mHEALTH AND UNREGULATED DATA: IS THIS FAREWELL TO PATIENT PRIVACY?

J. Frazee, M. Finley, & JJ Rohack, MD*

http://dx.doi.org/10.18060/3911.0021

I. INTRODUCTION

Mobile health, or mHealth is a rapidly expanding industry. Globally, the total number of mHealth applications ("mHealth apps") on iOS and Android systems surpassed 100,000 in Q1 of 2014.[1] Market revenue for this industry is projected to reach $26 billion by 2018[2] and the number of mHealth users is projected to reach 1.7 billion worldwide by 2018.[3] mHealth is defined as "medical and public health practice supported by mobile devices," and it is quickly becoming a defining feature of popular technologies such as "mobile phones,… personal digital assistants,… and other wireless devices."[4] Users of mHealth apps produce volumes of data about their health, and this data is highly revealing. Several commentators note that the health data produced by patients' use of mHealth is more revealing than their Electronic Health Record (EHR).[5] Despite this reality, the vast majority of mHealth apps are not subject to significant regulation. The current regulatory scheme governing mHealth is narrow and only concerns a small fraction of the mHealth market, even including those apps covered by the

*J Frazee, BA, University of Houston School of Law; MA Finley, JD, LLM, Vice President, Baylor Scott & White Center for Healthcare Policy; JJ Rohack MD, The William R. Courtney Centennial Endowed Chair in Medical Humanities, Chief Health Policy Officer, Baylor Scott & White Health.

[1] RESEARCH2GUIDANCE, MHEALTH APP DEVELOPER ECONOMICS 2014: THE STATE OF THE ART OF MHEALTH APP PUBLISHING 16 (2014) *available at* http://www.research2guidance.com/r2g/research2guidance-mHealth-App-Developer-Economics-2014.pdf [https://perma.cc/GFV4-2J5X].

[2] *Id.* at 7.

[3] *Id.*

[4] WHO GLOBAL OBSERVATORY FOR EHEALTH, MHEALTH: NEW HORIZONS FOR HEALTH THROUGH MOBILE TECHNOLOGIES, 6 (2011), *available at* http://www.who.int/goe/publications/goe_mhealth_web.pdf [https://perma.cc/PR83-JRNQ] (defining mHealth as "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices.").

[5] *See* JANE SARASOHN-KAHN, HERE'S LOOKING AT YOU: HOW PERSONAL HEALTH INFORMATION IS BEING TRACKED AND USED 5 CA Healthcare Found. (2014).

Health Insurance Portability and Accountability Act (HIPAA)[6]. This paper investigates mHealth apps that are not subject to FDA oversight or HIPAA and the privacy issues involved, and ultimately proposes a United States labeling system intended to ensure consumer confidence and stimulate growth in the mHealth market.

II. THE CURRENT REGULATORY SCHEME

There are two significant regulatory questions for any mHealth app: (1) whether the app will be subject to agency regulation; and (2) whether the app will be subject to HIPAA. Beyond this, no federal laws specifically regulate mHealth applications.[7]

A. Agency Regulation

Multiple agencies share regulatory jurisdiction over the mHealth industry, including: the Food and Drug Administration (FDA), the Office of the National Coordinator for Health Information Technology (ONC),[8] and the Federal Communications Commission (FCC) (hereinafter referred to collectively as "the agencies"). In 2012, Congress directed the agencies, in Section 618 of the Food and Drug Administration Safety and Innovation Act (FDASIA), Public Law 112-144, to collaborate and issue a report

> that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, that promotes innovation,

[6] Health Insurance Portability and Accountability Act of 1996, Public Law 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 29 and 42 U.S.C.) 104th Cong. (1996).

[7] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 19 (2013) [hereinafter INFORMATION RESELLERS] *available at* http://www.gao.gov/assets/660/658151.pdf [https://perma.cc/BA2T-PWLZ].

[8] The ONC is an office within the Department of Health and Human Services and is not an independent agency.

> protects patient safety, and avoids regulatory duplication.[9]

In fulfilling this charge, the agencies issued the "FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework," which explains, in part, that the FDA will primarily regulate health IT with medical device functionality. [10] Health IT with medical device functionality is used to diagnose and treat illnesses, as opposed to software that supports administrative functions like scheduling and documentation.[11]

With respect to mHealth applications, the FDA explained its regulatory approach in a guidance document entitled "Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff." [12] The current approach is for the FDA to focus on a subset of mHealth apps that the agency refers to as "'\mobile medical applications" or "mobile medical apps."[13] An app is determined to be a "mobile medical app" based on two criteria: the app must transform a mobile device into a medical device within the meaning of section 201(h) of the Food, Drug, and Cosmetic Act ("FD&C Act"), [14] and the app must be intended for use as

[9] U.S. FOOD & DRUG ADMIN., FDASIA HEALTH IT REPORT: PROPOSED STRATEGY AND RECOMMENDATIONS FOR A RISK-BASED FRAMEWORK 3 (2014) [hereinafter FDASIA REPORT], *available at* http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf [https://perma.cc/9ZPN-GG3V].

[10] *Id.* at 12.

[11] *Id.* at 11-12.

[12] U.S. FOOD AND DRUG ADMIN., MOBILE MEDICAL APPLICATIONS, GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2015) [hereinafter FDA MEDICAL APPLICATION GUIDANCE], *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf [https://perma.cc/2L65-4NPF].

[13] *Id.* at 7 ("…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.").

[14] Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 321(h) (2016). Section 201 (h) of the Food, Drug, and Cosmetics Act defines device as

a regulated medical device or as an accessory to a regulated medical device.[15] If an app qualifies as a mobile medical app, it will be subject to certain regulatory controls, depending on its risk classification.[16]

There are three device classes.[17] Class I devices are generally considered low risk. These devices are usually exempt from premarket approval, although they must adhere to "general controls."[18] Class II devices are considered moderate risk or present well-understood risks. These devices are generally required to submit 510(k) premarket notification.[19] They are also subject to general controls, as

> an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is… intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes.

[15] FDA MEDICAL APPLICATION GUIDANCE, *supra* note 12.

[16] *Id.* at 30.

[17] Medical Device Amendments of 1976, Pub. L. No. 94-295, 90 Stat. 539. (1976).

[18] 21 CFR §§ 800-98 (1999); FDA MEDICAL APPLICATION GUIDANCE, *supra* note 12, at 19, General controls include: Establishment registration, and Medical Device listing (21 CFR Part 807); Quality System (QS) regulation (21 CFR Part 820); Labeling requirements (21 CFR Part 801); Medical Device Reporting (21 CFR Part 803); Premarket notification (21 CFR Part 807); Reporting Corrections and Removals (21 CFR Part 806); and Investigational Device Exemption (IDE) requirements for clinical studies of investigational devices (21 CFR Part 812).

