2016

The Privacy Risks Surrounding Consumer Health and Fitness Apps, Associated Wearable Devices, and HIPAA's Limitations

Gabrielle Addonizio

The Privacy Risks Surrounding Consumer Health and Fitness Apps, Associated Wearable Devices, and HIPAA's Limitations

Gabrielle Addonizio

December 7, 2015

I. Introduction

Since the release of Apple's iPhone in 2007[1], the smartphone industry has been constantly changing. There is so much information and many new resources accessible at our fingertips by downloading mobile applications onto smartphones. A recent trend in the mobile world is the concept of Mobile Health or "mHealth". Mobile Health (mHealth) is the combination of healthcare services and the mobile industry that allows the consumer or patient be connected and interacting with data for health related purposes.[2] Through mobile technology applications, people are able to connect and send their healthcare information to their physicians, and potentially share their health information to others.[3]

The mHealth market proposes many concerns about the way patients' and consumers' health data is managed and stored, creating a big shift from the physician's office system to mobile apps and storage in the cloud. [4] Patients and consumers are becoming more involved in their own health care through mobile health and fitness apps and wearable devices. However, there are many privacy risks associated with this convenience. The user needs to be aware of the privacy risks surrounding mobile health and fitness apps along with associated wearable devices.

---

[1] Press Release, Apple, Apple Reinvents Phone with iPhone (Jan. 9, 2007), *available at* http://www.apple.com/pr/library/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.html

[2] Anne Marie Helm & Daniel Georgatos, *Privacy and MHealth: How Mobile Health "Apps" Fit Into Privacy Framework Not Limited to HIPAA,* 64 Syracuse L. Rev. 131, 132-133, (2014) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2465131.

[3] *Id*.

[4] Dongjing He, Muhammad Naveed, Carl A. Gunter & Klara Nahrstedt, *Security Concerns in Android mHealth Apps*, Dep't. of Computer Sci., Univ. of Ill. 645 (2014).

Privacy law applicable to mHealth is often seen as whether HIPAA protects and applies to the application. Unfortunately, HIPAA does not protect everything healthcare related. On the big scale, the federal government does not regulate mobile health applications. [5] With the technology changing rapidly, privacy and security risks are going to get more complex. The privacy data protection needs to begin with the mobile app developers through self-regulation. The developers and companies need to have an understanding of what HIPAA protects in order for the mobile app and wearable devices data to be HIPAA complaint.

This paper will discuss the privacy risks associated with mobile health and fitness apps and their corresponding consumer wearable devices, such as FitBit and Apple Watch. The privacy risks include, but are not limited to, the collection of information without user's consent, sending private health information to advertisers and data brokers, undeveloped and nontransparent privacy policies, and private information being sent via unencrypted networks. Part II of this paper provides an overview of mobile health apps and consumer wearable devices, and how the user's private information is being used and where it is being sent. Part III explains some privacy faults found in mobile health and fitness apps as well as consumer wearable devices, including the inadequate privacy policies that are currently available. Part IV analyzes the scope of HIPAA and whether it serves as a source of privacy protection in the mHealth industry.

Part V considers the Federal Trade Commission ("FTC") and its role in mHealth regulation as a basis for consumer protection. Part VI suggests that mobile app developers and consumer wearable device designers focus on consumer privacy from the developmental stage. This could happen through implementing encrypted networks, possibly avoiding advertising and analytical

[5] Daniel F. Schulke, Note, *The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing*, 93 B.U.L. Rev. 1699, 1700-1701 (2013).

services, and drafting clear and understandable privacy policies. Part VII concludes by saying that mobile health and fitness apps along with consumer wearable devices provide great benefit to the consumer. However, protecting the user's private information needs to be a priority and the entities collecting this information should to engage in self-regulation.

II. Mobile Health Apps and Consumer Wearable Devices

As smartphones become increasingly prevalent in society, so have a variety of applications that provide a wide array of services. A mobile app is purchased or downloaded through online stores, such as the App Store for iPhone or the Google Play Android Store. [6] Mobile health apps, whether consumer or physician focused, have made dramatic changes within the healthcare industry.[7] For example, physicians have found the mobile health apps to be very useful in increasing the access to healthcare and easing the communication between patient and medical provider. [8] The consumer-focused apps also are also beneficial by providing resources for a healthy lifestyle.

According to Digitaltends.com, there are 100,000 apps dedicated to mobile health for Android and iOS (iPhone) operating systems, which doubled over the last two years.[9] The most popular health related apps for the consumer are the health and fitness apps. For purposes of this paper, the analysis will be on privacy risks associated with mobile health apps connected to the

---

[6] *Mobile Health and Fitness Apps: What Are The Privacy Risks?*, PRIVACY RIGHTS CLEARINGHOUSE (July 15, 2013), https://www.privacyrights.org/print/mobile-health-and-fitness-apps-what-are-privacy-risks.

[7] Peter McLaughlin & Melissa Crespo, *The Proliferation of Mobile Devices and Apps for Health Care: Promises and Risks*, BLOOMBERG BNA (May 21, 2013), http://www.bna.com/the-proliferation-of-mobile-devices-and-apps-for-health-care-promises-and-risks/.

[8] Robyn Wittaker, *Issues in mHealth: Findings from Key Informant Interviews*, J. MED. INTERNET RES. (Oct. 2, 2012), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3510768/.

