC).

151 *Supra* note 146.

152 15 U.S.C. §§ 44 & 45(a). The FTC does not have jurisdiction under the FTC Act over most non-profit organizations, although it does have jurisdiction over sham charities or other non-profits that in actuality operate for profit.

153 *Non-HIPAA Covered Entities: Privacy and Security Policies and Practices of PHR Vendors and Related Entities Report*, MAXIMUS FEDERAL SERVICES 1 (Dec. 13, 2012), https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf.

ample of this is in 2008, when Tiversa, Inc. notified LabMD that it had received sensitive patient information from LabMD.[154] The FTC began an investigation of LabMD[155] in 2010 after learning of this breach and filed a complaint alleging that LabMD failed to "reasonably protect the security of consumers' personal data, including medical information."[156] The complaint states that on two LabMD exposed the "personal information of approximately 9,300 consumers"[157] and that consumer information "was found on a [peer-to-peer file-sharing] network through Limewire"[158] and documents containing "personal information, such as names and SSNs, of several hundred consumers" were found in the hands of identity thieves."[159]

Finally, Congress enacted the Mobile Device Privacy Act in 2012 which advised the FTC to create regulations on manufacturers and sellers of mobile devices to disclose to consumer's information about the installation and purpose specific software.[160]

III. ANALYSIS

As access becomes easier, there are important privacy concerns for U.S. consumers resulting from mobile advertising practices. These concerns are "the collection, use, and disclosure of consumers' personally identifying information that accompanies mobile advertising and the generation of unsolicited mobile advertising."[161]

Health data applications allow individuals to live a better lifestyle.[162] However, in 2015, 92% of health institutions used non HIPAA-compliant messaging apps.[163] Unfortunately, health related applications not regulated by HIPAA

---

154 LABMD, Inc. v. Fed. Trade Comm'n, 776 F.3d 1275, 1277 (11th Cir. 2015).

155 *Id.*

156 *Id.*

157 Complaint at 4-5, In the Matter of LabMD, Docket 9357 (Aug. 28, 2013).

158 *Id.*

159 *Id.*

160 The Mobile Device Privacy Act was introduced to the house in 2012 by Rep. Edward Markey to ensure regulations requiring sellers or manufacturers of mobile devices and software to disclose to consumer's information about the installation and purpose of such software. *See* Mobile Device Privacy Act, H.R. 6377, 112th Cong. (2012).

161 Ashton McKinnon, *Sacrificing Privacy for Convenience: The Need for Stricter FTC Regulations in an Age of Smartphone* Surveillance, 34 J. OF THE NAT'L ASS'N OF ADMIN. LAW JUD. 486, 492 (2014).

162 Stuart Lier, *Health apps and HIPAA: APIs as tools for protecting health data*, PROGRAMABLEWEB.COM (Jan. 14, 2015), http://www.programmableweb.com/news/health-apps-and-hipaa-apis-tools-protecting-health-data/analysis/2015/01/14.

163 *2015 Infinite Convergence Mobile Messaging for Healthcare Institutions Study Finding Sheet*, NETSFERE 4 (2015), https://www.netsfere.com/downloads/2015_infinite_convergence_mobile_messaging_for_healthcare_institutions_study_findings_sheet.pdf.

create multiple privacy and security concerns. These applications often ask consumers to enter private and personal information, yet transmit unencrypted information to advertising and data analysis sites without consumer consent.[164] Although there are multiple benefits to utilizing health applications – for example the ability to track health information – these non-HIPAA regulated entities should be governed,[165] especially because if a consumer is unaware of the repercussions of data sharing it can lead to unintended loss of privacy and the misuse of data.[166] Therefore, HIPAA should include non-covered entities and create stricter guidelines of data usage with the assumption of nondisclosure.[167] Additionally, rules governing health information should maintain the balance between the need for patient privacy and the sharing of patient data.[168] Furthermore, privacy laws should set stricter standards on who has control and use of personally identifiable information.[169] Finally, the numerous lawsuits reveal that the miscommunication has led to a level of legal uncertainty regarding HIPAA regulations and data sharing.[170]

In a recent report, the Department of Health and Human Services analyzed five areas that HIPAA and NCEs lacked protection and why there is a need to change the law.[171] The report stated that consumers do not have the same rights when trying to obtain personal data from a covered entity (CE) or business associate versus non-covered entities (NCE).[172] Since NCE's are not required to provide consumers with access to data, consumers may not be able to obtain requested PII if shared through health apps or mHealth technology.[173] If consumers disclose their own PII though health social media, it may be outside the reach of HIPAA.[174]

Furthermore, there is a difference in the type of encryption,[175] adequacy of safeguards, and security standards between covered entities and non-covered

---

164 Flaherty, *supra* note 47, at 417.

165 *Id.* at 419.

