COMMENT

MIND THE GAP: ADDRESSING GAPS IN HIPAA COVERAGE IN THE MOBILE HEALTH APPS INDUSTRY*

ABSTRACT

Current smartphone platforms are offering a growing number of mobile health apps to meet health and wellness needs and even address the continuing shortage of primary care physicians. The increasing sophistication in smartphones can transform a phone into a sensitive device capable of capturing a variety of medical information. Newer iterations of smartphones have integrated abilities to track our health information and can be paired with wearable health technology, such as the Fitbit, to constantly monitor an individual's activity rates and vitals.

This new wave of mobile health technology is not, however, an unmitigated blessing. Mobile health apps can collect, aggregate, and sell patient health data to third parties. The Health Insurance Portability and Accountability Act ("HIPAA") affords certain robust protections to mobile health apps tied to "covered entities" as defined by statute. Mobile health apps that are not tied to "covered entities" are part of the mobile health apps industry that is essentially unregulated. Simply put, the amount of protection health data receives depends on who holds the data, not the type of information being held.

This article addresses the gap in HIPAA coverage in mobile health apps between "covered" and "non-covered" entities and proposes that HIPAA coverage should be expanded to cover private health care information regardless of who holds it. In lieu of HIPAA expansion, agencies and the industry should itself step up to close gaps in HIPAA coverage however they can. Doing so will not only

* J.D. Candidate, University of Houston Law Center, 2018.

protect sensitive health data, it will also provide a predictable business environment for companies and entrepreneurs to innovate and improve health care quality, participation, and accessibility.

TABLE OF CONTENTS

I. INTRODUCTION

In Robin Cook's medical thriller, *Cell*, he describes the fictional iDoc as "a smartphone functioning as a twenty-first-century primary-care physician" backed up by a remote team of doctors and supercomputers.[1] The smartphone constantly monitors data on all iDoc users, and bases its real-time titration on algorithms that continuously learn and upgrade.[2] While the idea of creating a fully functional iDoc may seem far from realization, the mobile health industry marches toward an iDoc-like device. In 2012, for example, Qualcomm and the X Prize Foundation partnered to host a four-year, $10 million competition (The Qualcomm Tricorder XPRIZE) to build a "handheld, mobile device able to quickly diagnose a range of health problems and measure real-time information such as respiratory rate and blood pressure."[3] The competition drew inspiration from Star Trek's fictional medical "Tricorder" device, a handheld device that was able to quickly gather vital medical information regarding a patient's physical condition.[4] While the competition's winning devices[5]—though impressive by today's standards—are a far cry from the miracle machines of science fiction, they certainly promise to "stimulate innovation and integration of precision diagnostic technologies."[6]

---

1. ROBIN COOK, CELL 30, 37–38, 41 (2014) (explaining that iDoc is supported by a super computer that continuously monitors real time health data and updates the iDoc's knowledge basis, and a group of doctors who provide input when a problem arises with iDoc's automated decision-making process).

2. *See id.* at 216–17 ("iDoc is able to titrate lifesaving medication according to real-time physiological value rather than trying to treat symptoms, which is the old 'sick' care medical paradigm. iDoc is the perfect primary-care doctor since it is based on an algorithm that is capable of learning and will be continually upgraded as new medical information is incorporated.").

3. Douglas Main, *The Race to Build a Real Star Trek Tricorder*, POPULAR MECHANICS (Feb. 1, 2012), http://www.popularmechanics.com/science/health/a7472/the-race-to-build-a-real-star-trek-tricorder-6649721/?click=pm_latest [https://perma.cc/8VKY-U83X].

4. *See id.*

5. *See* XPrize Foundation, *Congratulations to Our Winners!*, QUALCOMM TRICORDER XPRIZE, https://tricorder.xprize.org/teams [https://perma.cc/P9N5-YDZK] (last visited Nov. 3, 2017) (naming the dxtER by Final Frontier Medical Devices and the DeepQ Kit by the Dynamical Biomarkers Group as winners of the Qualcomm Tricorder XPRIZE and discussing the features of each device).

6. XPrize Foundation, *Overview*, QUALCOMM TRICORDER XPRIZE, http://tricorder.xprize.org/about/overview [https://perma.cc/9K28-8Z79] (last visited Jan. 9, 2017). Unlike the omniscient iDoc or Tricorder, the winning device is "expected to accurately diagnose 13 health conditions (12 diseases and the absence of conditions)—10 required core conditions and a choice of three elective conditions—in addition to capturing five real-time health vital signs, independent of a health care worker or facility, and in a way that provides a compelling consumer experience." *Id.*

Although we may not have an iDoc or Tricorder in our pockets just yet, current smartphone platforms are offering a growing number of mobile health apps that are "consumer-directed software application[s] that can be installed on mobile devices using the iOS or Android operating systems,"[7] to meet health and wellness needs.[8] The increasing sophistication in smartphones can transform a phone into a sensitive device capable of capturing a variety of medical information.[9] Newer iterations of smartphones have integrated abilities to track our health information and can be paired with wearable health technology, such as the Fitbit, to constantly monitor an individual's activity rates and vitals.[10]

With the continuing shortage of primary care physicians and the aging of the baby boomer population, the growth of mobile health is not likely to slow.[11] Tech companies are taking notice. Apple, for example, has made moves to become a bigger player in mobile health by acquiring companies in the health care industry[12] and releasing developer tools specifically for health

7. Health Discovery Corp., 159 F.T.C. 1187, 1188 (2015).

8. *See* Fed. Trade Comm'n, FTC Releases New Guidance for Developers of Mobile Health Apps: Tool Created in Conjunction with HHS and FDA Will Help Businesses Determine Applicable Laws and Regulations (Apr. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps. (noting the increase in use of mobile health products and recognizing the need for increased regulatory clarity so that consumers may be provided with effective tools to make proper health care decisions) [https://perma.cc/J7HR-9PKY].

9. *See* Fazal Khan, *The "Uberization" of Healthcare: The Forthcoming Legal Storm Over Mobile Health Technology's Impact on the Medical Profession*, 26 HEALTH MATRIX 123, 138 (describing how mobile health applications can "transform smartphones or tablets into microscopes, stethoscopes, EKGs, dermatoscopes, and even mini-laboratories that can test bodily fluids").

10. *See* Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y L. & ETHICS 1, 7–8 ("Fitbit makes several versions of a wearable device that 'tracks every part of your day—including activity, exercise, food, weight and sleep,' according to its website."). The article addresses the lack of protection employees face from potential employer abuse of employee's health and fitness data. *Id.* at 21 ("While several federal laws appear to prohibit employers' potential misuse of health and fitness data, significant gaps remain in the federal protection of these data.").

11. *See* Khan, *supra* note 9, at 130–31 (focusing on both the aging baby boomer population coupled with the retiring baby boomer doctor population contributing to a projected shortage of 90,000 primary care physicians within the next five years).

