Gabrielle Addonizio

The Privacy Risks Surrounding Consumer Health and Fitness Apps with HIPAA's Limitations and the FTC's Guidance

Mobile Health ("mHealth") has been a recent trend in the mobile world. Mobile Health combines healthcare services and the mobile industry allowing the consumer or patient to connect and interact with data for health related purposes.[1] Through mobile technology applications, people are able to connect and send their healthcare information to their physicians, and potentially share their health information with others.[2]

The mHealth market creates concerns about the way patients' and consumers' health data is managed and stored, causing a big shift from the physician's office system to mobile apps and storage in the cloud.[3] Patients and consumers are becoming more involved in their own healthcare through mobile health and fitness apps and wearable devices. However, there are many privacy risks associated with the convenience of the mobile health and fitness apps, along with their associated wearable devices.

Privacy law applicable to mHealth is often seen as whether HIPAA protects and applies to the application (app(s)). The average consumer does not read or understand the privacy policy, (if there is one) prior to downloading the app.[4] Furthermore, many consumers do not understand how they are compromising their own privacy when they "agree" to these policies.[5] Unfortunately, HIPAA does not protect everything healthcare related. On a larger scale, the federal government does not regulate mobile health applications.[6] However, the Federal Trade Commission (FTC) along with the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC), Office for Civil Rights (OCR), and the U.S. Food and Drug Administration (FDA) created a web-based guidance for mHealth app developers that helps the developers comply with any necessary federal laws that

might apply to their app.[7] Developers and companies, therefore, need to have an understanding of what HIPAA protects in order for the mobile app and wearable devices data to be HIPAA compliant.

The privacy risks associated with mobile health and fitness apps and their corresponding consumer wearable devices, such as FitBit and Apple Watch, 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. Unfortunately, the scope of HIPAA does not serve as a source of privacy protection for consumers against the inadequate privacy policies present in the mHealth industry.

The mobile app developers and consumer wearable device designers need to focus on consumer privacy from the developmental stage through implementing encrypted networks, possibly avoiding advertising and analytical services, and drafting clear and understandable privacy policies. Protecting the user's private information needs to be a priority and the entities collecting this information should be transparent as to its purpose behind collecting said information, creating a self-regulation process to ensure they are collecting only the information necessary for the function of the app.

As smartphones become increasingly prevalent in society, so have a variety of applications that provide a wide array of services. Mobile health apps, whether consumer or physician focused, have made dramatic changes within the healthcare industry.[8] 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. 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] Generally, these apps are for those who want to personally track and/or analyze their health and exercise routines.[11] They include, diet and exercise programs, symptoms checkers, health and lifestyle magazine subscriptions, and sleep trackers.[12] Many of these consumer apps have the option to connect to the consumer's social network profile, whereby users share their HEALTH information on social networks like Facebook.[13]

The personal and health information obtained in these apps varies depending on the app's purpose. Many of these apps require basic personal information—name, email, age, gender, height, and weight—to create an account or profile.[14] Some apps may also 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.[15]

It is becoming more apparent that mobile apps usually take the consumers' private information and data without the consumers' permission. When the user allows the app to see or use their current location for GPS purposes, the apps do not generally disclose to the user that this information will be sent to advertising companies.[16] Many app users do not know where the information is going or how the developer plans on using it.

Consumers cannot assume that the information they put into the app is private and protected. According to the Privacy Rights Clearinghouse, of the forty-three popular health and wellness apps analyzed, all presented some risk to the consumer.[17] From the same analysis, there were three main causes of informational privacy risks in the mobile health and fitness apps in order of most risk: insecure network communications; advertising; and third party analytics, .[18]

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.[19] 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.[20] Third, through the consumer health apps communications platform or a social network connection, the exposure to privacy attacks increases.[21] Once this information is public, consumers typically have minimal control over it.

Many of the health and fitness apps have unencrypted network connections for the transmission of the personal information. For malicious actors this means information is sent in plaintext, viewable to anyone.[22] 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.[23]

The mobile apps downloaded for free rely on advertising for revenue while the paid apps usually depend on the purchase price of the app for its revenue.[24] 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.[25]

Generally, mobile health applications are largely unregulated to protect consumers' privacy rights. The privacy protections limits whatever protection the developer privacy policy entails.[26] But people still purchase (and download) mobile apps despite the unclear, irrelevant, or

nonexistent privacy policy.[27] The privacy policy should describe the app's information sharing policies and describe potential risks, but some do not.[28] The goal of established privacy policies is to protect the developer from lawsuit, not to protect the consumer's privacy.

HIPAA is often seen as serving as an all-encompassing source of protection for medical information. However, HIPAA only concerns an individual's "protected health information" or "PHI."[29] This information is an individual's identifiable health information held and used by a covered entity or its business associate and transmitted electronically, on paper, or orally.[30] 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.[31]

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.[32] Health and fitness applications, 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.[33] 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).[34] Generally, covered entities may use or disclose PHI to the individual, for treatment, payment or health care operations, except "when the individual who is subject of the information authorizes in writing."[35] 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 administrative activities.[36] It is possible for a mobile health app to be covered

by HIPAA and the app developers are highly encouraged to use the Office of Civil Rights' guidance that provides examples where HIPAA *does* regulate the health apps.[37]

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. While the consumer may be entering identifiable personal health information, such as their name, address, date of birth, 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 not 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.[38] It is difficult for HIPAA to protect the mobile health and fitness app information because the information that is collected is not used directly for treatment.[39]

Consumer protection laws, such as the FTC Act, have attempted to fill this mobile health app privacy gap.[40] The FTC Act grants the FTC the power to oversee the mHealth app.[41] 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."[42] 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, specifically against the app developers who have secretly accessed the consumers' information on their devices for their "unfair and deceptive" practices.[43] Even though the FTC has not yet 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.[44] 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.[45] 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."[46] The FTC Rule does not prevent the sale of personal health data nor does it require health apps to get consent from consumers for uses and disclosure of information.[47] There are some gaps in this FTC Rule that does not address some privacy issues. 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.

Due to the limited scope of HIPAA and its lack of protection for consumers, the onus is on app developers to prioritize privacy. As discussed above, app developers should take advantage of this new web-based guidance tool for app developers will serve as a reference to know what the laws are and which laws could possibly apply to the specific mobile health app.[48] 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.[49] If that

privacy sensitive information is necessary, the data stored or transmitted needs to be encrypted.[50] The developer needs to start self-regulating to protect privacy through its transparent, understandable, and specific privacy policy, its disclosures and notices, and only sending information to the necessary third parties upon the express assertive consent of the user. From the developer's standpoint, investing in the data security measures recommended might result in a change of the developer's business model and having the app cost money to download, which in turn might deter some consumers from downloading it. However, this is the cost that is associated with protecting consumer's private information. 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.[51] Until the developers start making privacy a priority, companies will continue to profit off of private consumer data unbeknownst to them. So, unfortunately, right now it is "user beware."

---

[1] 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).
[2] *Id.*
[3] Symposium, Dongjing He, Muhammad Naveed, Carl A. Gunter & Klara Nahrstedt, *Security Concerns in Android mHealth Apps*, 2014 AMIA ANNU SYMP PROC. 645 (2014).
[4] Fran Rosch, *Study Finds Mobile Privacy Concerns Often Traded for Free Apps*, NORTON PROTECTION BLOG (Dec. 10, 2014, 4:51 PM), https://community.norton.com/en/blogs/norton-protection-blog/study-finds-mobile-privacy-concerns-often-traded-free-apps.
[5] *Id.*
[6] Daniel F. Schulke, Note, *The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing*, 93 B.U.L. REV. 1699, 1700-1701 (2013).
[7] Jonathan Havens, Michelle Jackson, Julia Kernochan Tama, & Thora A. Johnson, *FTC Creates Compliance Tool for Mobile Health App Developers; Simultaneously Releases Business Guidance*, ALL ABOUT ADVERTISING LAW BLOG (Apr. 6, 2016) http://www.allaboutadvertisinglaw.com/2016/04/ftc-creates-compliance-tool-for-mobile-health-app-developers-simultaneously-releases-business-guidance.html#more-3836.
[8] 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/.

[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.
[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] *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.
[12] *Id*.
[13] See Helm, *supra* note 1, at 138.
[14] 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.
[15] *Id*.
[16] Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J.,(Dec. 18, 2010), http://www.wsj.com/articles/SB10001424052748704368004576027751867039730.
[17] *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.
[18] *Id*.
[19] Symposium, Dongjing He, Muhammad Naveed, Carl A. Gunter & Klara Nahrstedt, *Security Concerns in Android mHealth Apps*, 2014 AMIA ANNU SYMP PROC. 645 (2014).
[20] *Id*.
[21] *Id*.
[22] *See* PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 11.
[23] 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/.
[24] *See* PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 11.
[25] *Id*.
[26] *Id*.
[27] *Id*.
[28] *See* Carns, *supra* note 14.
[29] 45 C.F.R § 160.103 (2015).
[30] *Id*.
[31] *Id*.
[32] Adam H. Greene, *When HIPAA Applies to Mobile Applications*, MOBIHEALTHNEWS, (June 16, 2011), http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/.
[33] *Id*.
[34] 45 C.F.R § 160.103 (2015).
[35] 45 C.F.R § 160.502(a) (2015).
[36] 45 C.F.R § 160.103 (2015).
[37] OFFICE FOR CIVIL RIGHTS, *Health App Developers, What Are Your Questions About HIPAA?*, (2016), http://hipaaqsportal.hhs.gov/a/pages/helpful-links.

[38] *See* Greene, *supra* note 32.
[39] *Id*.
[40] Hank Creasy & David Knoespel, *The New Generation of Electronic Health Records: What Health Apps Know About You*, 64 VIRGINIA LAWYER 25 (June 2015).
[41] 15 U.S.C. §§ 41-56 (2012).
[42] 15 U.S.C. § 45 (a)(2) (2012).
[43] 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. *See* Helm, *supra* note 1.
[44] FED. TRADE COMM'N, *Complying With The FTC's Health Breach Notification Rule*, (Apr. 2010), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.
[45] *Id*.
[46] *Id*.
[47] *Id*.
[48] FED. TRADE COMM'N, *Mobile Health Apps Interactive Tool*, (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.
[49] Craig Michael Lie Njie, *Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications*, PRIVACY RIGHTS CLEARINGHOUSE (Aug. 12, 2013), https://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.
[50] *Id*.
[51] 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.