[19] U.S. Food & Drug Admin., *FDA Premarket Notification 510(k)*, FDA.GOV (Sept. 16, 2015), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/default.htm [https://perma.cc/7TUS-KEG9] (device manufacturers are required to prove that the device to be marketed is "substantially equivalent" to another legally marketed device–meaning the new device is as safe as another device with similar functionality that is already on the market).

well as "special controls,"[20] based on the particular device type. Class III devices are high risk or present risks that are poorly understood. These devices are also subject to general and special controls, as well as premarket approval,[21] and certain other regulatory controls.

Mobile medical apps are a small fraction of the overall mHealth market and the vast majority are Class I or Class II devices.[22] The FDA lists 191 medical mobile apps that have cleared the 510(k) approval process as of February 11, 2016.[23] The agency claims that this is not a comprehensive list; however, it exceeds the total listed in a comprehensive analysis compiled at the end of 2013 by the industry research group MobiHealthNews, which listed the total of approved mobile medical apps at 103. [24] The FDA maintains a database that lists approved mobile medical apps, however these apps are listed alongside other devices that have received 510(k) approval and are not uniquely identified as

[20] 21 U.S.C. § 360c(a)(1)(B). The Secretary of Health and Human Services promulgates special controls when determined to be necessary for the assurance of safety and effectiveness. Special controls include: Performance standards; Post-market surveillance; Patient registries, Special labeling requirements; Premarket data requirements; and Guidelines.

[21] FDA Premarket Approval (PMA) http://www.fda.gov/medicaldevices/deviceregulationandguidance/howtomarketyourdevice/premarketsubmissions/premarketapprovalpma/default.htm [https://perma.cc/73ZD-THLV]. *See* U.S. Food and Drug Admin., *supra* note 19 (Premarket approval uses scientific evidence to ensure the safety and effectiveness of devices that are particularly risky or present poorly understood risks).

[22] Christy Foreman, Dir. Office of Device Evaluation, Ctr. for Devices and Radiological Health, Health Information Technologies: Administration Perspectives on Innovation and Regulation (Mar. 21, 2013), http://energycommerce.house.gov/hearing/health-information-technologies-administration-perspectives-innovation-and-regulation#video (Director Foreman testified that there had not been a Class III mobile medical application to date).

[23] U.S. FOOD AND DRUG ADMIN., *Examples of Pre-Market Submissions that Include MMAs Cleared or Approved by FDA*, FDA (Feb. 11, 2016) http://www.fda.gov/medicaldevices/digitalhealth/mobilemedicalapplications/ucm368784.htm [https:// perma.cc/E3LF-2DLN] [hereinafter *Pre-Market MMAs*] (last updated Feb. 11, 2016).

[24] *103 FDA Regulated Mobile Medical Apps*, MOBIHEALTHNEWS (Nov. 25, 2013), *available at* http://mobihealthnews.com/research/103-fda-regulated-mobile-medical-apps/ [https://perma.cc/W2MM-QN8A].

apps.[25] As a result, approved apps are not easily searchable and may be difficult to identify as apps rather than any other medical device. Given the pace of the FDA's approval of mobile medical apps, it is reasonable to assume that the total number of approved apps is near the listed 191,[26]a small fraction of the more than 100,000 mHealth apps on the market.[27]

The FDA is pursuing this narrow regulatory framework for a variety of reasons. First, the FDA is following a risk-based approach,[28] with its primary focus on those apps that pose significant risk to patient safety.[29] Using the risk-based framework laid out by the Medical Device Amendments of 1976,[30] the agency categorizes mobile medical apps by class. Apps presenting significant risks are sent to market after obtaining the proper approval. Second, Congress directed the FDA to promote innovation in the mHealth industry[31] and

[25] *Pre-Market MMAs*, *supra* note 23.

[26] *Id.*

[27] RESEARCH2GUIDANCE, *supra* note 1 at 7.

[28] FDA MEDICAL APPLICATION GUIDANCE, *supra* note 12 at 3.

[29] *Id.* at 8 (2015), ("…we intend 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.").

[30] FDASIA REPORT, *supra* note 9 at 5 n.7.

> The Medical Device Amendments of 1976 created three device classes. The three classes are based on the degree of control necessary to assure that the various types of devices are safe and effective. Class I devices are generally low risk. Such devices are for the most part exempt from premarket review and are subject–unless exempt–to the requirements for reporting of adverse events, manufacturing and design controls, registration and listing, and other "general" controls. Class II devices generally present moderate or well-understood risks. Such devices are subject to general controls and are usually subject to premarket review. Class II devices are also subject to "special controls" that are closely tailored to the risks of the particular device type. Class III devices generally present high or poorly understood risks. In addition to general controls, Class III devices are subject to premarket approval and certain other regulatory controls.

[31] *Id.* at 3.

has expressed concern that regulation could stifle the industry in its infancy. Several bills have been proposed to restrict or limit FDA regulation over the mHealth industry, including: The Medical Electronic Data Technology Enhancement for Consumers' Health Act of 2015 ("MEDTECH Act"),[32] the Preventing Regulatory Overreach to Enhance Care Technology Act of 2014 ("PROTECT Act"),[33] and the Sensible Oversight for Technology which Advances Regulatory Efficiency Act of 2015 ("SOFTWARE Act");[34] none have been passed by Congress. Third, stakeholder comments have emphasized that a flexible regulatory scheme is necessary to allow for the development of new technologies.[35]

With limited resources and significant pushback from both Congress and stakeholders, it is not surprising that the FDA is conducting a narrow regulatory framework. However, commentators have expressed concern over the FDA's light touch on the industry,[36] citing potential danger to patients, or claiming that unreliable technology will inhibit adoption of mHealth by medical professionals, while others assert that more stringent regulation could provide economic benefit to stakeholders.[37]

[32] Medical Electronic Data Technology Enhancement for Consumers' Health (MEDTECH) Act, S. 1101, 114th Cong. (2015).

[33] Preventing Regulatory Overreach To Enhance Care Technology Act of 2014, S. 2007, 113th Cong. (2014).

[34] Sensible Oversight for Technology Which Advances Regulatory Efficiency Act of 2013, H.R. 2396, 114th Cong. (2015).

[35] FDASIA REPORT, *supra* note 9, at 9.

[36] *See generally* Natalie R. Bilbrough, *The FDA, Congress, and Mobile Health Apps: Lessons from DSHEA and the Regulation of Dietary Supplements*, 74 MD. L. REV. 921 (2015) (proposing an "Office of mHealth" within the FDA to provide greater expertise and further regulate the industry); Alex Krouse, *iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices*, 9 IND. HEALTH L. REV. 731 (2012) (suggesting a decentralized approval process for mHealth devices); Daniel F. Schulke, *The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing*, 93 B.U. L. REV. 1699 (2013) (analyzing various regulatory models and ultimately suggesting a meta-regulatory approach).