12. *See* Christina Farr & Mark Sullivan, *Apple Acquires Personal Health Data Startup Gliimpse*, FAST CO. (Aug. 22, 2016), https://www.fastcompany.com/3062865/tim-cooks-apple/apple-acquires-personal-health-data-startup-gliimpse [https://perma.cc/6SQ5-N79G] (discussing Apple's 2016 acquisition of Gliimpse as a "major business opportunity for the company in the non-regulated side of health care"). Gliimpse is a platform that "enables any American to collect, personalize, and share a picture of their health data." *Id.*

apps and health research.[13] Mobile health and mobile health applications are seen as a way to bridge the gap in this continuing physician shortage. Some see it as a gateway to "providerless medicine,"[14] while others may see it as a tool for patients to make more informed decisions and keep them and their providers connected through the regular exchange of data.[15]

The promising wave of mobile health technology, however, is not without concern. Mobile health applications collect patient health data, some of it seemingly mundane but some of it also very sensitive.[16] Moreover, mobile health application companies can sell the aggregated data they collect on consumers to third parties.[17] The health data that mobile health application companies collect may also be improperly stored or transported, making it susceptible to security breaches.[18] Health Insurance Portability and Accountability Act ("HIPAA") and certain consumer protection agencies afford mobile health applications,

---

13. *See HealthKit*, APPLE DEVELOPER, https://developer.apple.com/healthkit/ [https://perma.cc/3826-WS4W] (last visited Nov. 3, 2017) (discussing how health care app developers can integrate their apps with Apple software to allow Apple to access health information for use in its "Health" app and to allow researchers to access the same information). Apple and HealthKit are discussed in greater depth below. *See infra* Part V.C.1 (discussing proposed solutions to the gap in HIPAA coverage for mobile health applications, including adoption of stricter app development guidelines by Apple, which currently prohibits the use of health data for reasons other than improving health).

14. *See* Khan, *supra* note 9, at 129–30 (discussing the providerless option but instead proposing "doctors and physician extenders should reach a 'grand bargain' to reform restrictive scope of practice reforms on a nationwide basis and stand as a united front to extract concessions from the federal government to protect against mobile health corporations and related financial interests from altering the regulatory landscape to bring about the 'Uberization' of healthcare—that is, providerless medicine").

15. Anna Marie Helm & Daniel Georgatos, *Privacy and mHealth: How Mobile Health "Apps" Fit into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131, 137 ("Indeed, mHealth has the potential to lead to more informed healthcare decisions by delivering valuable, current, and actionable information to doctors, patients, and researchers—wherever they are.").

16. *See* Sarah R. Blenner et al., *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*, 315 JAMA 1051, 1051–52 (finding that the mobile health applications shared consumers' insulin and blood glucose levels with third parties). A quick overview of popular medical applications on the Apple App Store shows apps that track ovulation and fertility, screen for depression, and offer support for pornography and sex addiction. *See* Apple Inc., *Medical*, ITUNES, https://itunes.apple.com/us/genre/ios-medical/id6020?mt=8 [https://perma.cc/AB2A-5F33] (last visited Nov. 3, 2017).

17. *See* FED. TRADE COMM'N, SPRING PRIVACY SERIES: CONSUMER GENERATED AND CONTROLLED HEALTH DATA (2014) [hereinafter SPRING PRIVACY SERIES], https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf [https://perma.cc/R7UL-Q9XZ] (finding third parties were able to purchase "[c]onsumer information such as exercise routine, dietary information, and symptom searches" from health and fitness apps).

18. *See infra* Part IV.B n.117 and accompanying text (discussing *GMR Transcription Servs.*, a case in which improperly secured, sensitive health data was uploaded online, allowing users to find that data using a simple search engine search).

and the data they collect, certain protections.[19] The more robust HIPAA protections, however, only extend to mobile health apps tied to "covered entities" as defined under the statute.[20] Entities not covered by HIPAA are not obligated to comply with HIPAA regulations. In sum, the amount of protection health data receives depends on who holds the data, not the type of information being held.[21] This gap in regulation leaves a large part of the mobile health apps industry essentially unregulated and many health application consumers mistakenly thinking that the information they share is afforded more protection than it really is.[22]

This Article addresses the gap in HIPAA coverage in mobile health applications between "covered" and "non-covered" entities and proposes that HIPAA coverage should be expanded to cover private health care information regardless of who holds it. Doing so would not only protect consumers and patients, but also would serve as a boon to companies and entrepreneurs by providing a predictable business environment in which to develop mobile health care technology.[23] In the absence of reform at the federal level, stopgap measures can help close the gap some but not all the way.[24]

Part II will cover the regulatory framework that governs mobile health applications and the agencies that are involved in this industry.[25] Part III discusses agency involvement regarding HIPAA and its enforcement.[26] Part IV discusses why consumers should be concerned about this gap in coverage and why the health app industry should care as well.[27] The final section,

19. *See infra* Part II (examining the protections afforded to health data under HIPAA).

20. *See generally* Part II (noting covered entities are subject to HIPAA and HHS's corresponding HIPAA rulemakings, while non-covered entities are not, but may be regulated by other agencies sharing concurrent jurisdiction with HHS).

21. *See infra* Part II.A (discussing application of HIPAA to covered entities and the difference between covered entities and non-covered entities).

22. *See infra* Part IV.C (discussing privacy policies in mobile health applications and how their existence can make consumers think their data is automatically afforded rights and protections).

23. *See infra* Part IV.D (discussing the mobile health applications industry's awareness of gaps in HIPAA coverage and their desire for clarification).

24. *See infra* Part V (noting enforcement problems with alternative proposed solutions such as agency intervention, stricter development guidelines for health apps, and self-enforcement by the health app industry).

25. *See infra* Part II (discussing application of HIPAA to health data recorded by mobile health applications).

26. *See infra* Part III (discussing the role that various agencies such as the FTC and HHS play in enforcing HIPAA).

27. *See infra* Part IV (suggesting consumers should be concerned about HIPAA coverage gaps due to possibility of sale and use of health data by insurance companies and

Section V, proses several changes that can help close the HIPAA coverage gap.[28] The scope of this Comment will only address mobile health apps, although the analysis may be applied to other parts of the digital health industry, such as websites.[29] Unless otherwise stated, mention of mobile health applications will pertain only to those entities not covered by HIPAA.

II. THE REGULATORY SCHEME FOR HEALTH APPLICATIONS

A. Health Insurance Portability and Accountability Act

Congress passed the Health Insurance Portability and Accountability Act ("HIPAA") in 1996 to improve the applicability of health insurance coverage and to protect against abuse in health care delivery.[30] HIPAA provides federal statutory protections for health information.[31] It provides federal security and privacy protections for individually identifiable health information and gives patients specific rights with respect to that information.[32] Privacy laws regarding mobile health applications largely depend on whether HIPAA applies to the specific application.[33]

HIPAA, however, does not apply to health care applications in all situations.[34] HIPAA only applies to organizations that are considered to be "covered entities."[35] In other words, mobile health applications "used by individuals to manage their own health, but not offered or provided to the individual by a covered entity or a business associate, are outside of HIPAA's scope."[36]

---

possibility of data breaches; and suggesting the app industry should be concerned because of potential confusion whether apps are covered entities).

28. *See infra* Part V (discussing proposed solutions to HIPAA coverage gaps, including legislative expansion of HIPAA, agency intervention, stricter development guidelines for health apps, and self-enforcement by the health app industry).

29. *See infra* Part II (discussing HIPAA and its applications concerning health data).

30. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 ("To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery . . . .").

31. Helm & Georgatos, *supra* note 15, at 147.

32. *See infra* Part II.A.1–3 (discussing the HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Breach Notification Rule).

33. Helm & Georgatos, *supra* note 15, at 133, 156. (stating that application of HIPAA privacy protections to an app depends on whether the app meets certain criteria, such as the involvement of a "covered entity").

34. *See infra* Part II.A (discussing when HIPAA applies).

35. 45 C.F.R. § 164.500(a) (2016) ("Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to *covered entities* with respect to protected health information." [emphasis added]).