[9] Alex Boxall, *2014 Is The Year Of Health And Fitness Apps, Says Google*, DIGITAL TRENDS (Dec. 11, 2014), http://www.digitaltrends.com/mobile/google-play-store-2014-most-downloaded-apps

smartphone and wearable devices. These mobile health apps referenced are consumer apps, not provider apps. Consumer health apps are those that are marketed by the developers, not a healthcare provider or covered entity, directly to the consumer for the consumer's own personal use. [10] Provider apps include reference apps from medical textbooks and journals, clinical decision support tools that allow providers to check a patient's diagnosis based on symptoms, access to electronic medical records, and apps that allow the conversion of a smartphone into a medical device for diagnosis and treatment. [11] Some examples of provider apps are Medscape[12], which offers health care providers access to medical and educational information; Isabel[13], which helps diagnose patient illnesses based on symptoms; Epocrates[14], which provides doctors with drug information, calculate patient measurements, and look up other providers for referrals.

In general, consumer apps are for those who want to personally track and/or analyze their health and exercise routines. [15] More specifically, they include, but are not limited to, diet and exercise programs, symptoms checkers, health and lifestyle magazine subscriptions, and sleep trackers. [16] For example, MyFitnessPal is used for health and fitness tracking to help keep count calories and diary overall healthy eating.[17] MapMyRun uses the phone's GPS to track the duration, distance, speed, calories burned and route traveled for physical activity. [18]Also, WebMD mobile

---

[10] Srishti Miglani, *Caveat Emptor: Use of Mobile Health Applications and Information Confidentiality*, 11 A.B.A. HEALTH LAW 2 (2015) *available at* http://www.americanbar.org/publications/aba_health_esource/2014-2015/october/caveat.html
[11] *See* Helm, *supra* note 2.
[12] JP Medved, *Top 7 Medical Apps for Doctors*, CAPTERRA MEDICAL SOFTWARE BLOG, April 24, 2015, http://blog.capterra.com/top-7-medical-apps-for-doctors/
[13] *Id*.
[14] *Id*.
[15] *See* PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 6.
[16] *Id.*
[17] https://www.myfitnesspal.com/
[18] http://www.mapmyrun.com/

app is similar to the website where medical, disease, and symptom research can be found. [19]These apps are not intended for physicians' use, medical treatment or diagnosis. Many of these consumer apps have the option to be connected to the consumer's social network profile, whereby users can share their information on social networks like Facebook. [20]

The personal and health information obtained in these apps varies depending on the apps purpose. Many of these apps require the basic personal information- name, email, age, gender, height, and weight- to create an account or profile.[21] While it is not as personal, some apps may ask about the lifestyle and exercise habits of the consumer. The diet and exercise apps include counting calories based on the information provided by the consumer, mapping runs through the GPS on the phone, and connecting others through the social networks. [22]

Smartphones are not the only "device" that can collect consumers' health data. Wearable devices, such as the FitBit and the Apple Watch are other ways this information can be gathered. These wearable devices are traditionally worn on the wrist and can monitor the user's heart rate, stress level, body temperature, sleep patterns and other sensitive health information. [23] Corresponding mobile apps can be downloaded to the smartphone and can store this health information. [24] This stored health information is monitored and collected in real time. For example, the FitBit can be worn while doing basically anything and the mobile app can be opened at any

---

[19] http://www.webmd.com/mobile
[20] *See* Helm, *supra* note 2, at 138.
[21] Ann Carrns, *Free Apps For Nearly Every Health Problem, but What About Privacy?*, N.Y. TIMES, Sept. 11, 2013, http://www.nytimes.com/2013/09/12/your-money/free-apps-for-nearly-every-health-problem-but-what-about-privacy.html.
[22] *Id.*
[23] Matthew R. Langley, *Hide Your Health; Addressing The New Privacy Problem of Consumer Wearables*, 103 GEO. L.J 1641, 1642 (Aug. 2015).
[24] Morgan Brown, *What's Next for Wearable Technology and What It Means for Health Data,* TRUE VAULT (July 28, 2014), https://www.truevault.com/blog/whats-next-wearable-tech-health-data.html.

time to check on the health statistics- steps taken, distance traveled, calories burned- it has collected up to that point. [25] The Apple Watch monitors the users' heart rate and daily activities constantly through out the day ranging from the amount of hours the user sits throughout the day to recording a workout. [26] The convenience of wearable devices, such as fitness trackers, coupled with the health apps allow users to track their daily health and fitness activities but not without privacy concerns.

A. How The Private Information Used and Where Does It Go?

Both Apple and Google have publically acknowledged the importance of the smartphone users' privacy, and protect its users by requiring the apps to get the user's permission before using certain information, such as location. [27] Although it is unknown how Apple enforces or interprets its policy, Apple says the iPhone Apps "cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." [28]

It is becoming more apparent that mobile apps usually take the consumers' private information and data without the consumers' permission. For example, app developers are able to take the consumers' mobile address book at will, usually without the consumers' knowledge. [29] When the user allows the app to see or use their current location for GPS purposes, the apps do

---

[25] David Pogue, *Wearable Devices Nudge You To Health*, N.Y. Times, June 26, 2013, http://www.nytimes.com/2013/06/27/technology/personaltech/wearable-devices-nudge-you-to-a-healthier-lifestyle.html?_r=0.
[26] APPLE WATCH, http://www.apple.com/watch/health-and-fitness/.
[27] Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J., Dec. 18, 2010, http://www.wsj.com/articles/SB10001424052748704368004576027751867039730.
[28] *Id*.
[29] Nicole Perlroth & Nick Bilton, *Mobile Apps Take Data Without Permission*, N.Y. TIMES BITS BLOG, Feb. 15, 2012, http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/?_r=0 .

not generally disclose to the user that this information will be sent to advertising companies. [30] Many app users do not know where the information is going or how the developer plans on using it.