166 STEVE OLSON AND AUTUMN S. DOWNEY, SHARING CLINICAL RESEARCH DATA loc. Chapter 3 (2013) (ebook).

167 *Id.*

168 *Ensuring Privacy and Security of Health Information Exchange in Pennsylvania*, PAEHI 3 (2014) http://www.paehi.org/_files/live/Privacy_WhitePaper_2014_FINAL.pdf.

169 1-1 DATA PRIVACY, PROTECTION, AND SECURITY LAW § 1.02 (2015).

170 OLSON AND DOWNEY, *supra* note 166.

171 U.S. DEP'T OF HEALTH AND HUMAN SERVICES, *supra* note 67, at 20.

172 *Id.* at 5.

173 *Id.* at 20.

174 *Id.* at 9-10.

175 *Id.* at 23. Valid encryption processes for data must be at rest and in motion to comply with NIST Special Publication 800-111. In addition, "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" 45 C.F.R. § 164.304 (2013).

entities.[176] Moreover, the third-party use for NCEs and CEs needs to be addressed.[177] The largest discrepancy is marketing. Although HIPAA limits the information disclosed to third parties, the information disclosed to NCEs are not subject to these same protections and may receive unauthorized marketing if the "NCE [does] not promise to not use the data in such a manner."[178] Thus if HIPAA does not apply, consumers may not have the right or ability to access information accessed by third parties.[179]

Encryption is important.[180] Many times a consumer log into their apps with a user name and password, however a study found that "only six percent of free apps and fifteen percent of paid apps used encrypted connection when sending data to third parties."[181] Since federal law has been silent, some states have enacted stricter privacy protections while others have not. While useful, this can lead to a general misunderstanding of what laws do and do not apply and if the state law preempts federal law. Additionally, privacy notices must be clear, efficient, and notice should be required. The consumer must know what the agreement is stating. Privacy policies should not use industry jargon since this can overwhelm the reader.[182] NCEs should be required to act with the same level of transparency as CEs. Under HIPAA, consumers should know when and how information is being collected, just as CEs understand to whom and what information they can disseminate. The issue is that if information is transmitted to a non-covered entity, "the protections of HIPPA may not apply," thereby disadvantaging the consumer.[183]

In 2016, there a number of mergers between health-focused companies and tech companies.[184] Large companies like Nokia Technologies are acquiring smaller companies like health device maker Withings,[185] which makes weight scales, blood pressure cuffs, trackers, and thermometers.[186] Asics acquired Runkeeper, an application designed to track outdoor fitness activities, for $85 million.[187] As large entities continue to acquire smaller organizations, the need

---

176 U.S. DEP'T OF HEALTH AND HUMAN SERVICES, *supra* note 67, at 23.

177 U.S. DEP'T OF HEALTH AND HUMAN SERVICES, *supra* note 67, at 23-4. Third Parties are entities not governed by an organization or business association i.e. a vendor. *Id.*

178 *Id.* at 22.

179 *Id.* at 5.

180 *Id.* at 23.

181 *Id.*

182 *Id.*

183 *Id.* at 22.

184 Heather Mack, *A closer look at the 30 mergers and acquisitions of 2016*, MOBILEHEALTHNEWS, http://www.mobihealthnews.com/content/closer-look-30-mergers-and-acquisitions-2016 (last visited Feb. 17, 2016).