36. U.S. DEP'T OF HEALTH AND HUM. SERVS., EXAMINING OVERSIGHT OF THE

Under HIPAA, covered entities include: (1) health plans, (2) health care clearinghouses, and (3) health care providers who transmit health information in electronic form.[37] HIPAA coverage also extends to business associates of covered entities.[38]

Covered entities are subject to the HIPAA rules, which include the HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Breach Notification Rule.[39] The Department of Health and Human Services ("HHS") created these rules to create a standard to protect private health information when it is in the hands of covered entities or being transmitted between covered entities.[40] These covered entities are permitted—sometimes mandated—to disclose a person's personal health information without their authorization.[41]

The following sections provide a more in-depth explanation of the three HIPAA Rules: The Privacy Rule, Security Rule, and Breach Notification Rule.

1. HIPAA Privacy Rule. The HIPAA Privacy Rule (the "Privacy Rule") protects any identifiable health information that is held by a covered entity or their business associates[42] and affords patients certain rights to their protected health information ("PHI") regardless of the media in which the information is stored.[43] PHI is information that can identify a

---

PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 9 (2016), [hereinafter EXAMINING OVERSIGHT] https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/BB6S-NTEB] The report further clarifies that information sent from these non-covered applications would only become subject to HIPAA once they are received by a HIPAA-covered entity. *Id*. at 9 n.40.

37. 45 C.F.R. § 160.102(a) (2016).

38. *Id*. § 160.102(b). HHS provides examples on its websites of some common business associates under HIPAA, including: third-party administrators helping a health plan with claims processing, a consultant who performs utilizations review for a hospital, and an independent medical transcriptionist that provides transcription services to a physician. OFF. FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH AND HUM. SERVS., BUS. ASSOCS. 1–2 (2003), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [https://perma.cc/XPY8-2VCB].

39. *See infra* Part II.A.1–3 (discussing the HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Breach Notification Rule).

40. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. 160–64) ("The purpose of this final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Currently, no standard measures exist in the health care industry that address all aspects of the security of electronic health information while it is being stored or during the exchange of that information between entities.").

41. *See infra* Part II.A.1 (discussing the HIPAA Privacy Rule and its exceptions).

42. EXAMINING OVERSIGHT, *supra* note 36, at 14; *see also* 45 C.F.R. § 160.103 (2016).

43. 45 C.F.R § 160.103 (2016) ("Protected health information means individually

person and is related to their physical and mental health, the provision of health care services to that person, or payment for health care services.[44] Examples of personal identifiers under HIPAA include, among many others: names, medical record numbers, biometric identifiers, and account numbers.[45] Patients have the right to request and inspect a copy of their PHI from the covered entity.[46] Patients can also request to make changes to that information.[47] The patients have the right to know if anyone has received their records and to have their records sent to a designated third party.[48] The Privacy Rule also allows patients to place restrictions on who can see their information.[49] If there is an unauthorized disposition of PHI, the Privacy Rule allows patients to launch complaints with the covered entity itself or with the Office for Civil Rights.[50]

HIPAA has carved out specific exceptions for releasing data, but if a covered entity wishes to use a patient's PHI for a reason that does not qualify as an exemption, the covered entity must get authorization from the patient before it can use his or her data.[51] HIPAA carved out the following exemptions that allow covered entities to release a person's PHI: (1) when mandated by law; (2) for treatment and payment; (3) to family members and friends involved in a patient's health care unless the patient objects; (4) for activities beneficial to public health; and (5) for

---

identifiable health information: . . . (i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium.").

44. *Id.* § 160.103 ("Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to . . . [p]reventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body.").

45. 45 C.F.R. § 164.514 (2016). There are 18 identifiers recognized under HIPAA. Others include geographic subdivisions smaller than a state, social security numbers, and IP addresses. *Id.*

46. *Id.* § 164.524(a) ("[A]n individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set . . . .").

47. *Id.*

48. *Id.* § 164.528.

49. *Id.* § 164.510.

50. *Id.* § 160.306 ("A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary."); *see also How to File a Health Information Privacy or Security Complaint*, U.S. DEPT. OF HEALTH & HUM. SERVS., (last visited Feb. 20, 2018), https://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html [https://perma.cc/676Y-HL5U] (explaining the procedure of filing a complaint with the Office of Civil Rights).

51. *Id.* § 164.508 ("Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section.").

research purposes as long as the data is de-identified.[52] If the PHI is transferred to another covered entity, HIPAA rules still apply to the information regardless of the data type.[53]

While the Privacy Rule protects PHI by attaching rights and obligations to it, the HIPAA Security Rule ("Security Rule") addresses the more practical security measures with respect to safeguarding the data itself.[54] It is important to reiterate that the Privacy Rule does not cover applications if they do not fall into the "covered entity" category, although they may be subject to other consumer law protections.[55]

2. HIPAA Security Rule. Once covered entities or their business associates possess a patient's PHI, HIPAA requires that information be kept safe through its Security Rule.[56] Covered entities must "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits."[57] These covered entities must also protect against "reasonably anticipated" threats or disclosures of information and train their workforce accordingly to safeguard their data.[58] The Security Rule further requires physical safeguards to the data, such as facility access controls and workstation security.[59] The HIPAA Security Rule includes administrative and technical controls, such as risk analysis and audit controls.[60] Importantly, HIPAA provides flexibility in its Security Rule, allowing covered entities to achieve the statutory requirements in any way they see fit; smaller and less complex operations can institute more cost-conscious means to remain lawful under HIPAA and can change with new technologies.[61]

3. HIPAA Breach Notification Rule. In the event that a covered entity suffers a breach in unsecured health information,

---

52. *Id.* § 164.514. De-identification includes removing the identifiers previously discussed in note 45.

53. EXAMINING OVERSIGHT, *supra* note 36, at 15 n.71.

54. *See infra* below Part II.A.2 (discussing the HIPAA Security Rule).

55. *See infra* Part II.C (discussing non-covered entities).

56. *See generally* 45 C.F.R. § 164.306 (Security Standards: General Rules).

57. *Id.* § 164.306(a)(1).

58. *Id.* § 164.306(a) (Covered entities and business associated must "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information.").

59. EXAMINING OVERSIGHT, *supra* note 36, at 16.

60. *Id.* ("Technical safeguards include access controls, audit controls, integrity, person or entity authentication, and transmission security.").

61. 45 C.F.R. § 164.306(b).

HIPAA mandates the covered entity to inform every individual affected or possibly affected by the breach.[62] This requirement is known as the HIPAA Breach Notification Rule and applies uniformly to all patients under HIPAA.[63] Breaches involving 500 or more people in a state or jurisdiction require the covered entity involved to inform both the prominent media outlets in their state or jurisdiction as well as the Secretary of HHS.[64] Business associates of a covered entity that suffer a breach are required to inform the covered entity, who in turn must notify patients of the breach.[65]

The protections afforded to individuals under HIPAA were further buttressed by the Health Information Technology and Economic Clinical Health Act.[66] This Act, discussed in the next section expanded protections in efforts to keep up with emerging technologies.[67]

B. Health Information Technology and Economic Clinical Health Act

The Health Information Technology and Economic Clinical Health Act (the "HITECH Act") was enacted in 2009 as part of the American Recovery and Reinvestment Act, commonly known as the Recovery or Stimulus Act.[68] Congress enacted the HITECH Act to promote meaningful use of health information technology, but concerns regarding electronic health privacy and security led HHS to strengthen HIPAA protections as well.[69] The HITECH Act amended HIPAA by expanding the coverage of the Security Rule.[70] Under the HITECH Act, the Security Rule applies to covered entities and to business associates of the covered entities.[71] The HITECH Act allows patients to have access to their electronic health records and gives HIPAA more

62. *Id.* § 164.404 ("A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.").

63. *Id.*

64. 45 C.F.R. §§ 164.406, 164.408. The statute outlines the manner and timeliness of communication for each type of breach specified.

65. *Id.* § 164.410.