[37] MOBIHEALTHNEWS RESEARCH, FDA REGULATION OF MOBILE HEALTH 47 (2nd ed.) (on file with the *Indiana Health Law Review*).

B. HIPAA and mHealth

The regulatory efforts of the FDA are an important first step for ensuring patient safety and promoting the adoption of mHealth in the healthcare industry. However, the majority of mHealth apps operate unencumbered by significant regulation. Beyond the FDA's regulation of mobile medical apps, mHealth apps face one significant regulatory question: when is an mHealth app subject to HIPAA?[38] HIPAA rules only apply to "covered entities" and their "business associates."[39] A covered entity is defined as a health plan, healthcare clearinghouse, or healthcare provider.[40] A business associate is a person, subcontractor, or organization that receives or transmits "protected health information" on behalf of a covered entity or the business associate.[41] Protected health information (PHI) means individually identifiable health information.[42] An mHealth app is subject to HIPAA if it receives or transmits a patient's PHI or is used by a covered entity or business associate.[43] PHI is created in the context of patient care and apps that store or transmit that information are subject to HIPAA. On the other hand, apps that are consumer oriented manage user-generated information that is not HIPAA protected, such as the calories in one's meal or the amount of steps one has taken on a given day. As long as an mHealth app does not deal in PHI or communicate with a covered entity or business associate it is not subject to HIPAA. Additionally, de-identified information is not subject to HIPAA protection.[44]

[38] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 104th Cong. (1996).

[39] 45 C.F.R. § 160.103 (2016).

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] Adam H. Greene, *When HIPAA Applies to Mobile Applications,* MOBIHEALTHNEWS (June 16, 2011), http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/ [https://perma.cc/Z2K5-5DR9].

[44] Dept. Health & Human Svcs., *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy*

For example, "Bob" is concerned that he might be an alcoholic and has been clinically diagnosed with depression. Bob uses a blood alcohol content calculator on his smart phone to help moderate his drinking and a mood-tracking app that allows him to enter his mood at a given time and track fluctuations. Two recently launched startup companies produced these apps and neither shares information with covered entities. The data collected by these companies is not subject to HIPAA, even though both of the companies' databases identify Bob by name and include a listing of his unique mobile identification number. Bob's self-regulation is not going well, so he goes to visit a physician at a nearby clinic. The physician prescribes Bob with anti-depression medication. At the physician's recommendation, Bob downloads a HIPAA compliant telehealth application that allows Bob to video chat with his physician rather than drive in to the clinic on a regular basis. Bob consults with his physician using the telehealth app once a month until his condition improves and his treatment ends a year later. The data collected by the telehealth app is subject to HIPAA regulation because Bob uses the app to consult with a healthcare provider (i.e. a covered entity).

Bob's communications with his physician are protected by the HIPAA Privacy and Security Rules.[45] However, Bob's entries in his smartphone using the blood alcohol content calculator and mood-tracking apps are not protected by such rules. Both apps were free to download and Bob agreed to their terms and conditions without reading their privacy policies, a common consumer practice.[46] The privacy policies for both apps state that data collected will be sold to third parties for marketing purposes. While Bob views his past

Rule (2012), [hereinafter *De-identification Guidance*] http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/#rationale [https://perma.cc/8HTW-J9LY].

[45] *See* 45 C.F.R. Part 160 and Part 164, Subparts A and 45 C.F.R. §§ 160.101-160.552, 164.102-164.534 (2013).

[46] SDL, MARKETING DATA AND CONSUMER PRIVACY: WHAT YOUR CUSTOMERS REALLY THINK 3 (Feb. 26, 2014), *available at* http://www.scribd.com/doc/214108509/SDL-Marketing-Data-and-Consumer-Privacy-What-Your-Customers-REALLY-Think [https://perma.cc/J3EX-MF73]. In a survey of more than 4,000 individuals, 65% of respondents reported that they rarely or never read privacy policies before making online purchases.

year as a success, he considers both his struggle with alcohol and depression deeply personal. Unbeknownst to Bob, he has documented both in great detail and his user generated health data can now be sold as a commodity on the open market through a system of data brokers.

III. USER GENERATED HEALTH INFORMATION

Like Bob in the above hypothetical, real-world persons are generating volumes of sensitive health data and signing it away as a commodity without fully understanding the implications. While mHealth apps and the services they provide can help users manage personal health, third party exploitation of that data may violate patient privacy and cause a chilling effect on the adoption of this useful technology.

A. How Consumer Data is Collected

A study by Evidon, an analytics firm (now restructured as Ghostery, Inc.), found that the top twenty mHealth apps sold "information to up to [seventy] third party companies."[47] Another study, conducted by Privacy Rights Clearinghouse, analyzed forty-three popular wellness apps for technical security risk and found that twenty of these apps transferred individually identifiable information about its users to third parties.[48] The study also found that approximately half of the apps analyzed published a privacy policy and complied

[47] Emily Steel & April Dembosky, *Worried- Well Online Have New Symptom to Fear*, CNBC: FIN. TIMES, (Sept. 1, 2013), *available at* http://www.cnbc.com/id/101002123 [https://perma.cc/22GD-5W9M].

[48] Craig Michael Lie Njie, *Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications*, PRIVACY RIGHTS CLEARINGHOUSE 7 (July 15, 2013) *available at* https://www.privacyrights.org/sites/privacyrights.org/files/CCPF-SmartphoneHealthApps-TechnicalReport-Final-July15-2013%281%29_0.pdf [https://perma.cc/3YGY-Q2GC]. The study ranked apps by risk level, indicating that apps with a risk level of 5 or higher transferred individually identifiable information to third parties. The study lists twenty apps at risk level 5 or higher. Therefore twenty of the apps studied transferred individually identifiable information to third parties.

with it.[49] In light of these two studies, the Federal Trade Commission (FTC) decided to run a similar experiment. Analyzing twelve mHealth apps, the team found a number of personal details were being transmitted to third parties.[50] For example, "22 third parties received additional information about our consumers such as exercise information, meal and diet information, medical symptom search information, zip code, gender, geo-location."[51] These studies point to a broad trend of data sharing, with few limitations on what type of data service providers are willing to sell or share with third parties.

A 2015 study mirroring the techniques used by Privacy Rights Clearinghouse and the FTC analyzed several categories of apps and similarly found mHealth apps sharing information with third parties[52]. However the researchers observed only three of the thirty mHealth apps tested sent medical information to third parties.[53] While this finding is significantly lower than the FTC report and Privacy Rights Clearinghouse Study, it is unclear why this difference exists.[54] Alongside this observation, the study notes that on the Android platform "Health & Fitness and Communication apps sent sensitive data, mostly [personally identifiable information] data, to more third-party domains than apps in other categories," while iOS apps did not similarly stand out

[49] *Id.* at 20.

[50] SPRING PRIVACY SERIES: CONSUMER GENERATED AND CONTROLLED HEALTH DATA, FED. TRADE COMM'N 26 (2014), *available at* https://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf [https://perma.cc/3YH5-BPDN].