Both iPhone and Android smart phones have an unique tracking identifying number. [31] According to Wall Street Journal study, the most common unique ID found was Apple's iPhone identifier, the UDID. [32] The apps that were tested in this study did not tell the users that the UDID was being requested, but Apple has explained to its app developers that the UDID is sensitive if it is associated with the user's other data. [33] The next common identifier was found on Android's operating system. [34] Android ID differs from Apple's UDID because the user is able to reset their Android ID if they do a "factory reset" on the phone to delete the phone's data and its settings. [35] Google does not consider their smartphone IDs to be identifying information. [36]

Megan O'Hollaran of Traffic Marketplace says the UDID is how the ad networks track everything the smartphone user is doing with the app. [37] Apple treats the iPhone's UDID as "personally identifiable information" because it can be connected to the user's personal information, such as name or e-mail address, yet the ad networks insist that the data is not linked to the individual. [38] There are serious privacy risk tied to UDID numbers, as they are extremely difficult or impossible to delete and can be tied to the user's other private information. [39] There are

---

[30] *See* Thurm, *supra* note 27.
[31] Jennifer Valentino-DeVries, *Unique Phone ID Numbers Explained*, WALL ST. J., Dec. 19, 2010, http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained/
[32] *Id*.
[33] *Id*.
[34] *Id*.
[35] *Id*.
[36] *Id*.
[37] *See* Thurm, *supra* note 27.
[38] *Id*.
[39] *See* Valentino-DeVries, *supra* note 31.

not many options for the user to opt out of the smartphone tracking, unlike regular computers where it is possible to delete or block the "cookies". [40]

The tracking companies often use these high-risk unique ID numbers for marketing and advertising purposes. For example, a company called Mobclix gathers this tracking and ID data, creates a profile for the smartphone user, matches the data with spending and demographic data provided by a market research company and offers these profiles to advertisers. [41] Another example is Google's advertiser network, AdMob, helps advertisers target certain smartphone users by location, type of device used, and demographic data, such as gender and age. [42] According to a study released by the FTC, twelve different health and fitness apps transmitted user data to 76 different third parties, including advertisers. [43] The data transmitted ranged from device information to exercise and dietary habits, and some sent names and addresses. [44] Smartphone apps, in particular health and fitness related apps, have the ability to access an abundant amount of users' personal data creating an increase in privacy risks and concerns.

Furthermore, there are greater threats to consumers' privacy coming from data brokers. [45] Data brokers collect, analyze, and compile personal information from the Internet and mobile devices and sell it to other data brokers, advertisers, and sometimes the government, without consumers' knowledge or approval. [46] In a CBS News 60 Minutes interview with the Federal

---

[40] *Id*.
[41] See Thurm, *supra* note 27.
[42] *Id*.
[43] FED. TRADE COMM'N, *Spring Privacy Series: Consumer Generated and Controlled Health Data*, May 7, 2014, https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf.
[44] *Id*.
[45] *The Data Brokers: Selling Your Personal Information* (CBS News broadcast Mar. 9, 2014), *available at* http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/
[46] *Id*.

Trade Commissioner Julie Brill, she said, "most people have no idea that [information is] being collected and sold and that it is personally identifiable about them, and that the information is basically a profile of them." [47] It is important for consumers to be aware of the personal information being loaded onto mobile apps and collected by associated consumer wearable devices.

III. The Privacy Problems: Mobile Health Apps and Wearable Devices

A. Privacy Faults in Mobile Health Apps

The mHealth apps require consumer data to provide the results the consumer is seeking. The consumer needs to be aware of the increasing privacy risks with mobile technology constantly changing. First, the apps allow a much larger and longer lasting collection of this data from the consumer. [48] Second, it is not only the information the consumer puts into the app that is being collected; there is a much broader range of data being collected that the consumer might not be aware of, such as lifestyle activities, location tracking, social network connections, etc. [49] Third, through the consumer health apps communications platform or a social network connection, the exposure to privacy attacks increases. [50] Once this information is public, consumers typically have minimal control over it.

Consumers cannot assume that the information they put into the app is private and protected. According to the Privacy Rights Clearinghouse, of the 43 popular health and wellness apps analyzed, all presented some risk to the consumer. [51] From the same analysis, there were three

---

[47] *Id*.
[48] Dongjin He, Muhammad Naveed, Carl A. Gunter & Klara Nahrstedt, *Security Concerns in Android mHealth Apps*, Dep't. of Computer Sci., Univ. of Ill. 645 (2014).
[49] *Id*.
[50] *Id*.
[51] *See* PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 6.

main causes of informational privacy risks in the mobile health and fitness apps. Insecure network communications, advertising, and third party analytics were the greatest to least risky, respectively. [52]

Many of the health and fitness apps have unencrypted network connections for the transmission of the personal information. For those that are scanning the network for data, this information is clear and viewable to anyone. [53] They are constantly collecting new information about the consumer because of the nature of mobile apps downloaded onto a mobile device and it being connected to the Internet even when the consumer is not using the app. [54]

The mobile apps that are downloaded for free rely on advertising for revenue while the paid apps usually depend on the purchase price of the app for its revenue. [55] The free apps may share personally identifiable information with the advertising companies, or allow the ad companies to track the consumer unbeknownst to them. Similarly, the mobile apps can send non-personal information to the data analytics companies over a non-secured network connection and could potentially be collected in a database that connects the usage of other apps using the same analytics company. [56]

B. Privacy Faults in Wearable Devices

Consumer wearable devices, such as FitBit the Apple Watch, also have privacy risks. Wearables paired with their health apps collect users' personal sensitive information on a more

[52] *See* PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 6.
[53] *Id*.
[54] Larry Alton, *How Wearable Tech Could Spark a New Privacy Revolution*, TECHCRUNCH (Sept. 12, 2015, 9:49 PM), http://techcrunch.com/2015/09/12/how-wearable-tech-could-spark-a-new-privacy-revolution/.
[55] *See* PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 6.
[56] *Id*.

detailed level.[57] These wearable devices are connected via Bluetooth to a mobile app that provides the consumer with the data it has collected. The wearable devices collect the data and wirelessly sends the data to the mobile app. [58] That data can now be sent to the cloud for storage and/or analysis. [59]

Ruby Zefo, Chief Privacy and Security Counsel for Intel, says "… data from wearable devices can be used for the common good, such as disease prevention... However, each of these benefits carries risk." [60] Not only do the wearable devices have the mobile app privacy risks linked to them, they also have their own privacy risks. These privacy risks include identity theft, stalking and tracking, robbery, profiling and discrimination. [61] Wearable devices have similar, if not the same, location tracking abilities as the mobile apps do.