185 *Id.*

186 *Id.*

187 *Id.* Runkeeper is a tracking device that allows users to set goals, create a plan, and track their runs. Consumers are asked to either create an account, or log in with either their

for data security increases and regulation of these large companies needs to be investigated.[188] Under HIPAA, many of these larger organizations do not fall under a cover entity and therefore may not be subject to HIPAA enforcement.[189]

In addition, there needs to be clear and effective guidelines on how to properly draft a privacy policy that will provide a consumer with a transparent view of how their information is being disclosed and collected.[190] First, mobile application privacy policies must be easily understood by consumers. They should provide accurate information that describes the data collection and use policy, as well as inform the user of the risks and rewards of the mobile app.[191] Secondly, consumers should be provided with a choice as to whether they would like to share personal information. This is only possible if there is a level of transparency that provides the consumer with such a choice.[192] In order for policymakers to keep up with changing times there must be an ongoing dialogue between technologist and politicians. Policymakers need to have a discussion with developers regarding reasonable security measures and best practices.[193]

Companies handling PII that use service providers to handle data should ensure that service provides are capable of providing and maintaining security.[194] In addition, companies handling secure data should take steps to protect data and take additional measures to protect consumer data. [195]

Compare data information in an app to cookies on a desktop computer.[196] The regular consumer knows that if you don't want a website tracking your information you delete the cookie history from your browser. However, users of applications are not entitled to the same benefits of deleting these cookies from data-collecting apps;[197] and once information is released from a covered

---

Facebook or Google accounts. *See generally Homepage*, RUNKEEPER, https://runkeeper.com/index (last visited Feb. 17, 2017).

188 *Id*.

189 *Id*.

190 Buchta, *supra* note 38, at 1, 2.

191 *Id*.

192 *Id*.

193 FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 53 (2016), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

194 *Id*. at 34, n. 139.

195 *Id*. at 33-34.

196 *What Are Cookies? Computer Cookies Explained*, WHATARECOOKIES.COM, http://www.whatarecookies.com/ (last visited Feb. 18, 2017) (web cookies are small files sent from a website that store data specific to a user or website).

197 McKinnon, *supra* note 161, at 492.

entity, the protections of HIPAA may not apply.[198] Moreover, companies should take additional steps to secure information.[199] For example, companies could take an in-depth defense approach.[200] A company taking this approach would be required to examine its security on multiple levels, including data passed over home networks.[201]

IV. HIPAA-COMPLIANT APPLICATIONS

Recently, the U.S. Department of Health and Human Services marked its 12th HIPAA settlement.[202] In October 2016, St. Joseph's Health in California agreed to settle for $2.14 million for violating HIPAA laws.[203] In 2012, St. Josephs notified the Office of Civil Rights (OCR) that files containing PHI were accessible via the internet for over a year disclosing the information of roughly 31,800 individuals.[204] Although there have been multiple suits, there are health apps that are HIPAA-compliant like AirStrip, which allows physicians to view live patient data remotely.[205] In addition, apps like Fitbit, Google Fit, and Smart Text are also HIPAA-compliant.[206] These applications show how an application can be HIPAA-compliant and still provide the typical user with important information.

A. FitBit

Fitbit is the newest form of wearable technology.[207] The information gath-

198 Samuels & DeSalvo, *supra* note 1, at 8.

199 PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 193, at 30.

200 *Id.*

201 *Id.*

202 Amy Butler, C*alifornia's St. Joseph Health Agrees to $2.14 Million HIPAA Settlement*, LINKEDIN (Oct. 19, 2016), https://www.linkedin.com/pulse/californias-st-joseph-health-agrees-214-million-hipaa-amy-butler?articleId=6194633210039713793.

203 Press Release, Dep't of Health and Human Serv., $214 million HIPAA settlement underscores importance of managing security risk (Oct. 18, 2016) (on file with author).

204 *Id.*

205 *Airstrip Technologies adds Diversinet HIPAA-compliant SD*, HEALTHIT SECURITY (Dec. 17, 2012), http://healthitsecurity.com/news/airstrip-adds-diversinet-hipaa-compliant-sdk.

206 *See Fitbit Extends Corporate Wellness Offering with HIPAA Compliant Capabilities*, FITBIT (Sept. 16, 2015), https://s2.q4cdn.com/857130097/files/doc_news/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities.pdf (announcing FitBit is HIPPA compliant); *see also Terms and Conditions*, GOOGLE FIT (Oct. 28, 2014), https://developers.google.com/fit/terms; *Privacy Policy*, TELMEDIQ, https://www.telmediq.com/privacy-policy/ (explaining how and why information is collected from users).