[51] *Id.* at 27.

[52] Jinyan Zang et al., *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps,* TECH. SCIENCE (Oct. 30, 2015), http://techscience.org/a/2015103001 [https://perma.cc/6YHF-BFN8].

[53] *Id.*

[54] This anomalous finding may be due to the sample size, the research methods (this research group did not use WireShark or tcpdump to monitor non-TCP traffic, while Privacy Rights Clearinghouse did), or changing attitudes among app developers toward privacy implications. There is no clear explanation for the difference in this study and others that indicate broad sharing of behavioral data.

by category.[55] Among the mHealth apps tested, nearly all shared information with third parties that the researchers deemed sensitive, including personally identifiable information, behavioral data, and location data.[56]

Several commentators note that the data revealed by patients' digital footprint is more revealing than their EHR.[57] A physician is only able to test a finite number of variables during a patient visit, whereas mHealth apps continuously monitor patients' habits. Furthermore, much of the data collected occurs without the user being involved or aware that a data transmission has taken place.[58]

A qualitative study conducted by the International Institute of Communications looked into users' perceptions of data management and found "limited awareness" of the techniques by which user data was collected.[59] The study identified two types of data collection: actively collected data and passively collected data. Actively collected data is information that is voluntarily revealed to the service provider by the user–for example, entering what one ate that day into a diet tracking app.[60] And passively collected data[61] is information that is automatically revealed to the service provider and does not require active participation by the user–for example, location metadata[62] being sent to the service provider along with one's diet entry. The study also distinguishes a subset of passively collected data called inferred data. Inferred data is information that is inferred from existing data through analytic models–for example, analyzing a user's dietary patterns to predict that this

[55] Jinyan Zang et al. *supra* at note 52.

[56] *Id.*

[57] JANE SARASOHN-KAHN, HERE'S LOOKING AT YOU: HOW PERSONAL HEALTH INFORMATION IS BEING TRACKED AND USED 5 (2014).

[58] *Personal Data Management: The User's Perspective*, International Institute of Communications, 12 (2012) (on file with the *Indiana Health Law Review*).

[59] *See id* at 14.

[60] *Id* at 12.

[61] *Id.*

[62] Metadata is data that describes other data. For instance, an app may store calorie counts as a series of numbers. Metadata could help make sense of this raw data by labeling the numbers as "calorie counts."

particular user will likely develop type 2 diabetes.[63] Users are aware of actively collected data, because it requires their active participation; but users generally are not aware of passively collected data or inferred data because it occurs without their participation.[64]

B. How Consumer Data is Used

The data produced by mHealth users is stored in a number of places. Some information is stored locally on the user's mobile device, however the bulk of user data is stored on servers. These servers may belong to the company that developed the mHealth app, or, as is more often the case, to a contracted third party that offers server storage as a service. For many users, the chain of storage and data sharing should ideally end here, so that only the key service providers have access to user data. But rarely does the chain of data sharing end here. Often, data is shared with or sold to a number of third parties. The primary buyers in the consumer information data market are called data brokers.[65] Additionally, other entities purchase consumer data for a variety of purposes.

1. Use by Data Brokers

In 2014, the FTC released a report titled "Data Brokers: A Call for Transparency and Accountability."[66] The report examines the products offered by nine prominent data brokers and the types of data they collect, as well as common industry practices.[67] The FTC found that these companies collect a great deal of information about consumers–one company, Acxiom, reported to have "over 3000 data segments

[63] *Personal Data Management: The User's Perspective*, *supra* note 58 at 13.

[64] *Id.* at 40.

[65] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, i (2014) (defining data brokers as "companies that collect consumers' personal information and resell or share that information with others.").

[66] *Id.*

[67] *Id.* at i.

for nearly every U.S. consumer."[68] While some of the data collected by data brokers is publicly available or seemingly benign, the FTC notes that other information is sensitive, specifically citing health data.[69]

The report identifies mobile devices as a new source of consumer data that "has dramatically increased the availability, variety, and volume of consumer data."[70] Data that is collected is used to create descriptive profiles about consumers, and these profiles include consumers' health information. For example, a consumer profile may include descriptive elements such as: "Ailment and Prescription Online Search Propensity", "Buy Disability Insurance", "Geriatric Supplies", "Allergy Sufferer", "Tobacco Usage", "Purchase History or Reported Interest in Health Topics including: Allergies, Arthritis, Medicine Preferences, Cholesterol, Diabetes, Dieting, Body Shaping, Alternative Medicine, Beauty/Physical Enhancement, Disabilities, Homeopathic Remedies, Organic Focus, Orthopedics, and Senior Needs", among other information. [71] Additionally, consumers are categorized more generally with labels "such as 'Expectant Parent,' 'Diabetes Interest,' [or] 'Cholesterol Focus.'"[72] To some degree, such labels provide benefits to consumers. On the other hand, these labels can be used in ways that are adverse to consumer interests. For instance, the report states, "while data brokers have a data category for 'Diabetes Interest' that a manufacturer of sugar-free products could use to offer product discounts, an insurance company could use that same category to classify a consumer as higher risk."[73]

Consumers are often unaware that data brokers even exist because data brokers do not interact directly with consumers.[74] Only two of the nine data brokers studied by the FTC required the data sources they contracted with to provide notice to consumers that their information will be

[68] *Id.* at 8.
[69] *Id.* at v.
[70] *Id.* at 5.
[71] *Id.* at B-6.
[72] *Id.* at 47.
[73] *Id.* at vi.
[74] *Id.* at i.

shared with third parties.[75] Additionally, "seven of the nine data brokers buy from or sell information to each other."[76]

The findings of the FTC reiterated those of a separate report issued by the Government Accountability Office (GAO) in 2013.[77] The GAO similarly identifies the collection of health data as a cause for concern and notes that "mobile devices have enabled even cheaper, faster, and more detailed data collection and sharing among resellers and private-sector companies."[78] Additionally, the GAO report explains that there is no federal privacy law that specifically addresses mobile applications and technologies,[79] nor does federal law generally restrict the methods for data collection or the sources of collection.[80] Ultimately, the statutory landscape leaves consumers with "limited legal rights to control what personal information is collected, maintained, used, and shared and how."[81]

2. Use by Other Entities

New uses for data are being discovered, and while less is known about these practices, it is important to note that health data extends beyond the context of data brokers and the products they offer. On June 26, 2014, Bloomberg reported that the largest hospital chains in the Carolinas and Pennsylvania were using consumer data to identify high-risk patients.[82] The chains reportedly use this data to predict when patients might fall ill due to unhealthy habits and intervene before reaching a point that would require more costly care. Similarly, a study conducted by a student at the Carolina Health Informatics Program of the University of

[75] *Id.* at 16.

[76] *Id.* at 14.

[77] INFORMATION RESELLERS, *supra* note 7.

[78] *Id.* at 19.

[79] *Id.* at 24.

[80] *Id.* at 18.

[81] *Id.* at 17.

[82] Shannon Pettypiece & Jordan Robertson, *Hospitals Soon See Donuts-to-Cigarette Charges for Health*, BLOOMBERG TECH. (June 26, 2014, 12:35 PM), http://www.bloomberg.com/news/articles/2014-06-26/hospitals-soon-see-donuts-to-cigarette-charges-for-health [https://perma.cc/ZD6K-WJMG].

North Carolina at Chapel Hill reveals that mHealth data can be used to improve risk profiling in the insurance industry and track users' engagement with health and wellness activities.[83]

While evidence of such use is scant, it is clear that providers and insurers could use mHealth data to monitor and profile patients' behaviors. Used in this manner, mHealth data could provide increased understanding of patient populations, but such use may simultaneously motivate paternalistic practices. In a system where global payments to providers are based on population health, direct intervention may be a more common interaction with patients. For instance, a patient with diabetes mellitus who is not physically active as recommended will have higher blood glucose and increased risk for infections. That patient may receive a phone call or home visit from a care coordinator to motivate them to get into an exercise program as a result. Ultimately, patients may be unwilling to use mHealth tools if doing so means that their behaviors will be monitored and judged by providers and insurance companies.

IV. EXISTING POLICY IS INADEQUATE IN THE MHEALTH CONTEXT

Data collection, analysis, and use have been a subject of concern for quite some time. A common reference point for policies governing data practices is the Fair Information Practice Principles (FIPPs).[84] These guidelines were initially created by an advisory committee to the Secretary of Health, Education, and Welfare and were the basis of the Privacy Act of 1974,[85] which governs federal agencies' collection and use

[83] Dave Barrett, *mHealth at BCBSNC–An Evaluation of the Collection and Usage of Mobile Health Data through Existing BCBSNC Resources,* UNC CAROLINA HEALTH INFORMATICS PROGRAM, http://miksa2.ils.unc.edu/chip/practicum/files/posters/pdf/dave_barrett.pdf [perma.cc/JKW7-SDLC].

[84] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, DHEW PUB. NO. (OS)73-94, RECORDS, COMPUTER, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973), *available at* https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/929M-5XJH].

[85] 5 U.S.C. § 552a (1974).

of personal information. In 1980 the FIPPs were revised by the Organisation for Economic Co-operation and Development (OECD) and became an internationally recognized set of privacy principles.[86] The FIPPs are principles and while they have been used as a reference point for the creation of laws at home and abroad, they do not carry any legal authority themselves. These principles are admirable (e.g., collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability[87]), but they are broad and do not adequately address consumer concerns regarding mHealth privacy on their own. Additionally, there are a limited number of torts associated with privacy harms, and those that do exist are ill suited to address the privacy issues involved in large-scale, systematic data collection.[88] Furthermore, statutory protections, implemented before the age of cloud computing, are insufficient and broadly permit third party access.[89]

A. The Fair Information Practice Principles Were Drafted Before Big Data

The FIPPs were created over four decades ago and rest on certain assumptions about data and its usage that must be reevaluated in a new age of computing. These principles continue to serve as meaningful guidelines, but forward thinking policies will require more nuanced considerations.

[86] OECD, OECD Guidelines on the Protection of Privacy and Transborder FlowS of Personal Data (1980), *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [http://perma.cc/P4XF-PGQH]. (These guidelines were recently updated in 2013 with additional enforcement and privacy protections).

[87] *Id.*

[88] President's Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective 6-7 (2014), *available at* https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/W79K-PK3G].

[89] *See* Electronic Communications Privacy Act, 18 U.S.C. § 2702 (1986) (allowing third party access to customer communications or records with legal consent).

In short, "big data" has changed the game.[90] While big data encompasses much more than mHealth, it is necessary to understand the tools and economic forces of big data to see why the FIPPs are no longer adequate. Put simply, exponential growth in computing power is continuously occurring and this growth has altered the ground rules upon which the FIPPs were built.

1. *Big Data and Emerging Analytical Techniques*

In January of 2014, President Barack Obama ordered a comprehensive review of big data technologies by counselor John Podesta and the President's Council of Advisers on Science and Technology.[91] Two workgroups executed this order in a 90-day, simultaneous effort, and produced insightful reports on the technologies and policy implications of big data.[92] These reports (hereinafter referred to as the "Big Data Report" and the "PCAST Report") supplement one another to explain what big data is, what its benefits and pitfalls may be, and how current and future policy will be affected by big data.

Big data is commonly thought of as the "3 Vs": Volume, Variety, and Velocity.[93] Volume refers to the sheer amount,

[90] Jonathan Stuart Ward & Adam Barker, *Undefined By Data: A Survey of Big Data Definitions*, ARXIV.ORG (Sept. 20, 2013, 1:51:18 PM), COMPUTER SCIENCE DATABASES *available at* arXiv:1309.5821, http://arxiv.org/abs/1309.5821/ [http://perma.cc/M53M-MWZ2] (defining big data as "a term describing the storage and analysis of large and or complex data sets using a series of techniques including, but not limited to: NoSQL, MapReduce and machine learning.")

[91] *Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, WASHINGTON POST (Jan. 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html/ [http://perma.cc/HKC4-VCHE].

[92] JOHN PODESTA ET AL., BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 3-4 (2014), *available at* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[93] *IT Glossary*, GARTNER, INC., https://www.gartner.com/it-glossary/big-data/ [http://perma.cc/K8QD-6JQ9] (last visited Feb. 17, 2016). Gartner's *IT Glossary* defines big data as "high-volume, high-velocity and/or high–variety information assets that demand cost-

variety refers to the different types, and velocity refers to how quickly it is produced.[94] It is "big" because the amount of data sources has grown exponentially in recent years. As stated in the Big Data Report, "[t]he declining cost of collection, storage, and processing of data, combined with new sources of data like sensors, cameras, geospatial and other observational technologies, means that we live in a world of near-ubiquitous data collection."[95] Data can be "born digital"[96] or "born analog."[97] Data that is born digital is created by users or automated computer proxies for use by a computer system (e.g. entering food one has eaten into a diet tracking application, posting a review of the app, or metadata that is passively collected with a given transaction).[98] Data that is born analog comes from the physical world (e.g. a photo of a wound, one's heartbeat measured by a sensor, or the video content of a sonogram).[99] All of this seemingly disparate data can be assembled and analyzed together to reveal unexpected insights about a specified group or individual, a technique known as "data fusion."[100] The results of such assembly and analysis can be useful in healthcare research.

For example, one study used data taken from neonatal monitors to find early warning signs of infection that were unobservable to attending physicians.[101] Similarly, the hospital systems in the Carolinas and Pennsylvania, mentioned above, were able to use consumers' purchase history information to identify patients at risk of hospital

effective, innovative forms of information processing for enhanced insight, decision making, and process automation."

[94] PODESTA ET AL., *supra* note 92, at 4.

[95] *Id.* at 4. (explaining just how big "big data is," the report indicates that in 2013 an estimated four zetabytes were produced worldwide–a zetabyte equals 1,000,000,000,000,000,000,000 bytes, or units of information.").

[96] *Id.* at 4.

[97] *Id.*

[98] *Id.* at 19.

[99] *Id.* at 22.

[100] *Id.* at 4.

[101] IBM, SMARTER HEALTHCARE IN CANADA: REDEFINING VALUE AND SUCCESS 5 (2012) *available at* https://www.ibm.com/smarterplanet/global/files/ca__en_us__healthcare__ca_brochure.pdf [https://perma.cc/ZKZ8-CN2F].

admission due to unhealthy habits.[102] While both of these uses of big data analytics provide a benefit, namely fighting infections in premature infants and reducing healthcare costs through early intervention, the second example poses a privacy issue that the first does not. It seems unlikely that parents would object to improved care for their infants. But are patients comfortable with the notion that insurers are monitoring their daily habits? This type of monitoring practice may lower treatment costs and assist behavioral change, but it may also do harm to patients' perceptions of healthcare institutions and violate basic notions of privacy that people hold.[103]

Such considerations are particularly important in the context of mHealth. Users' data can be combined and analyzed to determine a number of piercing insights. Consider the variety of information that mHealth apps collect about a given user. Sleep monitoring apps track sleep schedules, motion during sleep, and so-called "sleep debt"; diet tracking apps record what foods the user ate and for which meal, their calorie count, a user's weight, and nutritional information; fitness apps record calories burned, whether a user does aerobic or anaerobic activities, and the frequency with which one exercises; alcohol tracking apps log how many drinks the user consumes, how frequently, and blood alcohol content; smoking cessation apps record the number and frequency of cigarettes consumed; pregnancy tracking apps record likely conception dates, due dates, and symptoms; mood tracking apps record emotional and psychological information; period trackers record menstruation dates, chart ovulation and fertility, and duration of menstruation and symptom searching apps record symptoms searched.[104] This snapshot of mHealth apps

[102] See discussion *infra* Part III.B.2.

[103] PODESTA ET AL., *supra* note 92, at 79. Professional practices are currently one of the few sectors that enjoy a great deal of public trust with personal data–a finding that may change as public awareness of health surveillance grows.

[104] This general list of apps and the types of data they collect was compiled through a search of the iOS App Store and Google Play Store. It is a small sample of the types of apps offered in mobile app markets and the information they collect.

and the information they record is far from a complete picture of what is available, but the variety of information is extraordinary. This variety, in and of itself, poses a difficult problem for the protection of individual privacy.

2. Big Data Weakens De-identification

Under the HIPAA Privacy Rule, patient data may be shared broadly so long as it is de-identified.[105] De-identification works by stripping identifying information about persons from a data set.[106] The Safe Harbor Method of the Privacy Rule requires the removal of eighteen specific fields of information.[107] Some privacy conscious companies similarly de-identify data they collect before selling or sharing that data with third parties.[108] But PCAST warns that de-identification as a method of protecting privacy has limited value moving forward, because re-identification methods are becoming highly sophisticated.[109] In fact, the Big Data Report states, "[c]ollective investment in the capability to fuse data is many times greater than investment in technologies that will enhance privacy."[110] Data fusion allows seemingly anonymous data to be re-

[105] *De-identification Guidance, supra* note 44.

[106] *Id.* Covered entities can satisfy the de-identification standards of the Privacy Rule by two methods: "1) a formal determination by a qualified expert; or 2) the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual."

[107] *Id.*

[108] *See, e.g., Privacy Policy,* N. Y. TIMES http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html#e [https://perma.cc/W7P5-JH8G] (last updated June 10, 2015) (discussing that they "share information about our audience in aggregate or de-identified form. Nothing in this Privacy Policy is intended to restrict our use or sharing of aggregated or de-identified information in any way."); *see also* PODESTA ET AL, *supra* note 92, at 8.

[109] PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, EXEC. OFFICE OF THE PRESIDENT: Big Data and Privacy: A Technological Perspective 44 (2014) [hereinafter *Big Data Report*] *available at* https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/F3RB-SC5Q].

[110] PODESTA ET AL., *supra* note 92, at 54.

identified.[111] Efforts to protect the privacy of users through de-identification are increasingly futile as this technique is becoming obsolete.[112]

Additionally, prohibitions on re-identification would be difficult. It is not always obvious which data elements will identify an individual. With a large enough data set, individuals can be identified through the "mosaic effect", whereby seemingly anonymous and unrelated data create patterns from which identifying information can be inferred. [113] While data fusion paints a seemingly bleak picture for the privacy of health information, the problem is one that can be compartmentalized.

B. Compartmentalizing Health Data

Re-identification poses a real problem for the privacy of health data. But solving the problem for PHI is different from

[111] K. El Emam et al., *Evaluating the Risk of Re-identification of Patients From Hospital Prescription Records* 62 CANADIAN J. OF HOSPITAL PHARMACY 307, 307-319; (2009); G. Loukides et al., *Symposium, The Disclosure of Diagnosis Codes Can Breach Research Participants Privacy*, 17 J. AM. MED. INFORMATICS ASSOCIATION 322-327 (2010); B. Malin & L. Sweeney, *How (Not) to Protect Genomic Data Privacy in a Distributed Network: Using Trail Re-identification to Evaluate and Design Anonymity Protection Systems*, 37 J. OF BIOMEDICAL INFORMATICS, 179-192 (2004); L. Sweeney, *A Presentation at the Workshop on the HIPAA Privacy Rule's De-Identification Standard, Data Sharing Under HIPAA: 12 Years Later*, Washington, DC. March 8-9 (2010).

[112] *Big Data Report, supra* note 111, at 38-39. Programming languages used by those who manage data typically have commands like "join" that connect data sets based on common data points. To illustrate how easy it is to re-identify data, suppose a company has matrix A with five columns of data and matrix B with five columns of data. Suppose matrix A and B overlap on one common data point. A programmer can write a command that "joins" matrix A and B based on their common data point, creating one matrix with 9 columns of data. Given the sheer amount of data being produced by users and stored by data brokers, it does not take long to find a consistently unique data point to merge data sets with–like a cell phone's IMEI or any other device-specific number.

[113] OFFICE OF MGMT. AND BUDGET, EXEC. OFFICE OF THE PRESIDENT: Open Data Policy—Managing Information as an Asset Memorandum for the Heads of Executive Departments and Agencies (2013), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf [https://perma.cc/D73R-XKU3].

solving the problem for mHealth data. When PHI is de-identified, it is no longer PHI and its disclosure is not restricted.[114] If that data is re-identified, then it is once again PHI and receives all of the legal protections originally prescribed to PHI.[115] On the other hand, mHealth data, as discussed above, typically does not fall under the auspices of HIPAA.[116] There are no requirements to de-identify data from non-HIPAA apps (though doing so is encouraged[117]), and it is often sold to or shared with third parties.

Currently the only protections afforded to users of mHealth apps not covered by HIPAA are those detailed in the privacy policy of the app. Privacy policies evolved from the "notice and consent" model prescribed by the FIPPs.[118] But consumers struggle to understand privacy policies, and many do not bother reading them before agreeing to their terms.[119] Additionally, the technical nature of *how* data is collected, secured, and shared is difficult to understand as a consumer–particularly when it is embedded in the legal language of a privacy policy. Even if consumers do choose to read privacy policies, doing so is not particularly enlightening. Privacy policies are written primarily to cover the developing company's legal notice requirements and not to accurately inform the consumer.[120] One study came to the conclusion that, "[t]he only way for a user to know how great a privacy risk an app may be posing is by doing a technical evaluation–something beyond the ability of almost all users."[121] PCAST similarly observed, "Only in some fantasy

[114] *De-identification Guidance, supra* note 44.

[115] *Id.* at 9.

[116] *See infra* Part II.B.

[117] *Using Consumer Health Data: Some Considerations for Companies,* FED. TRADE COMM'N: BUSINESS BLOG (Apr. 28, 2015, 9:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/04/using-consumer-health-data-some-considerations-companies [https://perma.cc/7RXU-ZYEQ].

[118] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 86, at xxvi; *see also Big Data Report, supra* note 109, at 38.

[119] SDL, *supra* note 46 (finding in a survey of more than 4,000 individuals, 65% of respondents reported that they rarely or never read privacy policies before making online purchases).

[120] Craig Michael Lie Njie, *supra* note 48, at 20-21.

[121] *Id* at 21. The technical evaluation techniques described in this study require users to intercept the internet traffic of their mobile devices

world do users actually read these notices and understand their implications before clicking to indicate their consent."[122] Under the "notice and consent" model, the consumer is incapable of modifying the privacy policy and is left with a binary choice: agree to the terms or stop participating in digital society. A new system is needed to restore meaningful choices to consumers.

V. REMOVING UNCERTAINTY WILL PROVIDE MEANINGFUL CHOICES IN THE MHEALTH MARKET

Congress deemed health information uniquely private and worth protecting when it passed HIPAA's stringent Privacy and Security Rules. One would expect that user generated data should receive the same protections, but such data presents a unique problem. As noted in the Big Data Report, "[t]he powerful connection between lifestyle and health outcomes means the distinction between personal data and health care data has begun to blur."[123] Data one may never think of as health information can be extrapolated and cross-referenced to produce deep insights into an individual's health. For instance, by cross-referencing purchasing information with additionally purchased consumer data, Target was able to identify customers who were in their second trimester of pregnancy.[124] However mHealth applications are uniquely revealing. Such apps produce detailed logs of a user's health information, and do not require costly or difficult analysis. While it is true that data fusion allows some health information to be inferred, inferred data does not provide the level of detail and granularity that mHealth apps effortlessly expose. In particular, devices that measure biometric information through sensors provide data that cannot be inferred to the same level of accuracy. If the unfettered trade of detailed

by connecting a "man-in-the-middle, SSL-enabled proxy server", and decoding their internet traffic through a series of software tools that go far beyond the average user's understanding of computers. *Id.* at 11.

[122] *Big Data Report, supra* note 109, at xi.

[123] *Id.* at 23.

[124] Charles Duhigg, *How Companies Learn Your Secrets*, N. Y. TIMES MAGAZINE (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0 [http://perma.cc/LGG3-NGAT].

biometric and behavioral data is allowed, HIPAA's privacy protections will become obsolete.

Additional government intervention is needed, but given the inherent problem in defining or regulating "health data" the government cannot realistically ban the sale of health data. Instead, Congress should create a simple labeling system. In particular, there is a need for two labels: (1) a label that reads "HIPAA Compliant", and (2) a label that reads "Confidential." Apps marked HIPAA Compliant would be just that, compliant with the regulations of HIPAA and suitable for use by covered entities and their business associates.[125] Apps marked Confidential would guarantee that user data is not sold to or shared with third parties. Apps with no label will continue under the current notice and consent regulatory scheme.

A. "Confidential" Label Provides a Meaningful Consumer Choice

The current notice and consent framework of the FIPPs does not provide consumers with meaningful choices. Rather, an unregulated data market incentivizes companies to pursue a single business model: collect and sell as much data as possible.[126] As a result, there is little incentive to provide consumers with tools to restrict data collection. Industry representatives argue that ubiquitous collection actually provides a benefit to consumers, because the data market subsidizes the true cost of software and provides consumers with free services.[127] The premise of this argument is that personal data is a commodity and consumers are trading this commodity in exchange for digital services. If one accepts

[125] Letter from Tom Marino & Peter DeFazio, Members of Congress, (Sept. 18, 2014), *available at* http://actonline.org/wp-content/uploads/2014/09/Letter-to-Secretary-Burwell-September-18-2014.pdf [http://perma.cc/KN7R-9BC6] (Representatives Marino and DeFazio have already suggested a "voluntary badge program" to indicate HIPAA compliance).

[126] *Big Data Report, supra* note 111, at 54 (referring to this phenomena as a "digital land grab" that has resulted in "structural over-collection").

[127] GOV'T ACCOUNTABILITY OFFICE, *supra* note 7, at 40.

that personal data is a commodity, then the currencies of the data market become clear. Consumers that wish to have their personal data kept from third parties will have to pay the full cost of the software. Many consumers already believe that if they pay for the software they are using, then only the service provider will use their data,[128] but there is no guarantee that this is the case. In fact, paid mHealth apps have been found to collect and share data only marginally less than free apps. [129] The "Confidential" label would unambiguously provide that guarantee.

The current "notice and consent" system relies on contractual agreements. Consumers are responsible for reading, and accepting or denying, the terms of each service contract. The Confidential label is meant to simplify the most important privacy component of the contractual agreement - data sharing with third parties. It is intended to bind companies to certain terms. The essential terms of the Confidential label are: (1) Products with confidentiality labels cannot sell or share consumer data with third parties; (2) Products with confidentiality labels cannot revoke the label once it has been adopted;[130] (3) If a company offering products with a Confidential label goes bankrupt or is sold to a third party, it can only transmit consumer data to the new parent company and cannot sell data to additional third parties.[131] The Confidential label would serve as a condensed privacy policy that is actually intelligible, with terms enshrined in law and not up to the whims of changing contracts.

Creating such a label would standardize the terms of data use in the user and service provider relationship. Consumers interested in keeping their mHealth data from third parties would not have to wade through extensive privacy policies,

[128] INTERNATIONAL INSTITUTE OF COMMUNICATIONS, *supra* note 58, at 12.

[129] Craig Michael Lie Njie, *supra* note 48, at 15.

[130] This term aims at preventing mid-service changes in privacy policies, so that a service provider cannot simply reorder the terms of their agreement and have users unwittingly agree to retroactive third party access to data.

[131] Natasha Singer & Jeremy B. Merrill, *When a Company Is Put Up for Sale, in Many Cases, Your Personal Data Is, Too,* N. Y. TIMES, http://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html.

but instead could look for a product that is marked Confidential. For privacy conscious consumers, this label would provide a meaningful choice in a marketplace where currently the only choice is to broadcast health data or live without mHealth tools.

B. Voluntary Labeling

These labels should be adopted voluntarily by companies rather than mandated. It is unrealistic, and unwieldy to have an agency determine each and every app that needs to be labeled HIPAA Compliant or Confidential before the app goes to market. There are more than 100,000 apps in the mHealth market,[132] but only a fraction of this total enjoys a wide user base. Diverting agency resources to regulate unused or underused apps does not address the heart of the problem.

Mandating that mHealth developers not sell or share data would likely require most companies to restructure code–because data sharing is often automated–contracts, and business models. A number of stakeholders have voiced concerns to Congress and Federal agencies that costly economic impact will accompany mandatory regulatory compliance. [133] Allowing voluntary adoption rather than mandating increased privacy protections would still allow companies to provide free options to consumers while providing privacy conscious consumers with a meaningful choice. This would increase the range of products available to the consumer. Furthermore, voluntary adoption allows companies to decide whether their company is compliant with the label's standards before labeling their product.

Adopting a HIPAA Compliant label would not result in any increased regulatory burden to developers–those who are subject to HIPAA must be compliant whether they are labeled or not. The benefit of the label is that it would clarify product availability for covered entities and business associates. Adopting a Confidential label, however, would result in an increased regulatory burden, because the

[132] *Infra* Part I; Jen Miller, *The Future of mHealth Goes Well Beyond Fitness Apps*, CIO, (Dec. 4, 2014 4:09 AM PT) http://www.cio.com/article/2855047/healthcare/the-future-of-mhealth-goes-well-beyond-fitness-apps.html [http://perma.cc/KA3C-2Z2E].

[133] *See* INFORMATION RESELLERS, *supra* note 7, at 29-30, 33, 37, 42-43.

developer would voluntarily revoke the right to sell consumer data.

The benefit of doing so rests on the assumption that consumers value their privacy enough to pay a higher cost upfront to offset developers' loss in revenue from data sales. Personal data has been estimated to be worth as little as $0.0005 per person for general information, such as age, gender, and location, to $0.26 per person for medical information, such as listed conditions like arthritis, high blood pressure, and diabetes.[134] Developers could calculate the estimated value of the data they collect and charge this cost upfront. It is conceivable that the first Confidential products could be marketed for the highest price, while competition would, over time, drive down prices to the benefit of consumers.

C. Labels Create Legally Enforceable Standards

These labels could be achieved by amending two existing pieces of legislation. The HIPAA Compliance label could be added to the HIPAA Privacy Rule, and the Confidentiality label could be added to the Federal Trade Commission Act (FTC Act).[135] The Department of Health and Human Services enforces HIPAA through the Office for Civil Rights, while the FTC has carried out enforcement actions against non-HIPAA mHealth developers for unfair or deceptive practices related to privacy policies.[136] Similarly, the FTC

[134] Emily Steel et al., *How Much is Your Personal Data Worth?,* FINANCIAL TIMES, (Jun. 13, 2013, 8:11 PM), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html [http://perma.cc/4GC5-2VQG] (select "Family & Health" tab).

[135] The HIPAA Privacy Rule is codified at 45 CFR Parts 160 and 164, Subparts A and E; the FTC Act can be found at 15 U.S.C. §§ 41-58 (2016).

[136] U.S. DEP'T OF HEALTH AND HUMAN SERVICES, *HIPAA Enforcement*, *available at* http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/; Payments MD, LLC, No. C-4505, F.T.C. (Jan. 27, 2015); Payments MD, LLC, No. C-4505. 2015 FTC LEXIS 24 (F.T.C., Jan. 27, 2015); GMR Transcription Services, Inc., No. C-4482, F.T.C. (Aug. 14, 2014); GMR Transcription Services, Inc., No. C-4482, 2014 FTC LEXIS 199 (F.T.C., Aug. 14, 2014); Accretive Health Inc., No. C4432, (Feb. 5, 2014); Accretive Health Inc., No. C4432, 2014 FTC LEXIS 30 (F.T.C., Feb. 14, 2014).

has hosted industry workshops that urge mHealth companies to protect user data,[137] and is the agency charged with consumer protection.

1. Enforcement

Enforcement mechanisms are already part of HIPAA and the FTC Act.[138] The Health and Human Services' Office of Civil Rights (OCR) is charged with enforcement of the Privacy Rule.[139] In the FTC Act, the FTC is charged with enforcement of consumer protection.[140] By piggybacking off of these existing resources and procedures, the labels could be created and enforced at a relatively low cost.

2. Compliance

Companies that choose to adopt a Confidential or HIPAA Compliant label would be responsible for assessing the company's ability to comply. Once a company adopts a label, the OCR and FTC should monitor company actions and receive patient and consumer complaints reporting misuse of data.

3. Exceptions

In order for the Confidentiality label to be technically feasible, a few exceptions to the ban on sharing data would be necessary. mHealth developers must be able to contract for server storage and cloud services. Additionally, mHealth developers must be able to analyze user data in order to improve technical performance and offer new services to their customers. It is common to have third parties perform such analysis and provide developers with relevant findings.

[137] *See Spring Privacy Series: Consumer Generated and Controlled Health Data*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data [http://perma.cc/UVX2-ZU74].

[138] The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E; the FTC Act can be found at 15 U.S.C. §§ 41-58 (2016).

[139] U.S. DEP'T OF HEALTH AND HUMAN SERVICES, *supra* note 136.

[140] The FTC's enforcement powers are granted in 15 U.S.C. § 57b (2016).

Much like the "business associates" referred to in HIPAA, which are granted certain access rights to PHI, the business associates of mHealth developers should be granted the ability to access and analyze user data.

VI. CONCLUSION

While the FDA has taken a meaningful first step in regulating mobile medical devices through the FD&C Act, apps not currently covered by HIPAA are producing volumes of patient data. This user-generated data is being commoditized and sold, and consumers are often unaware of the ramifications. This problem is significant, as data produced by mHealth users can be even more revealing than the person's medical record. A voluntary labeling system should be put in place that would provide meaningful choices for consumers and protect their data. By focusing on HIPAA compliance and standardizing data confidentiality, this labeling system could demystify much of the confusion and ignorance that currently exists for companies and consumers alike. The time has come to address the unregulated data market that silently exists in the U.S. today.