66. Timothy Newman & Jennifer Kreick, *The Impact of HIPAA (and Other Federal Law) on Wearable Technology*, 18 SMU SCI. & TECH. L. REV. 429, 432 (2015).

67. *See infra* Part II.B (discussing the HITECH Act).

68. Newman & Kreick, *supra* note 66, at 432.

69. *Id.*

70. HITECH Act § 13404 codified in 42 U.S.C. § 17934 (2012).

71. EXAMINING OVERSIGHT, *supra* note 36, at 14.

teeth by imposing mandatory penalties for violations.[72] Further, the HITECH Act also requires periodic audits of covered entities to assess their compliance with HIPAA.[73]

C. Non-Covered Entities

Mobile health applications can receive a fair amount of governmental oversight under HIPAA: the data itself may be subject to privacy protections, security protections, and periodic auditing to ensure compliance.[74] All the HIPAA rules and their associated protections, however, only apply to statutorily covered entities.[75] Entities falling outside of these "covered" categories, non-covered entities, are not subject to the rules or penalties of HIPAA and the HITECH Act.[76] Mobile health apps falling outside of the HIPAA rules are largely unregulated,[77] and non-covered entities instead are left under the auspices of agencies that may not necessarily directly regulate electronic health information but may have concurrent jurisdiction with HHS.[78]

III. AGENCY INVOLVEMENT AND ENFORCEMENT

Although only a few agencies are discussed in the section below, over half a dozen agencies touch on HIPAA and HIPAA enforcement in one way or another.[79]

A. Federal Trade Commission Act, the FTC, and Section 5

The Federal Trade Commission ("FTC"), through several rules, enforces requirements on businesses to protect user data

---

72. HITECH Act § 13410(d) codified in 42 U.S.C. § 1320d-5 (2012). Willful neglect violations, for example, carry a $50,000 penalty for each violation. *Id.*

73. OFF. FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUM. SERVS., *HIPAA Privacy, Security, and Breach Notification Audit Program,* HHS.GOV (Dec. 16, 2016), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit [https://perma.cc/G9GQ-NZ24].

74. *See supra* Part II.A.1–3 (discussing the HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Breach Notification Rule).

75. Helm & Georgatos, *supra* note 15, at 153–54. ("For HIPAA's privacy protections to apply to a mobile app, that app must involve a covered entity as well as PHI. Accordingly, the set of apps subject to HIPAA's protections is only a subset of the larger mHealth app population."). These protections extend to the Privacy Rule, Security Rule, and the Breach Notification Rule. *Id.* at 154.

76. *Id.* at 167–68.

77. *Id.*

78. *See infra* Part III (discussing how agencies are involved in the regulation of the mobile health applications industry); *see also* EXAMINING OVERSIGHT, *supra* note 36, at 17 n.80.

79. Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1214 (2014). Some of the other agencies identified include the FCC, FDA, FTC, and HHS. *Id.*

and privacy.[80] The FTC polices unfair or deceptive practices in relation to Section 5 of the Federal Trade Commission Act.[81] The FTC has used Section 5 of the Act against businesses believed to have made false or misleading claims about privacy or security, where such claims were likely to injure consumers.[82] Regarding the mobile health application industry, Section 5 covers HIPAA and non-HIPAA covered entities, which makes the Act the main federal statutory protection for health information not covered under HIPAA.[83] Due to the common interests between the HHS and FTC, the agencies have worked closely in areas of concurrent jurisdiction to enforce health privacy and security.[84]

The FTC applies its own Health Breach Notification Rule for entities that do not fall within HIPAA's Breach Notification Rule.[85] This notification rule, however, only applies to vendors of personal health records and related entities.[86] Still, the FTC's Health Breach Notification Rule imposes similar requirements as the HIPAA Breach Notification Rule, including notifying individuals, related vendors, and the media of a breach under certain circumstances.[87]

B. Department of Health and Human Services Office of Civil Rights

The Office of Civil Rights ("OCR") enforces the HIPAA Rules under HIPAA and the HITECH Act.[88] Results from OCR enforcement of the HIPAA Rules have been mixed, with the Privacy Rule receiving a high volume of resolved cases since the OCR began enforcing the HIPAA rules in 2003.[89] OCR

80. EXAMINING OVERSIGHT, *supra* note 36, at 17.

81. 15 U.S.C. § 45(a) (2012).

82. *See* PaymentsMD, LLC, No. C-4505 (F.T.C. Jan. 27, 2015), https://www.ftc.gov/system/files/documents/cases/150206paymentsmddo.pdf [https://perma.cc/AZE4-7SCB]; GMR Transcription Serv. No. 122-3095, 2014 WL 492352, at *4 (F.T.C. Aug. 14, 2014).

83. EXAMINING OVERSIGHT, *supra* note 36, at 17.

84. *Id.* at n.80 ("For example, FTC staff collaborated with OCR to bring a set of cases involving faulty data security practices that implicated both HIPAA and the FTC Act.").

85. *See* HITECH Act § 17937 (2012).

86. 16 C.F.R. § 318.1 (2017).

87. 16 C.F.R. §§ 318.3(b), 318.5(a)(2)(ii) (2017).

88. Office for Civil Rights; Delegation of Authority, 74 Fed. Reg. 38,630 (Aug. 4, 2009) (to be codified at 45 C.F.R. 160, 164). The OCR coordinates with the Department of Justice for matters involving criminal violations. OFF. FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUM. SERVS., *Health Information Privacy: Enforcement Highlights*, HHS.GOV (Oct. 31, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html [https://perma.cc/7J6P-YQ3N].

89. *Id.*

enforcement of the HIPAA Security Rule has fallen behind, which even resulted in the HHS publishing the 2013 report, "The Office for Civil Rights Did Not Meet All Federal Requirements in its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule."[90]

1. Food and Drug Administration ("FDA"). FDA oversight into the mobile health apps industry applies only to the subset of apps subject to FDA medical device regulations.[91] The FDA makes it clear that it regulates software, not hardware, so it cannot regulate the sale of smartphones; rather, it can regulate mobile apps on smartphones that might analyze and interpret medical information in the same way a desktop might, for example, interpret EKG waveforms.[92] The majority of mobile health apps, however, fall outside of the FDA's purview because they do not qualify as medical devices.[93]

IV. WHY CONSUMERS SHOULD BE CONCERNED ABOUT GAPS IN HIPAA COVERAGE

There are currently over 250,000 mobile health applications in the market, with nearly 100,000 of those applications appearing within the last year.[94] As explained in Part II, HIPAA protections do not cover many of these applications.[95] The following section explains the risks engendered by the lack of HIPAA coverage.[96]

---

90. U.S. DEP'T OF HEALTH & HUM. SERVS., OFFICE OF INSPECTOR GEN., THE OFFICE FOR CIVIL RIGHTS DID NOT MEET ALL FEDERAL REQUIREMENTS IN ITS OVERSIGHT AND ENFORCEMENT OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT SECURITY RULE (Nov. 2013), *available at* https://oig.hhs.gov/oas/reports/region4/41105025.pdf [https://perma.cc/7EUW-9N37]. The findings include that "OCR had limited assurance that covered entities complied with the Security Rule and missed opportunities to encourage those entities to strengthen their security over ePHI." *Id* at ii.

91. FOOD & DRUG ADMIN., U.S. DEP'T OF HEALTH & HUM. SERVS., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUS. AND FOOD AND DRUG ADMIN. STAFF 7 (2015), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf [https://perma.cc/J3J9-9FH5].

92. *Id.* at 8 (noting that EKG regulation is under 21 C.F.R. § 870.2340 ("Electrocardiograph")).

93. *See id.* (explaining the FDA's intent "to apply this oversight authority only to those mobile apps whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended.").

94. *mHealth App Market 2016: Top 10 Changes and Reasons to Be Optimistic for the Years to Come*, RESEARCH2GUIDANCE, https://research2guidance.com/mhealth-app-market-2016-top-10-changes-and-reasons-to-be-optimistic-for-the-years-to-come/ [https://perma.cc/EXC8-KLPN] (last visited Feb. 8, 2018).

95. *See generally supra* Part II (discussing HIPAA protections for covered entities and concluding that those protections do not extend to non-covered entities).

96. *See infra* Part IV A–E.

A. Mobile Health Apps Collect and Sell Health Data

In 2014, the FTC conducted tests on twelve free mobile health applications and found that they collectively sent information to 76 different third parties.[97] The data included unique and consumer-specific information on: "[d]evice [i]nformation; [c]onsumer-specific identifiers; [u]nique device IDs capable of allowing third parties to track users' devices across apps; [u]nique third party IDs capable of allowing third parties to track users' devices across apps; and [c]onsumer information such as exercise routine, dietary habits, and symptom searches."[98] When all this data is aggregated by third parties and paired with unique consumer identifiers, this can essentially strip consumers of anonymity and allow them to be individually tracked.[99]

Although the FTC's study involved fitness applications, the same privacy concerns extend to applications that collect more sensitive medical data, such as medication compliance and disease status.[100] A 2016 study of diabetes applications, for example, found that 56 of 65 applications placed tracking cookies and shared information with third parties.[101] In these applications, insulin and blood glucose levels were regularly collected and shared.[102]

To what third parties are mobile health applications sending information? Typically, it will be "advertising and analytics companies, who attempt to better match advertisements to users who will buy; and who work to help app developers increase functionality and usability, respectively."[103] This aggregated data is valuable to these third party companies, who can then use it to guide future investments in pharmaceutical companies, for example, or to better target advertising campaigns.[104] Although

97. SPRING PRIVACY SERIES, *supra* note 17.

98. *Id.*

99. *See id.* ("There are significant privacy implications where health routines, dietary habits, and symptom searches are capable of being aggregated using identifiers unique to that consumer."). Target uses a Guest ID system to track consumers and form profiles on them based on their purchases and other information they acquire. Using this system, Target can even reliably predict when a female customer is pregnant and send them pregnancy-related ads and coupons. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

100. Blenner, *supra* note 16, at 1051.

101. *Id.*

102. *Id.*

103. SPRING PRIVACY SERIES, *supra* note 17.

104. Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, SCI. AM. (Feb. 1, 2016), https://www.scientificamerican.com/article/how-data-brokers-make-

this data is considered de-identified by law, these companies can attach unique identifiers to individual data they receive to match different pieces of information to the same nameless person.[105] While collected data may be used for advertising and marketing purposes, some fear that insurance companies may one day purchase aggregated data from mobile health apps and utilize it to set policy premiums.[106]

Because many of these mobile health applications are not covered by HIPAA protections, application developers and third parties do not have to fulfill certain requests. Examples of requests mobile health application companies do not have to honor include: giving consumers the data they have on them, restricting how the data is shared, or requesting permission when using the data for non-HIPAA-approved purposes.[107]

B. Improperly Stored Information May Be Stolen

Covered entities under HIPAA are required to ensure that PHI is "protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure."[108] For mobile health applications, protecting data normally involves encrypting data while stored and during any transfer process.[109] However, Privacy Rights Clearinghouse, a nonprofit consumer education and advocacy organization, found that only thirteen percent of free mobile health applications always used encrypted connections.[110] Because unencrypted

money-off-your-medical-records/ [https://perma.cc/M469-3XN7].

105. *Id.* (Tanner goes on to describe how this anonymous data can be re-identified. Harvard Professor Latanya Sweeny was able to use publicly-available, anonymous data sets to identify Massachusetts governor William Weld and find his recent hospital visit, diagnosis, and prescription.).

106. Emily Steel & April Dembosky, *Health Apps Run into Privacy Snags*, FIN. TIMES (Sept. 1, 2013), https://www.ft.com/content/b709cf4a-12dd-11e3-a05e-00144feabdc0. While the Genetic Information Nondiscrimination Act (GINA) does not allow for the use of genetic information (collected by apps, for example) to set insurance premiums for primary care insurance, GINA does not apply to life, disability, or long-term care insurance. Kira Peikoff, *Fearing Punishment for Bad Genes*, N.Y. TIMES (Apr. 7, 2014), https://nyti.ms/1mVTzYS.

107. *See generally supra* Part II (discussing HIPAA protections for covered entities and concluding that those protections do not extend to non-covered entities).

108. *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*, OFF. NAT'L COORDINATOR FOR HEALTH INFO. TECH, U.S. DEP'T HEALTH AND HUM. SERVS. 9 (Dec. 15, 2008), https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf [https://perma.cc/28XF-ZZDJ].

109. An example of this is found in *In re GMR Transcription Services, Inc.* discussed in greater depth *infra* notes 112–114.

110. Linda Ackerman, *Mobile Health and Fitness Applications and Information*

connections can expose a person's sensitive information to everyone on a network, this thirteen percent figure is a cause for concern.[111]

Not having adequate security measures, such as encryption, when transferring and storing sensitive health information can have predictably dire consequences for patients and consumers. In 2014, the FTC issued a final order against GMR Transcription Services, Inc., after discovering that GMR had exposed thousands of consumers' information, including medical histories and examination notes.[112] GMR would send patient files to typists in India, who would then transcribe the files and upload them for customer retrieval.[113] The information transcribed included: "names, dates of birth, addresses, e-mail addresses, telephone numbers, Social Security numbers, driver's license numbers, tax information, medical histories, health care providers' examination notes, medications, and psychiatric notes."[114] However, because the information was not encrypted and only stored in clear, readable text format, a major search engine was able to index thousands of medical transcripts belonging to GMR customers.[115] This meant anyone could find this sensitive information using a simple online search.[116] An entity covered by HIPAA would have required that the business holding the PHI implement reasonable protections of that information from the start.[117]

Aside from data encryption, non-covered entities do not have to meet any federal minimum standard when it comes to identity authentication.[118] Identity in applications is commonly verified through username and password combinations, which may have to meet complexity requirements and perhaps additional

---

Privacy: Report to California Consumer Protection Foundation, PRIVACY RTS. CLEARINGHOUSE 5 (Jul. 15, 2013), https://www.privacyrights.org/sites/default/files/mobile-medical-apps-privacy-consumer-report.pdf [https://perma.cc/DPL6-9BTR].

111. *See id.* at 22.

112. Press Release, Fed. Trade Comm'n, FTC Approves Final Order in Case Against GMR Transcription Servs. (Aug. 21, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-final-order-case-against-gmr-transcription-services [https://perma.cc/73T8-2SDA].

113. *In re* GMR Transcription Servs., No. 122-3095, 2014 WL 492352, at *1–2 (F.T.C. Aug. 14, 2014).

114. *Id.* at *2.

115 *Id.* at *3.

116. *Id.*

117. In its final ruling, the FTC required that GMR "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." *Id.* at *6.

118. EXAMINING OVERSIGHT, *supra* note 36, at 23–24.

measures to prevent unauthorized access to a patient's PHI.[119] Whatever identity verification measures mobile health applications use may not be the reasonable data security safeguards put in place by HIPAA and Section 5.[120]

C. Privacy Policies Do Not Necessarily Provide Notice or Protection

Non-covered entities are not required to inform users of the potential impacts a mobile health application may have on the security of their PHI.[121] A recent study determined that of the 600 most-used mobile health applications, only about thirty percent had privacy policies.[122] Of those applications with privacy policies, most were written with a high level of complexity and did not specifically address the application itself.[123] Other privacy policies may be difficult to find because they are hidden behind a web of links, fragmented, or simply hard to read on a small smartphone screen.[124] Few of the privacy policies that exist stipulate that they would ask users for permission before sharing their data.[125]

Due to this lack of clarity and consistency in privacy policies, consumers run the likely risk of being left without the adequate tools to make an informed decision. Some consumers rely on privacy policies, thinking that their existence protects their PHI and allows them to sue if their data is not protected,[126] yet these consumers fail to realize that the policies merely outline the medical application's practices, allowing the consumer only to read and agree to those practices.[127] On top of this misconstruction of policies and a general lack of transparency is the fact that privacy policies may change without notice, perhaps changing with it the user's legal rights.[128]

---

119. *Id.*

120. *Id.* at 24.

121. *Id.* at 25. ("However, for non-covered entities, there are no federal requirements for policies, or related notices, to inform individuals about practices that may impact the privacy and security of their health information.").

122. Ali Sunyaev et al., *Availability and Quality of Mobile Health App Privacy Policies*, J. OF AM. INFORMATICS ASSN. e30 (Aug 21, 2014), https://academic.oup.com/jamia/article/22/e1/e28/700676 [https://perma.cc/7P78-4QVX].

123. *See id.*

124. EXAMINING OVERSIGHT, *supra* note 36, at 26.

125. Blenner, *supra* note 16, at 1052.

126. *See* Chris Hoofnagle et al., *How Different Are Young Adults from Older Adults when It Comes to Information Privacy Attitudes & Policies?*, 17–18, 20 (Apr. 14, 2010), http://ssrn.com/abstract=1589864.

127. *See* Blenner, *supra* note 16, at 1051–52.

128. EXAMINING OVERSIGHT, *supra* note 36, at 28.

D. More Guidance for Innovators and Entrepreneurs

Inconsistent HIPAA coverage between covered entities and non-covered entities does not only affect consumers but entrepreneurs and innovators as well. Having separate rules for covered and non-covered entities causes confusion among entrepreneurs, particularly those who are new to the mobile health industry.[129] This confusion can lead to investor hesitation, which can then stifle economic growth and new technological innovations in mobile health.[130]

Mobile health technology companies recognize the benefits of having clearer, more uniform HIPAA rules in place and have even reached out to federal agencies for further guidance.[131] In 2016, the U.S. House of Representatives' Subcommittee on Commerce, Manufacturing, and Trade held a hearing specifically addressing health care applications.[132] Regulators, legislators, and stakeholders from health technology and medicine came forward to provide testimony on the potential for mobile health applications along with current deficiencies with the regulation.[133] Law professor Nicolas Terry pointed out that a

---

129. *See id.* at 5. (discussing that those in the industry will know where HIPAA begins and ends, but an entrepreneur may not have a good grasp on HIPAA oversight).

130. *Id.* at 5–6. ("This lack of clarity may impede innovation that could improve health or otherwise benefit individuals or the nation. For example, for HIPAA covered entities, it is often unclear to developers which information is considered to be or defined as 'individually identifiable health information' that is subject to protection by the HIPAA Rules, and which is not.").

131. *See The Disruptor Series: Health Care Apps: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 2–3 (2016) (statement of Diane Johnson, Senior Director, North American Regulatory Affairs Policy and Intelligence, Johnson & Johnson), http://docs.house.gov/meetings/IF/IF17/20160713/105197/HHRG-114-IF17-Wstate-JohnsonD-20160713.pdf [https://perma.cc/6S4P-JENQ]; *The Disruptor Series: Health Care Apps: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. (2016) (statement of Nicolas P. Terry, Hall Render Professor of Law & Executive Director, Hall Center for Law and Health, Indiana University Robert H. McKinney School of Law), http://docs.house.gov/meetings/IF/IF17/20160713/105197/HHRG-114-IF17-Wstate-TerryN-20160713.pdf [https://perma.cc/LN7F-TGVZ].

132. *See* The Disruptor Series: Health Care Apps: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce, 114th Cong. 1, 7 (2016), http://docs.house.gov/meetings/IF/IF17/20160713/105197/HHRG-114-IF17-20160713-SD002.pdf [https://perma.cc/CFL2-LTRH].

133. *See The Disruptor Series: Health Care Apps: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. (2016) (statement of Matthew Patterson, M.D., President, Airstrip), http://docs.house.gov/meetings/IF/IF17/20160713/105197/HHRG-114-IF17-Wstate-PattersonM-20160713.pdf [https://perma.cc/QY6V-Q9CY] ("[M]obile health technologies like those that Airstrip create incredible benefits to the American healthcare system, but their full potential can not [sic] be met without a careful and coordinated effort between Congress, federal agencies, and the industry as a whole.").

large portion of this industry is under-regulated, leading to most consumer applications working in what he calls a "HIPAA-free zone."[134]

While agencies have paired together in attempts to provide more guidance to the mobile health industry, the Congressional hearings make clear a need for further regulation or guidance, at least in certain areas.[135]

E. Interoperability

On a practical level, it is important for collected health data to not only be secure but usable as well. "Interoperability," or how health data is transferred from a mobile health platform to an electronic health record platform, would allow data to be readable by a doctor and allow her to add the data to a patient's file.[136] For this to occur, the data sent needs to be in a standardized format, but there can be a lot of variation in formats across the industry.[137] Lack of interoperability, then, can substantially limit the usefulness of mobile health applications.[138] In a letter to Congress, Fitbit (an NCE) cited their compliance with HIPAA as allowing them to "integrate more effectively with HIPAA-covered entities."[139] Expanding HIPAA coverage to non-covered entities, such as Fitbit, would not only help mitigate the data security risks seen previously

134. Statement of Nicolas P. Terry, *supra* note 131. ("The regulatory framework for most of these apps is complicated and, in some cases troubling. Here, the oversimplified binary of regulation versus innovation is a poor frame. Rather, we have a current technological space that is subject to both over-regulation and under-regulation.").

135. A great example of agency collaboration on this front is the FTC's Mobile Health Apps Interactive Tool, which was created with cooperation from HHS, ONC, OCR, and FDA. The Interactive Tool asks the user a series of questions and provides some guidance and information regarding which laws apply to the application. *Mobile Health Apps Interactive Tool*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [https://perma.cc/8758-3FP7] (last visited Feb. 21, 2018).

136. Daniel F. Schulke, Note, *The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing*, 93 B.U. L. REV. 1699, 1712 (2013).

137. *Id.*

138. *See id.* at 1713 ("Without standard harmonization, mobile applications will fail to offer the main benefit of having the ability to transfer clinical data almost instantaneously, securely, and frequently.").

139. *The Disruptor Series: Health Care Apps: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. (2016) (statement of Woody Scal, Chief Business Officer, Fitbit, Inc.), http://docs.house.gov/meetings/IF/IF17/20160713/105197/HHRG-114-IF17-20160713-SD010.pdf [https://perma.cc/2KNS-Y7L9] ("Fitbit has also announced compliant capabilities under the Health Insurance Portability and Accountability Act (HIPAA), which will enable Fitbit Group Health to serve a broader market and, in certain cases, integrate more effectively with HIPAA-covered entities, including health plans and self-insured employers.").

with the *GMR* ruling but has the added benefit of allowing integration with covered entities, which can make further use of the data.[140]

V. PROPOSED CHANGES TO COVER HIPAA GAPS

In order to better protect consumers and foster innovation, Congress should expand HIPAA to cover protected health information regardless of the entity that holds it. This section explores options at improving the current HIPAA coverage gap, starting first with federal legislative reform. The rest of the section addresses less robust remedies, such as self-policing from within the industry, that may serve as proxies for closing the gap in HIPAA coverage.

A. Expand HIPAA Coverage Through Congress

HIPAA can be strengthened and expanded through federal legislative action, which would result in the most robust and lasting closure to the HIPAA coverage gap.[141] HIPAA deficiencies with mobile health applications are a known issue to some legislators.[142] As seen in the Disruptor Series Hearing before Congress, legislators know that players in the mobile health applications industry and digital health feel innovations are outpacing regulations and that regulations need to catch up.[143]

Response from legislators to change the law itself, however, is lacking.[144] Regulatory change to HIPAA is possible—the HITECH Act, which modified how HIPAA rules were enforced, is proof of this.[145] As has been discussed throughout this paper, the HIPAA Rules application is based on the "covered" or "non-

140. *See supra* Part IV.B (discussing the GMR ruling).

141. *See supra* Part II.B (discussing how the HITECH Act strengthened the regulations and enforcement of HIPAA).

142. *See supra* Part IV.D (discussing the Congressional hearing recently held regarding health care applications).

143. *See supra* Part IV.D (discussing testimony given in Congressional hearing regarding deficiencies in regulation). *See also* statement of Matthew Patterson, *supra* note 133 (speaking specifically about applications requiring FDA clearance: "Innovation will always outpace classification and regulation. Therefore, real-time dialogue is essential to expedite classification and clearance.").

144. There appears to be more of a push from congressmen and women to have HHS provide further clarification. *See* Letter from Tom Marino, Member of Congress, et al. to the Honorable Sylvia Mathews Burwell, Sec'y of Health & Human Servs., (Mar. 9, 2016), https://healthitsecurity.com/images/site/attachments/Marino-DeFazio-HHS-Letter.pdf [https://perma.cc/P63Q-XNK8] (expressing a lack of urgency from HHS to provide further guidance in the fast-moving mobile health applications industry).

145. *See supra* Part II.B (discussing the HITECH Act and how it strengthened the regulation and enforcement of HIPAA).

covered" status of an entity.[146] In order to better protect consumers and patients, any regulation should opt to replace the "covered" and "non-covered" paradigm with one that targets the type of data being shared regardless of who holds it.[147]

B. Agency Intervention[148]

In lieu of federal legislative reform, agencies may be equipped to close gaps in HIPAA coverage. A group of congressmen and women sent a letter to HHS Secretary Burwell in 2016 expressing worry that her agency had not done enough to address insufficient guidance regarding mobile health applications.[149] The letter, signed by eight congressmen and women, intimates that agency action, for the time being, is the proper avenue for redressing some of the gaps in HIPAA coverage.[150]

1. Tougher Enforcement of Privacy Policies by the FTC. Another way that agencies can look to close the HIPAA gap is to spend more resources policing and enforcing the privacy policies of mobile health applications. As it stands, both the Android and Apple application platforms have guidelines that require mobile health applications to have privacy policies.[151] The FTC has experience in enforcing actions against organizations that engage in unfair and deceptive practices, such as a companies not adhering to their own privacy policies.[152] As discussed earlier,

146. *See supra* notes 35–36 and accompanying text.

147. Statement of Nicolas P. Terry, *supra* note 131 ("In my opinion federal data protection law that obviates the gaps between our commercial sectors and protects health information wherever it happens to reside is overdue and a necessary precondition for the full embrace of disruptive health apps by both medical professionals and consumers.").

148. One option this Comment does not explore is the expansion of certain HIPAA definitions, such as "business associate" via administrative means to include more mobile health apps under HIPAA's purview. *See* 45 C.F.R. § 160.103 (defining "business associate").

149. Letter from Tom Marino, *supra* note 144 ("We have serious concerns about the consequences of HHS inaction. Advances in mobile health technology have the potential to dramatically improve patient outcomes and the accessibility of health care. This innovation is coming at a rapid pace, but your agency has done little to demonstrate it can manage the significance.").

150. *See id.*

151. *See infra* Part V.C.1–2 (discussing developer privacy guidelines). Although this is the case, there are still findings that not many mobile health applications comply with these guidelines. *See supra* Part IV.C (discussing privacy policies); *App Store Review Guidelines*, APPLE DEVELOPER § 5.1.1 https://developer.apple.com/app-store/review/guidelines/#legal [https://perma.cc/7U23-J599] (last visited Feb. 22, 2018).

152. EXAMINING OVERSIGHT, *supra* note 36, at 31–32 ("FTC has a well-developed body of law enforcing privacy and security practices that are unfair and deceptive, including taking action against an organization that adopts a code of conduct, but does

some mobile health application companies do maintain privacy policies, some even going as far as informing users whenever the application intends to use their data.[153] Although enforcing privacy policies would not be the strongest proxy for closing the HIPAA gap between covered and non-covered entities, it can incentivize mobile health applications developers to craft their privacy policies more carefully.[154] This could, in effect, offer marginally more protections similar to those experienced by users of HIPAA-regulated mobile health applications.[155]

Further enforcing privacy policies would, as mentioned, not be a very robust option for closing the existing HIPAA gaps, the main reason being that non-covered entities do not need to comply with the HIPAA Rules.[156] At the end of the day, privacy policy enforcement may not be enforcing much in terms of user protections. Secondly, privacy policies may be changed without notice.[157] Lastly, not many unregulated mobile health applications have privacy policies.[158] If the FTC began cracking down on privacy policies, mobile health application developers may simply choose not to include a privacy policy or may remove existing user protections and notices to prevent liability.

2. Potential Issues with Agency Intervention. Turning to agencies to close the gaps in HIPAA coverage requires coordination between the numerous agencies that currently regulate this industry in one way or another.[159] HIPAA itself requires oversight in one form or another from over half a dozen agencies.[160] Requiring further regulation from each of these

---

not adhere to that code.").

153. *See supra* Part IV.C (discussing the frequency with which mobile health applications actually have privacy policies and how robust the protections may be).

154. *See id.* (referring to how some privacy policies may not even apply to the mobile health application being used by the user).

155. *See id.* (detailing that policing privacy policies can provide users of non-covered mobile applications more of an actual sense that the applications they are using is actually regulated or subject to some oversight, especially considering many see the existence of a privacy policy as automatically creating rights, obligations, and protections for them).

156. *See generally supra* Part II (discussing HIPAA protections for covered entities and concluding that those protections do not extend to non-covered entities).

157. *See supra* Part IV.C (discussing privacy policies in mobile health applications).

158. *See id.*

159. *See supra* note 135 (discussing the FTC's new interactive online HIPAA tool which required collaboration between several agencies, including the FTC, HHS, ONC, OCR, and FDA).

160. *See Cortez*, *supra* note 79, at 1200 (explaining that "over half a dozen federal agencies" are watching and responding to issues surrounding mobile health); *HIPAA Enforcement*, HHS.GOV (July 25, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html [https://perma.cc/SUQ3-TUVH] (providing that HHS'

agencies can lead to more confusion as to what rules may apply to non-covered mobile health applications and to which agency one needs to answer.[161] Agencies involved would likely need to spend more resources to prevent further confusion, as the FTC and partner agencies did when they developed the Mobile Health Apps Interactive Tool.[162]

C. Stricter Guidelines from Developers and App Stores

Apple's and Android's mobile operation system platforms combine for the lion's share of all smartphones used worldwide.[163] Each of these platforms comes with its own set of policies and guidelines developers must follow in order to sell their applications in each company's online application store.[164] Below, both Apple's and Android's application store policies are examined.

1. Apple's App Store. Apple's App Store Review Guidelines state that "[t]he guiding principle of the App Store is simple—we want to provide a safe experience for users to get apps and a great opportunity for all developers to be successful."[165] Aside from having a general privacy guidelines, Apple also has guidelines exclusively for health and health research applications.[166] The guidelines recognize that "[h]ealth, fitness, and medical data are especially sensitive . . . ."[167] They further

---

Office for Civil Rights, OCR, is responsible for enforcing HIPAA's Privacy and Security Rules); *Enforcement Process*, HHS.GOV (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html [https://perma.cc/X977-BME4] (showing that OCR works in tandem with the DOJ to enforce HIPAA's privacy requirements); *Administrative Simplification Overview*, CTRS. FOR MEDICARE & MEDICAID SERVS. (Oct. 23, 2017, 4:01 PM), https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html [https://perma.cc/5XWN-RE2G] (providing that the Centers for Medicare & Medicaid Services enforce the Administrative Simplification requirements of HIPAA and the Affordable Care Act); *Public Health*, HHS.GOV (Apr. 3, 2003), https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html [https://perma.cc/T4D5-CQWA](noting that the FDA, CDC, and OSHA, among others, have responsibilities under HIPAA).

161. Confusion among those in the mobile health industry was a reason why the Mobile Health Apps Interactive Tool was created. *See* Press Release, FTC Releases New Guidance for Developers of Mobile Health Apps, *supra* note 8.

162. *Id.*

163. *Smartphone OS Market Share, 2017 Q1*, IDC.COM, http://www.idc.com/prodserv/smartphone-os-market-share.jsp [https://perma.cc/9YKH-7GBG] (last visited Dec. 17, 2017) (Apple and Android make up over 99% of world smartphone operating system market share, with Android having 85% of the global market.).

164. *See infra* Part V.C.1–2 (discussing Apple and Android policies and guidelines).

165. *App Store Review Guidelines*, *supra* note 151.

166. *Id.* at § 5.1.3.

167. *Id.*

disallow applications from disclosing health, fitness, and medical research data to third parties for advertising or for reasons other than improving health.[168] The guidelines further require consent from human research and approval of the research from an independent ethics board.[169]

On its face, the health guidelines put forth by Apple appear to protect user data privacy as they prevent any transfer of user health data to third parties for advertising purposes.[170] They fail to provide other protections such as the HIPAA Disclosure Rule and rules for health data during transfer and while it remains idle.[171] The guidelines also leave room for applications to transfer data to organizations that purport to improve "health management," a term that is not further defined in the guidelines.[172] Apple's hands may also not be clean, as they may be collecting large amounts of data themselves in a push to become a more prominent figure in the health industry.[173]

2. Android's Play Store. Unlike Apple, Android's Play Store does not have dedicated guidelines for health and health research data.[174] It does, however, have minimum requirements for developers handling "personal or sensitive user data," which includes personally identifiable information, but not health data specifically.[175] The Play Store requires that applications post a privacy policy in both the Play Developer Console and within the application itself.[176] Developers must also securely handle

168. *Id.* ("Apps may not use or disclose to third parties data gathered in the health, fitness, and medical research context—including from the HealthKit API, Motion and Fitness, or health-related human subject research—for advertising or other use-based data mining purposes other than improving health management, or for the purpose of health research, and then only with permission.").

169. *Id.* (referring to "[a]pps conducting health-related human subject research").

170. *Id.*

171. *See id.*

172. *Id.*

173. *See* Elizabeth Dwoskin & Melinda Beck, *As Apple Moves into Health Apps, What Happens to Privacy?*, WALL ST. J. (Sept. 9, 2014, 7:21 PM), http://on.wsj.com/1uv3KrP. Apple is also pushing its wearable device, the Apple Watch, to insurers and employers, recently reaching an agreement with Aetna to have the giant insurer subsidize the watch to select large employers. *See* Press Release, Aetna, Aetna to Transform Members' Consumer Health Experience Using iPhone, iPad and Apple Watch (Sept. 27, 2016), investor.aetna.com/phoenix.zhtml?c=110617&p=irol-newsArticle&ID=2206242.

174. *See generally Privacy, Security, and Deception*, GOOGLE PLAY, https://play.google.com/about/privacy-security-deception/ [https://perma.cc/Y69Z-VXX6] (last visited Dec. 12, 2017) (providing only that "Apps that feature medical or health-related functionalities that are misleading or potentially harmful" are examples of "common violations" of Google Play's Privacy, Security, and Deception policy).

175. *Id.*

176. *Id.*

sensitive user information.[177] Google further requires that any application collecting data unrelated to the function of the application's described function must prominently highlight how the data will be used, and the user must provide affirmative consent.[178]

Regarding the HIPAA gap, Google's privacy guidelines do not prohibit the transmission of user health data to third parties for marketing or advertising purposes.[179] They do, however, require a secure transmission of data and a privacy policy.[180] However, taking into account that Android's platform accounts for a significantly larger portion of mobile operating systems, Google's lack of specific health data protections are likely to impact more smartphone users.[181] Considering Android's market share, mirroring Apple's health data protections could very well prove to be a significant move in closing the HIPAA coverage gap.

D. Self-Policing from the Mobile Health Industry

Perhaps the least robust way for closing the HIPAA coverage gap would be to encourage the mobile health industry to police itself. This would entail activities such as establishing organizations and adopting a code of conduct,[182] making efforts to further educate or train mobile health application developers in HIPAA and best practices, or having a third party police and rate mobile health applications.[183]

Because these efforts would be self-policing, there would be no requirement for non-covered mobile health application developers to follow any guidelines or best practices, or to continue following them down the road.[184] This means that

177. *Id.* (specifying that even transmission of data must be secure using modern cryptography).

178. *Id.* ("If your app collects and transmits personal or sensitive user data unrelated to functionality described prominently in the app's listing on Google Play or in the app interface, then prior to the collection and transmission, it must prominently highlight how the user data will be used and have the user provide affirmative consent for such use.").

179. *See generally id.* (noting that user health data is not mentioned in the "Prominent Disclosure Requirement").

180. *See id.*

181. *See supra* note 163 and accompanying text.

182. *See* EXAMINING OVERSIGHT, *supra* note 36, at 31 ("For example, in October 2015, the Consumer Electronics Association (CEA) issued 'Guiding Principles on the Privacy and Security of Personal Wellness Data.'").

183. One example of a sort of "watchdog" organization is the Privacy Rights Clearinghouse, which publishes reports on health privacy and health data, among other privacy issues. *About the Privacy Rights Clearinghouse*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/about [https://perma.cc/JLF3-ZX26] (last visited Dec. 27, 2017).

184. *See generally supra* Part II (discussing HIPAA protections for covered entities and concluding that those protections do not extend to non-covered entities).

non-covered entities may boast HIPAA compliance but are not obligated to remain HIPAA compliant.

VI. CONCLUSION

Given the foreseeable demand for health care in the near future, Congress must act to ensure that patient and consumer health information is protected regardless of who holds the information.[185] The technology is moving fast, and the government must act to capture its full potential.[186] In lieu of Congressional reform, agencies, along with the technology industry itself, should step up to close gaps in HIPAA coverage however they can.[187] Doing so will not only protect sensitive health data, it will also provide a predictable business environment for companies and entrepreneurs to innovate and improve health care quality, participation, and accessibility.[188]

Alexis Guadarrama

185. *See generally supra* Part I (discussing the shortage of physicians in the foreseeable future).

186. *See* Letter from Tom Marino, *supra* note 144 ("We have already seen incredible results from early investment in connected health innovation, and the slow pace of government should not stand in the way of patient access to the benefits of this life-changing technology.").

187. *See generally supra* Part V (discussing options to close the gap in HIPAA coverage).

188. *See* Letter from Tom Marino, *supra* note 144.