207 *See* Karla Grossenbacher, *Wearable Device Data: The Next Big Thing for Employment Litigation Cases*, LEXOLOGY (Sept. 23, 2016),

ered by this device can be personal, but information can be gathered directly from the manufacturer or the device itself.[208] FitBit released Fitbit for your placenta, which allows women to monitor their pregnancy and ensure healthy fetal development.[209] Users authorize Fitbit to access their personal information, including date of birth and email address.[210] Fitbit announced that it became HIPAA-compliant in 2015.[211] Fitbit complying with HIPAA regulations shows that HIPAA no longer governs just insurance agencies but can also govern businesses.[212]

B. Google Fit

Google Fit is another application that is HIPAA compliant and has protected consumer information while allowing the consumer to track and maintain his or her fitness data. Google Fit collects a user's heart rate, steps, time of activity, weight, and gender.[213]

Google Fit provides guidance for consumers and developers. According to its website, Google Fit collects information provided to them, information from a consumer's use of service, and it states that it uses this information in order to "provide, maintain, protect, and improve" the application and also to "protect Google and its users."[214] Google's privacy policy explains what information they collect, why they collect it, how they use it, and how to access and update information.[215] Google collects device specific information from their

---

http://www.lexology.com/library/detail.aspx?g=cc856253-1bd4-43f2-8a62-a00ddd0212d4 (wearable devices offer immediate data that allow users to access their own health and fitness information such as a consumer's calories, diet, heart rate, blood glucose levels, and location).

208 *Id.*

209 Adrienne LaFrance, *A Fitbit for Your Placenta*, THE ATLANTIC (Sept. 29, 2016), http://www.theatlantic.com/health/archive/2016/09/a-fitbit-for-your-placenta/502157/.

210 *See Privacy Policy*, FITBIT (Aug. 9, 2016), https://www.fitbit.com/legal/privacy-policy#collect (last visited Feb. 18, 2017).

211 Michal McAlpen, *Fitbit is now HIPAA compliant – is your business?*, CIO (Oct. 2, 2015), http://www.cio.com/article/2988280/compliance/fitbit-is-now-hipaa-compliantis-your-business.html.

212 *See Fitbit Extends Corporate Wellness Offering with HIPPA Complaint Capabilities*, FITBIT (Sept. 16, 2015), https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx ("Fitbits meet HIPPA compliance to ensure safeguarding new business and protecting consumers' privacy in order to keep their data secure.").

213 Joram Teusink, *Android Wear and Google Fit and its privacy and security*, TEUSINK (Feb. 13, 2015), https://www.teusink.eu/2015/02/android-wear-and-google-fit-security-privacy.html.

214 *Welcome to the Google Privacy Policy*, GOOGLE (Aug. 29, 2016), https://www.google.com/policies/privacy/.

215 *Id.*

consumers in order to improve the services they provide their consumers.[216]

Google also collects device-specific information and can associate device identifiers or a phone number with a consumer's account.[217] Google formatted its policy provisions in an easy layout, allowing the consumer to click on specific information, instead of outlining it all in one.[218]

C. Smart Text

Smart Text is a HIPAA-compliant text messaging system designed to help healthcare providers coordinate patient care and delivery.[219] By providing clients with the option to receive SMS text messages regarding medical issues, doctors can send PHI in a faster manner, thereby improving healthcare delivery.[220] As the number of applications increases, there is a mounting need for uniformity of the level of privacy and types of privacy agreements used by app developers. Despite the presence of a privacy policy, the typical consumer doesn't usually read it. Therefore, all applications should be required to have a privacy policy that a consumer is able to understand.[221]

If consumers can understand the policy, then they might read it. Furthermore, a general level of transparency needs to be initiated so when consumers click "agree" they know where their data is going and who is collecting it. In addition, they will know if they are agreeing to allow manufacturers to send their information to third party consumers or advertisers. Therefore, unless consumers are involved in the health industry they do not usually understand or know about HIPAA regulations. Simplification could improve "the efficiency and effectiveness of the health care system."[222]

While the apps mentioned above are HIPAA-compliant,[223] a consumer who downloads an app and inputs his or her own information, or downloads their electronic health records through a patient portal or app recommendation through a provider, is not protected by HIPAA regulations.[224] In such scenarios, the developer of the app is not considered a covered entity or business associate.[225] The developer is not "creating, receiving, maintaining or transmitting

---

216 Flaherty, *supra* note 47, at 433.

217 *Welcome to the Google Privacy Policy*, *supra* note 214.

218 *Id.*

219 *HIPAA Compliant Secure Text Messaging*, TELMEDIQ, https://www.telmediq.com/smarttext/ (last visited Feb. 18, 2017).