More often than not, the wearable devices are set in a "public" default privacy setting, which means that the profile the consumer created is possibly searchable on the Internet. [62] Specifically for the Apple Watch, when the user is wearing the watch, real time data is being collected and sent to the health app for storage and analysis. This real time data is sensitive

---

[57] Avi Goldfarb & Catherine Tucker, *Privacy and Innovation*, NAT'L BUREAU OF ECON. RESEARCH, Working Paper No. 17124, (June 2011), *available at* http://www.nber.org/papers/w17124.pdf.

[58] Ruby A. Zefo, *Wearable Devices: Keep Data Privacy in Check*, INFORMATIONWEEK, (Aug. 18, 2014), http://www.informationweek.com/mobile/mobile-devices/wearable-devices-keep-data-privacy-in-check/a/d-id/1298085.

[59] *Id*.

[60] *Id*.

[61] Jen Legnitto, *Why You Should Worry About Wearable Tech and Wireless Security*, PRIVATE WIFI BLOG, (May 30, 2014, 9:36 PM), http://blog.privatewifi.com/fitness-band-woes-why-you-should-worry-about-wearable-tech-and-wireless-security/; *See* Zefo, *supra* note 58.

[62] Kenneth Corbin, *What Happens With Data from Mobile Health Apps?*, CIO (Mar. 30, 2015, 10:11 PM), http://www.cio.com/article/2903573/healthcare/what-happens-with-data-from-mobile-health-apps.html.

information about the user that the health-app company is able to sell to third parties. [63] There are serious privacy implications from companies collecting sensitive health information, usually without the users' knowledge or permission.

C. Inadequate Privacy Policies

Generally, mobile health applications are largely unregulated to protect consumers' privacy rights. The privacy protections are limited to whatever protection the developer privacy policy entails. [64] Based on a study done in August 2014, out of the 600 most commonly used mHealth apps, only 30.5% had privacy policies. [65] The apps that did have privacy policies available did not make it clear to users, required an upper-level literacy, and did not focus on the app itself. [66] These mobile apps are still being purchased [and downloaded] successfully despite the unclear, irrelevant, or nonexistent privacy policy.[67] It is highly encouraged for consumers to read the privacy policy before using the app. The privacy policy should describe the app's information sharing policies and describe potential risks, but some do not. [68] The privacy policies often are established to protect the developer from lawsuit, not to protect the consumer's privacy. [69]

IV. HIPAA and Mobile Health Privacy

---

[63] FED. TRADE COMM'N, *Mobile Privacy Disclosures: Building Trust Through Transparency*, Staff Report, (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.
[64] *See* PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 6.
[65] Ali Sunyaev, Tobias Dehling, Patrick Taylor & Kenneth Mandl, *Availability and Quality of Mobile Health App Privacy Policies*, Journal of the Am. Med. Informatics Ass'n (2014) https://www.researchgate.net/publication/264942197_Availability_and_Quality_of_Mobile_Health_App_Privacy_Policies.
[66] *Id*.
[67] *Id*.
[68] *See* Carrns, *supra* note 21.
[69] *Id*.

There is a parallelism between the growth of mobile health technology and arising privacy issues and concerns. There is not much protection being offered by Federal Agencies. Many consumers believe that because these mobile health apps collect health information, the information is protected by HIPAA. Unfortunately, HIPAA has a limited scope of protection and technology is moving too quickly for HIPAA or any other Federal Agency to keep up.

A. HIPAA and The Privacy Rule

In 1996, HIPAA was passed to address the problem of protecting patient privacy.[70] HIPAA is only concerned with an individual's "protected health information" or "PHI". [71] This information is an individual's identifiable health information that is held and used by a covered entity or its business associate and transmitted electronically, on paper, or orally. [72] An individual's identifiable health information includes demographic information, such as name, address, birth date, and social security number, related to the individual's physical or mental health, health care services provided to the individual, or payment for such services. [73]

HIPAA's Privacy Rule protects the use and disclosure of individuals' health information ("protected health information" or "PHI") by covered entities along with holding the standards for the use and control of individuals' PHI. [74] The Privacy Rule attempts to create the balance between the necessary free flow of information for patient care and every individual's right to privacy and

[70] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVICES AND OFFICE FOR CIVIL RIGHTS, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last updated 2003).
[71] 45 C.F.R § 160.103
[72] *Id*.
[73] *Id*.
[74] *See Summary of the HIPAA Privacy Rule, supra* note 70, at 1.

security.[75] It only applies to HIPAA covered entities and their business associates.[76] To meet HIPAA's requirements, PHI needs to be communicated between covered entities and its' business associates. [77]

B. Covered Entities and Business Associates

Covered entities include health plans (such as individual and employer group plans that pay for the cost of medical services), health care providers who transmit health information electronically, and health care clearing houses (entities that process health care claims into standard format). [78] Mostly, health care clearing houses will receive PHI when providing processing services for health care providers or to health plan as business associates. [79] Generally, covered entities are permitted to use or disclose PHI to the individual, for treatment, payment or health care operations.[80] Covered entities must reasonably limit their use, disclosure, or request of PHI from another covered entity or business associate to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request." [81] Furthermore, a covered entity may not use or disclose PHI except "when the individual who is subject of the information authorizes in writing." [82]

A business associate is a person or organization that handles the PHI on behalf of the covered entity for functions such as claims processing, data analysis, billing, and other

[75] Barbara Fox, *Mobile Medical Apps: Where Health and Internet Privacy Law Meet*, 14 HOUS. J. HEALTH L. & POL'Y 193, at *213-214, (2014).
[76] *See Summary of the HIPAA Privacy Rule, supra* note 70, at 1.
[77] 45 C.F.R § 160.103.
[78] 45 C.F.R § 160.103.
[79] *See Summary of the HIPAA Privacy Rule, supra* note 70, at 3.
[80] 45 C.F.R § 160.502(a)(1).
[81] 45 C.F.R § 160.502(b).
[82] 45 C.F.R § 164.502(a).

administrative activities. [83] A business associate is a person who is not an employee of a covered entity. [84]Covered entities may disclose PHI to a business associate only if it helps the covered entity carry out its health care services. [85]

When a covered entity uses a business associate, there needs to be a contract in place to establish the permitted and required uses and disclosures of PHI by the business associate authorized under HIPAA, use of safeguards, reporting of uses and disclosures not according to the agreement, and breach notification procedures, along with other elements. [86] In particular, the Business Associate Agreement should clearly explain how the business associate will report and respond to data breaches, including those done by a business associates' subcontractor, as well as how the business associate responds to a compliance investigation. [87] Under a Business Associate Agreement, a covered entity needs to get satisfactory assurances to give business associates only PHI for the covered entity's purpose, or business associate administrative needs. [88] Business associates also need to get satisfactory assurances in writing from any sub-contractors they may use. [89] Business associates work on behalf of the covered entities; therefore, if the app developer or wearable device designer is not classified as a covered entity, the health data that is being analyzed is likely not done by a business associate and not protected by HIPAA.

C. mHealth and HIPAA

---

[83] 45 C.F.R § 160.103.
[84] *Id*.
[85] *Understanding HIPAA Privacy: Business Associates*, U.S. DEP'T OF HEALTH AND HUMAN SERVICES, (last updated 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html
[86] 45 C.F.R § 164. 504(e)(2).
[87] *Understanding HIPAA Privacy: Business Associate Contracts*, U.S. DEP'T OF HEALTH AND HUMAN SERVICES, (last updated 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
[88] 45 C.F.R § 164.502(a).
[89] 45 C.F.R § 164. 504(e)(2).

In determining whether the mobile health app falls under HIPAA protection, a developer needs to figure out (1) who will be using the application (the audience) and (2) what information will be on the application. [90] For example, if physicians will use the application to follow up with patients and discuss medical treatment, the app needs to be designed to comply with HIPAA because a covered entity is involved. [91] However, health and fitness application, such as an exercise tracker or a food diary, do not need to be HIPAA compliant because no covered entity or business associate is involved.[92] Despite the lack of privacy policies available for these mobile apps, there is high possibility that consumers are putting their confidence in the legal system assuming that their privacy is protected and only focusing on the short term personal benefit of the mobile app without considering the privacy risks they are compromising. [93]

While the consumer may be putting in his or her identifiable personal health information, such as their name, address, date of birth, into the application to create a profile or to simply start using the app, the application on the smart phone or the developers' locally or externally data storage locations are considered covered entities or business associates that are covered under HIPAA. HIPAA only applies to covered entities and their business associates, not health care consumers or technology engineers who could be developing these apps and wearable devices. [94] App developers and wearable device designers are not covered entities or business associates under HIPAA because they are likely not health care providers, health plans, or health care clearing houses. Furthermore, it is difficult for HIPAA to protect the mobile health and fitness app

[90] Adam H. Greene, *When HIPAA Applies to Mobile Applications*, MOBIHEALTHNEWS, (June 16, 2011), http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/.
[91] *Id*.
[92] *Id*.
[93] *See* Sunyaev, *supra* note 65.
[94] *See* Greene, *supra* note 90.

information because the information that is collected is not used directly for treatment. [95] These apps are collecting information the consumer voluntarily puts in as well as information in the background, such as location, while the phone is powered on.

The space between the consumer's personal information and protection of such information is where the privacy risks lie. For example, a consumer, a health care provider, and possibly other entities can use the Apple Watch and its associated HealthKit Platform to log and store the user's physical activity and health data. [96] The Apple Watch can monitor a person's daily activity, provide incentives or suggestions to increase such activity, monitor heart rate, calculate calories burned, and track distance traveled. [97] Many third party developers have designed health care apps can be utilized on the Apple Watch along with Apple's HealthKit platform. Healthcare providers may also have an opportunity to use the Apple Watch and its apps but there still may be much vulnerability surrounding data protection. There are several privacy and security concerns that exist, including the tracking and storage of the healthcare information, the transfer of healthcare information from user to healthcare provider and other third parties, and the variety of privacy policies that exists among the third party app developers. [98]

HIPAA's applicability to the Apple Watch and its apps is unclear because one of the major privacy concerns is that HIPAA does not protect the data that is stored on the consumers' devices.[99] For HIPAA to protect said data, the data would need to be PHI and used, transmitted, maintained,

---

[95] *See* Fox, *supra* note 75.
[96] Paul A. Drey, Sarah Wendler, & Patrick Gentry, *Peeling Back the Apple Watch: Do HIPAA and the Apple Watch Go Together?*, 12 A.B.A HEALTH LAW 1 (2015) *available at* http://www.americanbar.org/publications/aba_health_esource/2015-2016/september/applewatch.html
[97] *Id*.
[98] *Id*.
[99] *See* Greene, *supra* note 90.

stored, and in the control of a covered entity or business associate. [100] For example, when a user transmits his or her health data from the Apple Watch to the Mayo Clinic App [101], the health data becomes PHI and is protected once the Mayo Clinic has received it because the Mayo Clinic is a covered entity under HIPAA. [102]

Other vendors that store, use, or transmit the health data from the Apple Watch may be considered business associates of the covered entities. These entities should be considered business associates if "they create, receive, maintain, or transmit protected health information on behalf of a covered entity." [103] If the app transmits data to a covered entity, the covered entity then provides the same data to a vendor to be analyzed, that vendor is likely a business associate and protected under HIPAA. If this is how the data is going to flow, the covered entities need to establish a Business Associates Agreement with each of the third parties. This could lead to more data breaches if these agreements are not in place with all of the potential third parties that could get this data.

HIPAA does not protect the health and fitness apps used by consumers because the data is not being purposely transmitted and used by covered entities or business associates. Apple's HealthKit platform provides a privacy framework for the user to be in control of the information that is being released to the specific app but there is still uncertainty as to what the app does once it obtains the data. [104] Due to HIPAA's limited scope and only protecting PHI from covered

---

[100] *See* Drey, *supra* note 96.
[101] Brian Kilen, *Mayo Clinic Announces Apple Watch App For Patients and Physicians*, MAYO CLINIC NEWS NETWORK, Apr. 24, 2015, http://newsnetwork.mayoclinic.org/discussion/mayo-clinic-announces-apple-watch-app-for-patients-and-physicians/
[102] *See* Drey, *supra* note 96.
[103] *Id*.
[104] *The Healthkit Framework*, APPLE, INC., https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/

entities, the Federal Trade Commission has been involved in the attempting to regulate mobile health apps and consumers' health data protection.

V. The Federal Trade Commission's Consumer Protection

Consumer protection laws are another means of enforcing privacy protections. Consumer protection agencies, such as the Federal Trade Commission ("FTC"), have attempted to fill this mobile health app privacy gap.[105] The FTC through its broad consumer protection authority has been promoting privacy of mobile apps. [106] The FTC gets its' power to oversee mHealth apps from the FTC Act. [107] The FTC Act prevents persons or entities "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." [108] This includes acts or practices in mobile commerce, including the mHealth apps.

The FTC brings enforcement actions against companies that work in the mobile app industry. [109] These enforcement cases are against the app developers who have secretly accessed the consumers' information on their devices for their "unfair and deceptive" practices. [110] More specifically, the FTC sued a social networking app developer for collecting and storing the user's information from the mobile device regardless of whether the user gave consent. [111] Another enforcement example was FTC's first consumer protection case in mHealth industry for deceptive practices, not violations of consumer privacy. The FTC took action against app developers who

---

[105] Hank Creasy & David Knoespel, *The New Generation of Electronic Health Records: What Health Apps Know About You*, 64 VIRGINIA LAWYER, (June 2015), http://www.ewlaw.com/images/PDF_Articles/The_New_Generation_of_Electronic_Health_Records-_What_Health_Apps_Know_About_You.pdf
[106] *See* Helm, *supra* note 2, at 158.
[107] 15 U.S.C. §§ 41-56.
[108] 15 U.S.C. § 45 (a)(2)
[109] *See* FED. TRADE COMM'N, *supra* note 63.
[110] *See* Helm, *supra* note 2, at 160.
[111] *Id*.

said their apps, AcneApp and Acne Power, could treat acne but there was no competent and reliable evidence to support the claims. [112]

As for the consumers' protected health information and health privacy, FTC brought an action of "unfair act or practice" under the FTC Act against LabMD for its insufficient security measures protecting the patients' lab results. [113] While the FTC has not expressly enforced cases against a health or fitness app developer for deceptive or unfair acts or practices, it seems that it would be possible due to the broad scope of its prosecution powers. The FTC has suggested for the app developers to prioritize and focus on the mobile privacy disclosures to ensure compliance and prevent a lawsuit.

The FTC has another means of enforcement authority is through the FTC Health Breach Notification Rule ("FTC Rule") created by the American Recovery and Reinvestment Act of 2009. [114] The FTC Rule applies to a vendor of personal health records ("PHR"), a PHR- related entity, such as a business that interacts with a vendor of personal health records, and a third party service provider who are businesses that offer services for maintenance, disposal, use of health information to vendors. [115] The FTC Rule requires notice provided to the consumer and FTC when there has been "an unauthorized acquisition of the PHR identifiable health information that is unsecured and in a personal health record." [116] The FTC Rule does not prevent the sale of personal health data

[112] *Id*. at 162.
[113] *Id*.
[114] FED. TRADE COMM'N, *Complying With The FTC's Health Breach Notification Rule*, (April 2010), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule
[115] *Id*.
[116] *Id*.

nor does it require health apps to get consent from consumers for uses and disclosure of information. [117] There are some gaps in this FTC Rule that does not address some privacy issues.

The FTC has taken steps to educate the businesses and consumers on privacy concerns surrounding the mobile device industry. In March 2012, the FTC issued its Privacy Report, which sets forth the best business practices to protect consumers' privacy and control over personal data. [118] The Privacy Report requires companies, including mobile companies, who are involved with consumer personal data to observe three main principles: Privacy by Design, Simplified Consumer Choice, and Greater Transparency. [119] This means that the data collected should be limited to only that is necessary to run the app and perform the service requested, and companies should develop a standard language for the privacy policies that are particular to their industry, understandable, and accessible to the consumer on a mobile device. [120]

In February 2013, the FTC released a report, "Mobile Privacy Disclosures: Building Trust Through Transparency," that outlined privacy practice recommendations to app developers and consumers. [121] In April 2013, the FTC released another business guide, " Marketing Your Mobile App: Get It Right from the Start," that discusses truth in advertising and respect for user privacy. [122] As for truthful advertising, if there are objective claims about the app, there needs to be competent and reliable evidence that supports the claims before launching it. [123] Furthermore, any

---

[117] *Id*.
[118] FED. TRADE COMM'N, Pr*otecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers* (Mar. 2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[119] *Id*.
[120] *Id*.
[121] *See* FED. TRADE COMM'N, *supra* note 63.
[122] FED. TRADE COMM'N, *Marketing Your Mobile App: Get It Right From the Start*, (April 2013), https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf.
[123] *Id*.

disclosures that are made need to be clear and conspicuous, meaning the disclosure needs to be visible enough and understandable to the consumer. [124]

The FTC will likely pay close attention to the privacy procedures and policies implemented by these app developers and wearable device designers to ensure consumer protection. Even though the FTC has authority to penalize entities for deceptive or unfair conduct to consumers, there are still concerns about the lack of security on the consumer-generated health data that is stored on consumers' personal devices.

VI. Mobile App Developers Need to Prioritize Consumer Privacy

The conveniences of having consumer wearables and the corresponding health and fitness apps help improve the consumer's health and fitness habits. However, privacy is not the wearable designers and app developers priority. App developers need to care about privacy for several reasons. It is important to be proactive in protecting privacy from the start of the app, not once all of the information has been collected. To avoid any unnecessary headaches, the app developer should not collect privacy sensitive information if it is not necessary for the app to function.[125] If that privacy sensitive information is necessary, the data stored or transmitted needs to be encrypted. [126] Furthermore, once the database collects this private information, it is difficult to delete. Should that information become public, measures need to be taken to fix the problem so it is better to have a secure app embedded in the design. [127]

A. Risks Related To The Collection and Usage of Mobile Health and Fitness Apps Data

---

[124] *Id*.
[125] Craig Michael Lie Njie, *Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications*, PRIVACY RIGHTS CLEARINGHOUSE (August 12, 2013), https://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.
[126] *Id*.
[127] *Id*.

According to Privacy Rights Clearinghouse's (PRC's) research of Mobile Health and Fitness Apps Data practices, there are several risks associated with the collection, storage, transmission and usage of such data. [128] As previously stated and based on PRC's research, there are some apps that send data without the user' knowledge, some apps that connect to third party sites without the user's knowledge, and these connections can be unencrypted, exposing sensitive health data to everyone on a network.[129]

There are two types of data collection that apps can use. The first type is an explicit collection, where the app asks the user for information and the user can control the amount and type of information they provide.[130] These are often done through questionnaires or if the app requires an account to be created. [131] The second type is implicit data collection, where most users are not aware or have knowledge of how the app developers or third parties are using the data. [132] According to PRC's research, "almost half of the free mobile health and fitness apps we researched use some kind of third-party advertising…" [133] Of these apps, some send data to as many as 10 or more different advertisers within the first few minutes the app is being used, and none of these apps are sending the data over an encrypted network. [134]

B. The Difficulties App Developers and Wearable Device Designers Face To Be HIPAA Compliant

There are implications under HIPAA for app developers. An app developer needs to determine whether HIPAA will apply to how the app will be used and what type of information

[128] *Id*. at 14.
[129] *Id*.
[130] *Id*. at 15.
[131] *Id*.
[132] *Id*.
[133] *Id*.
[134] *Id*. at 15-16.

will be stored. [135] First, if the app has any chance to interact with a covered entity or use, store, or transmit PHI, the app developer needs to ensure the app is HIPAA compliant to avoid a violation of the HIPAA guidelines. [136]

Next, the app developer needs to be aware of protecting the PHI all the time. Whether the app communications include or might include PHI, the communications need to be sent via a HIPAA compliant server. [137] Also, the apps database needs to be encrypted, and in order to access this encrypted database, the app needs to be HIPAA compliant or else the app's functionality will be restricted. [138] Similar to the external communications, the mobile push notifications cannot include any PHI because there is an increased risk of that being accessed by the public. [139]

However, it is possible to go from being non-HIPAA compliant to HIPAA compliant if the right steps are taken. FitBit recently announced that it is now HIPAA compliant and can integrate with HIPAA covered entities, including the corporate wellness partners. [140] The FitBit Wellness program is the company's business to business offering that provides organizations with effective wellness programs. [141] Now being HIPAA compliant, the FitBit Wellness program can support HIPAA-covered entities that are seeking to improve the health and wellness of its members, such

---

[135] *See* McLaughlin, *supra* note 7.
[136] *Id*.
[137] *Id*.
[138] *Id*.
[139] *Id*.
[140] Press Release, FitBit, Fitbit Extends Corporate Wellness Offering with HIPAA Compliant Capabilities, (Sept. 16, 2015), *available at* https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx
[141] *Id*.

as Target Corp. [142] Also, the FitBit Wellness program will now allow health plans and self-insured employers enter into Business Associate Agreements with covered entities. [143]

C. Use Encrypted Networks and Secured Software

Many apps send private sensitive information over unencrypted networks. [144] Developers need to make sure that all networks transmitting communications are encrypted. This means they always need to use a HTTPS network, never a HTTP network to send data from the app to the server on the Internet. [145] As for wearable devices, the design, deployment, and management all need to be established using secured software. [146] In the design phase, wearable devices need to have secure code management, source coding, and software related testing to identify any issues. [147] There needs to be a trusted supply chain to "ensure no unintended malware or security bugs enter the supply chain." [148] Having a secure deployment phase is just as important as the design phase. Strong encryption is advised to ensure the integrity and privacy of data found on the device, in the cloud, or during the transmission to any third party. [149] Managing and auditing the software systems, the security of the communication channels, and the data storage cloud are necessary to ensure mobile device security and privacy. [150]

D. Avoid Advertising and Analytic Services

---

[142] *Id*.
[143] *Id*.
[144] *See* Lie Njie, *supra* note 125, at 14.
[145] *Id*.
[146] Milan Patel, *The Security and Privacy of Wearable Health and Fitness Devices*, SECURITY INTELLIGENCE (Sept. 10, 2015), https://securityintelligence.com/the-security-and-privacy-of-wearable-health-and-fitness-devices/.
[147] *Id*.
[148] *Id*.
[149] *Id*.
[150] *Id*.

As previously discussed, mobile apps frequently share personal information with third-party advertisers to target the user. Privacy-conscious consumers should avoid using apps that rely on advertisements for revenue. These users should try to use paid apps because they often carry a lower privacy risk than the free apps due to the lack of advertisements. If developers do not need to use ads in the apps as part of a revenue model, they should avoid doing so. [151] However, if it is necessary, the transmission of that data should be sent over an encrypted network. Also, if the data is being sent to analytics companies, the developer should not send the personal information, if possible. If not possible, the personal information should be anonymous so the user could not be identified. [152]

E. Develop Transparent Privacy Policies

The most significant way a developer can show the users' privacy is a priority is through a transparent privacy policy. Of the 43 mobile health and fitness apps the Privacy Rights Clearinghouse researched, only 50% of the free and paid apps had a privacy policy in place. [153] Based on the analysis, the privacy policies seemed to be written simply for the company's protection, not the consumers.[154] Privacy policies should explain what data the app collects, how it is being used, and with whom it will be shared. [155] Even if the developer does not believe that private sensitive information will be collected or privacy concerns will be raised, it is important to

[151] *See* Lie Njie, *supra* note 125, at 17.
[152] *Id*.
[153] *Id*. at 20.
[154] *Id*. at 20-21.
[155] *Best Practices for Mobile Application Developers*, FUTURE OF PRIVACY FORUM, http://www.futureofprivacy.org/wp-content/uploads/Best-Practices-for-Mobile-App-Developers_Final.pdf (last visited Nov. 2, 2015).

have a privacy policy in place. It should also be easily accessible and in a prominent location for users to find. [156]

The more clear, specific, and understandable the privacy policy is, the better the policy. If the purpose of collecting the data is not disclosed to the user, then the developer should not collect it. [157] If the use of the data is not disclosed to the user, the developer could be engaging in deceptive practices under the FTC Act. [158]Also, the developer should "obtain affirmative express consent before collecting and sharing sensitive information." [159]

If there are changes or updates that need to be done to the privacy policy, the developers need to make sure that these changes or updates reflect the new data use practices. [160] The new changes should be easily found and posted before the new data use practice. If these changes are material, the developer should gain new express consent by the user to make the user aware of these changes and allow them to process it. Providing a disclosure to the user before the collection of data or private information by the app will allow the user to make an informed decision about whether they want to continue using the app. [161]

Furthermore, the app platforms, such as Apple's App Store and Android's Google Play Store, should enforce their contractual agreement with the app developers that the apps have a privacy policy. [162] This could inform app developers of the importance of a privacy policy, educating them on the important information a privacy policy should comprise of as they develop

[156] *See* FED. TRADE COMM'N, *supra* note 63.
[157] *See Best Practices*, *supra* note 155.
[158] *Id*.
[159] *See* FED. TRADE COMM'N, *supra* note 63.
[160] *See Best Practices*, *supra* note 155.
[161] *See* FED. TRADE COMM'N, *supra* note 63.
[162] *Id*.

their apps. [163] The app platform might be the venue for the developer's privacy policy, where the developer can provide a link to the app's privacy policy, the actual text of the policy or a short notice statement of the app's data privacy practices. [164]

Moreover, developers should consider getting involved in trade associations to improve the privacy policy disclosures, creating the possibility of the mobile app industry privacy standard as to disclosures, terminology, format, notices, and consent forms. [165] Having this industry standard will make it easier for the user to understand the policy, reduce any confusion about the use of their data, and also allow users to compare apps to choose based on their personal privacy concerns. [166] For example, these trade associations can help eliminate the long, complicated, wordy policy that many users likely do not read, and replace them with standard icons and short disclosures that are convenient and understandable for the user. [167]

Through these efforts by the app developer, there could be a reduced number of potential privacy risks for the user. Informing the user of how the data is used, where it is being sent or stored while ensuring an encrypted network will create a level of comfort within the user. The privacy concerns start with the developer and how the developer chooses to design the application. The app developer should be proactive in its' app purpose, and make the users' privacy a priority.

VII. Conclusion

Mobile health and fitness apps provide great benefit to the consumer while simultaneously raising serious privacy risks. Users need to be cautious when using a health and fitness app or

[163] *Id*.
[164] *Id*.
[165] *Id*.
[166] *Id*.
[167] *Id*.

wearing a wearable device where private health information is being asked. It is clear that many of these apps release and share this private information with third parties.

As for the consumer wearables, this is becoming the new way for users to share sensitive, private and personal information about themselves. With many of them connected to a mobile app, similar privacy risks are involved. This is simply another means of companies to collect information about the user.

The scope of HIPAA for health app compliance is limited, despite the fact that many health and fitness apps are collecting this private data without asking permission and then distributing it to third party advertising and analytic agencies. Because HIPAA is limited to PHI and covered entities and their business associates, it does not cover or protect patient information for consumer health and fitness apps. Generally, there is no covered entity or business associate involved. Furthermore, it does not seem like the FTC has the solution for these privacy protection concerns. However, FTC will be able to protect the consumers' data by going after the app developers for unfair acts or deceiving practices through the FTC Act.

The app developer and wearable device designer are in the best positions to ensure privacy is protected. The developer needs to start self-regulating to protect privacy through its transparent privacy policy, its disclosures and notices, and only sending information to the necessary third parties upon the express assertive consent of the user. Until the developers start making privacy a priority, companies will continue to profit off of private consumer data unbeknownst to them.