220 *Id.*

221 McKinnon, *supra* note 161, at 510.

222 STEPHEN S. SU, A GUIDE TO HIPAA SECURITY AND THE LAW 5 (2007).

223 *Health App Use Scenarios & HIPAA*, BNA, http://src.bna.com/djt (last visited Feb. 18, 2017).

224 *Id.*

225 *Id.*

protected health information on behalf of a covered entity or another business associate."[226] Instead, the consumer obtains health information from her provider, combines it with health information she inputs, and uses the app to organize and manage that information for her own purposes.[227] There is no indication the provider or business associate of the provider hired the app developer to provide or facilitate this service."[228] Although there are apps out there that respect the privacy of consumers, there are other apps or manufacturers that gain to profit off the sales of consumer data.[229]

CONCLUSION

The increase in consumer health apps is fueling the need for Congress to update HIPAA regulations. The fact that consumers are not aware of the amount of data sharing that goes on behind the scenes is a problem. Since HIPAA, FDA, and FTC regulations are not consistent, the government needs to step in and adopt consistent consumer regulations and policies.[230] Although there are benefits to mobile medical devices, the issue with privacy and security can potentially outweigh these benefits. Therefore, the HIPAA regulations, FTC Act, and FDA regulations which are limited need to address the gaps within these regulations to keep medical data private.

Regardless of the benefits, users should be cautious when sharing data with their medical information. In a world where there are more than 2.2 million apps available for download, Congress needs to address these numbers.[231] When law and technology conflict, the law will not win and needs to be updated to keep up with changing times. This will strike a balance between consumer privacy and health apps. Finally**,** technologists and policy makers need to come to an understanding before this miscommunication creates a larger problem.[232]

The lack of security within health apps, paired with consumers' general lack

---

226 *Id.*

227 *Id.*

228 *Id.*

229 Flaherty, *supra* note 47, at 433; *see also* Noreena Hertz et al., *Should Companies Profit by Selling Customers' Data?*, WALL ST. J. (Oct. 24, 2013), http://www.wsj.com/articles/SB10001424052702304410204579143981978505724 (explaining how data is collected by companies for use to profit).

230 Flaherty, *supra* note 47, at 438.

231 *Number of apps available in leading app stores as of June 2016*, THE STATISTICS PORTAL, https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (last visited Feb. 17, 2017).

232 Bruce Schneier, *Can Laws Keep Up with Tech World?*, CNN (Dec. 21, 2015), http://www.cnn.com/2015/12/21/opinions/schneier-whatsapp-blocked-brazil/.

of knowledge regarding the security of their information, needs to be challenged. The Department of Health and Human Services has the authority to change these regulations especially since the intrusion of privacy must be purposeful.[233] It can be assumed that as businesses continue to collect information the dissemination and collection of this data is done purposefully. Consumers are at the center of their own care and the government needs to recognize this. The FTC, FDA, and HHS all have the ability to regulate privacy issues relating to mobile health apps yet continue to make unfulfilled promises. A widely adopted standard needs to be applied that will allow consumers to understand the privacy policies they are reading and provide them with the option to either opt in or opt out of data sharing. The gaps within policy involving privacy will continue to persist if not addressed, especially as innovators continue to find the newest measure of mobile health apps.[234] Non-covered entities should be required to inform consumers when policy updates or changes have been made and allow consumers to consent to continued usage of the application.[235] For true effectiveness, the FTC must enforce these privacy regulations.[236] In addition, one way that non-HIPAA-compliant applications can conform and protect consumer data is by providing a detailed list of where the data goes and the use of the data.

As stated, the gaps within HIPAA need to be adjusted to incorporate non-covered entities ensuring the health data information of consumers is kept private. If these gaps are not filled there will be continued confusion not just with consumers, but businesses and manufacturers.[237] Furthermore, companies should maintain a security tracking program that protects confidential information against breach from internal and external factors.[238] This will ensure that companies like Yahoo are held accountable for personal identifiable information being hacked or leaked.

---

233 *Health App Use Scenarios & HIPAA, supra* note 224.

234 *Supra* note 67, at 28.

235 *Id.*

236 *Id.*

237 *Id.*

238 *Best Practices for Consumer Wearables & Wellness Apps & Devices*, FUTURE OF PRIVACY FORUM 9 (Aug. 17, 2016) https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf.