DePaul University
University Libraries

DePaul Journal of Health Care Law

Volume 18
Issue 2 *Winter 2016*

Article 3

March 2017

To Cover Or Not To Cover? The Relationship Between The Apple Watch and The Health Insurance Portability and Accountability Act

Cristina M. Mares

TO COVER OR NOT TO COVER? THE RELATIONSHIP BETWEEN THE APPLE WATCH AND THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

Cristina M. Mares[*]

I. INTRODUCTION

The phenomenon of the Apple Watch and its corresponding healthcare applications, or "apps," are increasingly making their way into the daily lives of many Americans. Seventy-nine percent of Americans are willing to use a wearable device to manage their health and, in 2015, health apps had some of the highest number of downloads.[1] PricewaterhouseCoopers projects that healthcare will be the top three biggest mobile trends of 2016.[2] Generally, the Apple Watch and its apps are used to track and store information about the wearer's physical activity.[3] The Apple Watch can perform a variety of functions such as monitoring the user's daily activities, providing suggestions to improve health and activity, and awarding incentives for reaching daily goals.[4] Additionally, when paired with an iPhone, the Apple Watch can be used as a heart-rate monitor or an accelerometer for more personalized and accurate physical activity monitoring.[5] These health apps allow consumers to gain knowledge and perspective on their physical well-being as well as

---

[*]*J.D. Candidate, DePaul University College of Law, 2017. Cristina holds a B.A. in Communication Studies and Spanish from the University of San Diego. She has a special interest in the regulatory and compliance areas of health care law.

[1] Jennifer Elias, *In 2016, Users Will Trust Health Apps More than their Doctors*, Forbes (Dec. 31, 2016), *at* http://www.forbes.com/sites/jenniferelias/2015/12/31/in-2016-users-will-trust-health-apps-more-than-their-doctors/#3a81bec42d5f.

[2] *Id.*

[3] Paul A. Drey, Sarah Wendler, *Peeling Back the Apple Watch: Do HIPAA and the Apple Watch Go Together?* American Bar Association Health eSource, *at* http://www.americanbar.org/publications/aba_health_esource/2015-2016/september/applewatch.html.

[4] *Id.*

[5] *Id.*; *see also* Arthur Peabody, Jr., Health Care IT: The Essential Lawyer's Guide to Health Care Information Technology and the Law 79 (ABA Section of Science & Technology Law, 2013).

help patients better manage their ailments or illnesses and improve treatment compliance.[6]

There has also been an increase in healthcare apps for healthcare providers.[7] For example, there are several new apps designed to allow the healthcare consumer to track her own health and send the data to her electronic health record (EHR), thus providing real-time updates to her healthcare provider.[8] Healthcare providers are utilizing the Apple Watch and its related health apps as an opportunity to provide rapid communication between themselves and their patients that will, hopefully, aid in the quality of care of the patient.[9]

Streamlined communication between healthcare providers and their patients is a great advance in technology for the healthcare field. However, several issues of patient privacy and the security of personal health information (PHI) arise with the implementation of these devices and apps because of the information transmitted. The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) are the two major federal statutes that create a looming possibility of regulation of the Apple Watch and its apps in the healthcare world. These rules authorize the Secretary of Health and Human Services to promulgate regulations safeguarding the privacy of medical records containing personally identifiable information.[10] An area of concern is that current healthcare privacy laws do not address healthcare data stored on a consumers' own personal devices (e.g., Apple Watch, iPhone).[11] The surge of data breaches that have taken place recently within the healthcare field further emphasize the need to extend privacy and security laws to devices such as the Apple Watch and its related apps. Currently, PHI that is transmitted to healthcare consumers' Apple Watch or iPhone would not be protected, thus making sensitive data even more susceptible to unauthorized attacks.

Aware of the potential security risks, the Department of Health and Human Services (HHS) is also monitoring this "explosion of technology" and contemplating how HIPAA and other federal laws require these

---

[6] Peabody, *supra* note 5.
[7] Peabody, *supra* note 5 at 78.
[8] Drey, *supra* note 3.
[9] Kif Leswig, *The Apple Watch is a Smash Hit – In this One Field*, Business Insider (April 12, 2016), *at* http://www.businessinsider.com/the-apple-watch-is-a-smashing-hit-in-this-one-field-2016-4.
[10] Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 Am. J.L & Med. 416, 423 (2014).
[11] Drey, *supra* note 3.

technologies to have certain privacy and security protections in place.[12] The Food and Drug Administration (FDA), which generally has broad authority to regulate products marketed to the public, has recently decided to take "an almost hands-off approach" in order to give this sector of the technology industry freedom to develop new products without aggressive regulation.[13] However, the FDA is limited to regulation of this industry because any regulation it implements would generally apply to "medical devices." The Food, Drug, and Cosmetic Act (FDCA) defines "medical devices" as any product intended for use in the diagnosis, treatment, or prevention of disease, or intended to affect the structure or any function of the body."[14] Although an Apple Watch may not be considered a medical device, several healthcare apps may require FDA regulation if an app "acts as an accessory to a regulated medical device, turns a mobile gadget into such a device, or makes suggestions regarding a patient's diagnosis or treatment."[15] Unless the Apple Watch is used as a "medical device" pursuant to the FDCA, the FDA is limited in its scope of regulation of this sector of the technology industry. Lastly, the Federal Trade Commission (FTC) has shown concerns about the risks of health data that flow outside of a medical context, such as information collected via wearables[16] and mobile health apps.

The hesitation to heavily regulate the Apple Watch and related health apps has been due to the concern that regulation will inhibit innovation for technology companies developing these apps and devices. The positive effects these devices and apps have on the public is also something the government does not want to hamper; specifically because several corporations now incentivize their employees to use wearables and specific apps to live healthier lifestyles, while also decreasing insurance

---

[12] Alex Ruoff, *Privacy Watchdogs to Collect Tech Industry's HIPAA Questions, Health Data Privacy*, Health IT Law & Industry Report (BNA), 7 HITR 8 (Oct. 5, 2015).

[13] Adam Satarino, *Apple Watch, Other Consumer Products Get FDA Attention as Part of Tech Boom*, Health Care Pol'y Rep. (BNA) , 23 HCPR 525 (March 30, 2015).

[14] 21 U.S.C. § 321(h)(2)-(3) (2012).

[15] Steven Overly, *FDA Moves to Regulate Mobile Health Applications*, Washington Post (July 19, 2011), *available at* http://www.washingtonpost.com/business/capitalbusiness/fda-moves-to-regulate-mobile-health-applications/2011/07/18/gIQApwLdNI_story.html.

[16] Note that I will use the term "wearable" throughout; "wearables" (e.g., the Apple Watch) are defined as devices that are worn on the wrist, head, ankle, or any other body part, and serve to computerize the daily functions of its user. Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 Geo. L.J. 1641, 1642 (2014-2015). It can also be used to collect and store personal health data. *Id.*

costs.[17] The variety, complexity, and usefulness of healthcare apps that operate on the Apple Watch and iPhone highlight the difficulties involved in current and future regulation. Because HIPAA focuses on the privacy and security issues of healthcare apps used within the medical field, the new area of concern is the ineffective source of protection in the hazy area of patient and consumer health. The current issue is how to balance the protection of PHI without hindering this innovative area that is revolutionizing healthcare delivery.

This Article proceeds in four parts. In Part I, I discuss the current reach of HIPAA and HITECH protection of PHI on the Apple Watch and its related apps. In Part II, I examine how the HITECH Act and HIPAA Omnibus Rules changed the landscape of wearable and app security. In Part III, I discuss the increasing prevalence with which wearables are being implemented into medical research and into the workplace. Finally, in Part IV, I discuss the possible solutions that government or industry leaders could implement that may provide coverage and recourse to consumers if their PHI is stored on their wearable devices.

II. CURRENT HIPAA AND HITECH PROTECTION OF PHI ON THE APPLE WATCH AND ITS RELATED APPS.

Currently, federal privacy laws have a limited reach regarding PHI stored on consumers' personal devices. PHI includes any individually identifiable information maintained or transmitted by a covered entity or a business associate that relates to an individual's physical or mental health or the provisions of or payment for healthcare.[18] HIPAA's coverage extends to individuals, organizations, and agencies that meet the definition of a "covered entity" or if a covered entity engages a "business associate" to help it carry out its healthcare activities and functions.[19] HIPAA defines a "covered entity" as healthcare providers, health plans, or healthcare clearing houses who *electronically* transmit any health information in connection with a transaction covered by HIPAA.[20] A covered entity must comply with HIPAA Rule requirements to protect the privacy and security

---

[17] oline Chen and Shannon Pettypiece, *Target to Offer Fitbits to 335,000 Employees*, BNA Health Care Pol'y Rep. (BNA), 23 HCPR 1418, (Sept. 21, 2015).

[18] 45 C.F.R. § 160.103 (2014).

[19] HHS.gov, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html (last visited Dec. 4, 2015).

[20] *Id.*

of health information and must provide individuals with certain rights regarding their health information. A "business associate" is defined as a person or entity that creates, receives, maintains, or transmits PHI on behalf of a covered entity.[21] A covered entity that engages a business associate must have a written business associate contract that establishes specifically what the business associate has been engaged to do, therefore also requiring the business associate's compliance with HIPAA.[22]

HIPAA obligations and restrictions apply to the Apple Watch if PHI is stored on the device or issued through a healthcare app and is used by or in the control of a covered entity or a business associate. Apps like the Apple Health app[23] and HealthKit[24] were originally designed to allow individuals to keep track of health and fitness data in one place, but now other healthcare apps, like MyChart,[25] work in conjunction with Health app and HealthKit allowing instant transmission and storage of data to providers and consumers. Because MyChart gives patients access to their medical records, which are classified as PHI, the security concern is that this PHI may be essentially unprotected data if it is stored on a patient's Apple Watch or iPhone. Once the PHI is stored on a personal device, HIPAA protection disappears because the PHI is no longer linked to a provider. Conversely, once this health data is transmitted from the user's Apple Watch or health app to a hospital or clinic (covered entity), the health data then qualifies as PHI and is HIPAA-protected. Therefore, such data is subject to health record privacy and security rules. Because the data becomes HIPAA-protected upon receipt by a covered entity, it is important that each covered entity and business associate understand how HIPAA

---

[21] 45 C.F.R. § 160.103(1)(i).

[22] *Id.*

[23] The Apple Health app gives consumers an easy-to-read view of their health and fitness data on either iPhone or Apple Watch. Apple Health, *at* http://www.apple.com/ios/health/ (last visited Feb. 11, 2016).

[24] HealthKit allows apps that provide health and fitness services to share their data with the [Apple] Health app and with each other. Apple HealthKit, *at* https://developer.apple.com/healthkit/ (last visited Feb. 11, 2016). A user's health information is stored in a centralized and secure location and the user decides which data should be shared. *Id.*

[25] MyChart is a mobile app that gives patients access to their medical records. Epic, Mobile Applications and Portals, *at* https://www.epic.com/software-phr.php (last visited Feb. 5, 2016). Through MyChart, patients are able to view test results, view paperless statements and pay bills, update medications and allergies, connect to home devices, refill prescriptions, send messages to providers, as well as schedule appointments or view education topics triggered by electronic health record data. *Id.*

applies to the use of the app and how patient data is used, maintained, and stored.[26]

There are hundreds of health apps that are available for download. Some health apps are geared solely toward healthcare providers, others that are used by the general consumer, and other apps used by both providers and patients. Apps that are generally used by healthcare practitioners are considered to be "medium or high-risk" because they may "display, store, analyze or transmit patient-specific medical device data" or perform patient-specific diagnoses, analyses, and treatment recommendations.[27] The Doximity app[28] and other healthcare apps may be used in conjunction with the Apple Watch and most likely require compliance to HIPAA security rules due to the use of PHI. Next, apps used by both providers and their patients, like Cerner's HealtheLife app,[29] are most likely also deemed as medium to high-risk if PHI is used or transmitted between the practitioner and the patient. Finally, apps that are used by the general consumer are considered "low risk" because they generally "store, organize, or track health information" such as calorie intake or the amount of steps taken, data that is not considered to be PHI.[30] Low risk apps are not required to be HIPAA compliant and include apps like the Apple Activity app.[31]

---

[26] Drey, *supra* note 3.

[27] *FDA Says it Will Not Actively Regulate Low-Risk Mobile Medical Apps*, Sidley Austin LLP (Oct. 1, 2013), *at* http://www.sidley.com/en/news/fda-says-it-will-not-actively-regulate-low-risk-mobile-medical-apps-10-01-2013.

[28] The Doximity app is a HIPAA privacy-compliant communications app that physicians can use to send and receive clinical communications hands-free from the Apple Watch. Mark Sullivan, *Apple Watch Mania Sees 13 New Health Care Apps Announced in the Past Week*, Venture Beat (Apr. 14, 2015), *at* http://venturebeat.com/2015/04/14/apple-watch-mania-sees-13-new-health-care-apps-announced-in-the-past-week/.

[29] Cerner's Healthelife app is designed to keep patients more engaged and informed by sending notification reminders to the user's Apple Watch, as well as by tracking certain elements of the user's health data and displaying it on a small dashboard on the Apple Watch. *Id.* Cerner is also creating a system to collect biometrics and vitals data from patients via the Apple Watch and the app to store the data in the Cerner electronic health records system. *Id.*

[30] *FDA Says it Will Not Actively Regulate Low-Risk Mobile Medical Apps*, *supra* note 26.

[31] he Activity app provides a snapshot on the Apple Watch of the wearer's daily activity, such as how many calories the wearer burned, how often the wearer has stood up, and how many minutes of "brisk activity" were completed. *A Smarter Way to Look at Fitness*, Apple, *at* http://www.apple.com/watch/health-and-fitness/ (last visited Feb. 14, 2016).

A. HIPAA Privacy and Security Rules

With looming regulations facing the wearable market, HIPAA Privacy and Security Rules would be the most severe if compliance were to be expanded to this market. The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of PHI, as well as sets limits and conditions on the uses and disclosures of such information without patient authorization. The Privacy Rule also gives patients rights over their PHI, such as rights to examine and obtain a copy of their health records.[32] Because the Privacy Rule gives patients a right to examine and obtain a copy of their health records, many providers transmit this information to a patient via health apps like MyChart, Doximity, or Athenahealth[33] which are considered to be HIPAA-protected. However, if the patient proceeds to store PHI on a wearable device such as an Apple Watch, the Privacy Rule no longer applies, thus eliminating any recourse to the patient should the PHI be lost or stolen from a personal device. This distinction is significant because healthcare providers are liable for disclosed PHI pursuant to HIPAA, whether disclosure was intentional or due to mere negligence.[34] Further, any healthcare provider that integrates healthcare apps as a part of patient care will be required to inform the patient of her "rights as an individual" pursuant to the use and transfer of potential PHI through any app.[35] HIPAA has required that any covered entity must provide individuals with a written notice describing the entity's privacy practices, however with the increasing use of healthcare apps among physicians, such information about cyber privacy practices must also be included.[36]

The HIPAA Security Rule requires that covered entities and business associates must ensure the confidentiality, integrity, and availability of all electronic personal health information (ePHI) the

---

[32] HHS.gov, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (last visited Dec. 4, 2015).

[33] AthenahealthCommunicator allows patients to complete tasks online instead of calling the provider directly. Mobile Health Apps for Better Practice Management, athenahealth, *at* http://www.athenahealth.com/knowledge-hub/practice-management/mobile-health-apps (last visited Feb. 5, 2016). The app lets patients exchange messages with staff, manage payments, check lab results, and view appointments. *Id.*

[34] 45 C.F.R. § 164.502 (2013).

[35] June M. Sullivan, HIPAA: A Practical Guide to the Privacy and Security of Health Data 53 (ABA Health Law Section, 2004).

[36] *See* Sullivan, *supra* note 35 at 55 (the use of health care apps by a practitioner to transfer PHI to the patient may be included in the Privacy Notice section, "Right to Receive Confidential Communications of PHI.")

covered entity or business associate creates, receives, maintains, or transmits; and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.[37] Thus, healthcare providers are required to implement stringent security measures to protect patient information, such as "installing remote wiping applications (to remove data in the event the device is lost or stolen), and using properly secured services to send or receive health information. . . ."[38] The issue here is whether storage on a wearable device such as an Apple Watch would qualify as "maintaining" ePHI. Unless a covered entity or a business associate uses the device to maintain this sensitive data, the patient's stored ePHI in her own personal Apple Watch will not qualify under the Security Rule, once more eliminating any possible recourse if the wearer loses such data or if the data becomes compromised by an unauthorized third-party.

B. Data Breach Susceptibility

The lack of privacy protection or security guidelines pertaining to Apple Watches and its related healthcare apps is particularly problematic because of the reoccurring data breaches that have taken place in the healthcare world. Cyber attacks on healthcare organizations were the most prevalent cause of data breaches in 2014.[39] A majority of these data breaches have been attacks on covered entities, which means that such attacks happened even with the implementation of stringent security procedures required under HIPAA and HITECH. Employee negligence was the single leading cause of data breaches, with employees failing to follow security procedures or simply losing health records or computers containing electronic health records.[40] Employee negligence may increase as more and more health care providers implement the use of mobile health apps to communicate with patients. Liability falls on the covered entity or business associate if a breach occurs from any employee negligence. This HIPAA protection would give the patient a potential avenue of recourse from any breach that included PHI. Unfortunately, a patient does not have an opportunity of redress if she loses her Apple Watch with stored PHI as a result of her own negligence. Because healthcare will continue to be a prime target for hackers with the value of health records (PHI) on the rise,

---

[37] 45 C.F.R. § 164.306(a) (2013).
[38] Peabody, *supra* note 5 at 81.
[39] Alex Ruoff, *Health-Care Cyberattacks Now Most Prevalent Source of Breaches, Study Says*, Health Care Pol'y Rep. (BNA), 23 HCPR 734, (May 11, 2015).
[40] *Id.*

the market for stolen records will also grow, thus increasing the likelihood of breaches in this sector.[41]

Breaches are defined as the unauthorized acquisition, access, use, or disclosure of PHI which comprises the security or privacy of such information.[42] Covered entities and business associates who suffer a security breach of PHI are then subject to comply with HIPAA data breach notification standards. As long as health data is not stored and shared with any HIPAA-covered entity or business associate, the exchange of that data is not susceptible to HIPAA regulations at all.[43] The main security problems and weaknesses that wearables face are mobile phones and any connection to "cloud" storage,[44] not the actual device itself. Because wearables tend to link to mobile devices wirelessly via Bluetooth, data is sent and received between the wearable and mobile phone, making it a prime target for hackers.[45] Similarly, consumer data is often stored in cloud storage (iCloud for Apple), which is "probably the weakest link of all."

C. HIPAA Compliance or Something Else?

One question that arises with the nature of these data breaches is whether Apple and its related healthcare app developers should be required to implement privacy and security procedures pursuant to HIPAA. If this were to happen, would Apple Watch and other third-party app developers need to qualify as "business associates" as defined in HIPAA? These entities would be considered business associates if they create, receive,

---

[41] Akanksha Jayanthi, *Data Breaches in 2016: What Can we Expect?* Becker's Health IT & CIO Review, (Dec. 23, 2015), *at* http://www.beckershospitalreview.com/healthcare-information-technology/data-breaches-in-2016-what-can-we-expect.html (stating a Reuters report that found PHI to be ten times more valuable than a credit card number).

[42] 45 C.F.R. § 164.402 (2013).

[43] Langley, *supra* note 16 at 1649.

[44] "The Cloud" or "cloud computing" refers to an application that is hosted on or run on Internet servers that enables consumers to store media files and other data, rather than storing such information on an actual device. Joanna Stern, *What is the 'Cloud'?* ABC News, (June 26, 2012), *at* http://abcnews.go.com/Technology/cloud-computing-storage-explained/story?id=16647561.

[45] Gary Davis, *The Wearable Future is Hackable. Here's What You Need to Know*, McAfee Blog Central, (Feb. 18, 2015), *at* https://blogs.mcafee.com/consumer/hacking-wearable-devices/; *see also* Maggie Overfelt, *The Price of Wearable Craze: Personal Health Data Hacks*, CNBC, (Dec. 12, 2015), *at* http://www.cnbc.com/2015/12/12/price-of-wearable-craze-your-health-data-hacked.html.

maintain, or transmit PHI on behalf of a covered entity.[46] Unless an app is used merely to maintain an individual's physical activity (not PHI), an app developer or the Apple Watch would not need to comply with HIPAA privacy or security rules. Unfortunately, several healthcare apps (e.g., Apple Health app, HealthKit, and MyChart) are now integrating with each other for a more streamlined, easy-to-use experience, thus blurring the lines between what constitutes PHI and what does not. This means that the Apple Health app that was only used to track physical activity now has the capability to work hand-in-hand with apps such as MyChart or Athenahealth, which are designed to transmit and store PHI. Because these apps are used by covered entities they must comply with HIPAA Privacy and Security Rules, but mere storage of PHI on a patient's Apple Watch or other wearable device does not provide such protection.

Because wearables are not yet subject to HIPAA compliance, other guidelines have been created so that users may be proactive about security concerns on their devices. To create awareness of privacy and security concerns, HHS created a website solely dedicated to "mobile device privacy and security."[47] However, these guidelines merely explain how healthcare providers can help protect and secure patient health information when using mobile devices by using passwords, encrypting[48] sensitive data, and researching mobile apps before downloading.[49] Unfortunately, these guidelines do not mention privacy and security implications regarding the use of healthcare apps that store PHI on personal devices, such as an Apple Watch. Nonetheless, consumers may follow these guidelines to help protect and secure any wearable device.

Currently, there is no "checklist" for securing all apps because different apps have different security needs.[50] However, the Federal Trade Commission (FTC) expects app developers to "adopt and maintain reasonable data security practices" and offers a list of "tips for mobile app

---

[46] Drey, *supra* note 3.

[47] HealthIT.gov, Mobile Device Privacy and Security, *at* https://www.healthit.gov/providers-professionals/8-research-mobile-applications-apps-downloading (last updated Jan. 15, 2013).

[48] Encryption is a way to enhance the security of data by scrambling the contents so that only someone who has the right encryption key to unscramble it can read it. *What is Encryption?* Microsoft Windows, *at* http://windows.microsoft.com/en-us/windows/what-is-encryption#1TC=windows-7 (last visited Feb. 16, 2016). Encryption creates a stronger level of protection for personal information. *Id.*

[49] *Id.*

[50] *Mobile App Developers: Start with Security*, FTC, *at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security (last updated Feb. 2013).

security" on its website.[51] Healthcare app developers who create apps for consumers to help them manage and organize their information (e.g., inputting blood glucose levels or blood pressure readings) would fall under this category and would be subject to reasonable data security practices.[52] Conversely, an app developer that creates an app particularly for healthcare providers *and* their patients will be considered business associates of the provider and will be subject to HIPAA compliance. In that case, the provider would "contract[] with the app developer for patient management services that involve creating, receiving, maintaining and transmitting PHI. . ."[53] Unfortunately, app developers who offer a "direct-to-consumer" app that allows consumers to store, manage, and organize their health records on their personal devices or on the app itself are not subject to HIPAA protections.[54]

D. Consequences of a Data Breach to a Consumer.

The consequences of a data breach of PHI on a consumer's Apple Watch or other wearable device could be financially devastating to the user. Because the Apple Watch does not require strict security protection, it may be relatively easy for a sophisticated hacker to access and acquire PHI within the device. The access and acquisition of such sensitive data could create a significant risk of identity theft, as well as crippling financial harm to the owner. Fitbit, a fitness bracelet that tracks a wearer's physical activity, recently experienced such a breach after "online criminals" gained access to several customer accounts and attempted to defraud the company.[55] The criminals stole email addresses and passwords from third-party websites and used the data to access Fitbit accounts.[56] Consequently, the criminals ordered replacement products by using customer warranties, changed customer account information, and accessed customer data, such as biostatistics[57] and GPS history.[58] Although Fitbit does not maintain,

---

[51] *Id.*
[52] Health App Use Scenarios & HIPAA 2 (Feb. 2016) *available at* http://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/OCR-health-app-developer-scenarios-2-2016.pdf.
[53] *Id.* at 3.
[54] *Id.*
[55] Akanksha Jayanthi, *Fitbit accounts targeted by online fraudsters*, Becker's Health IT & CIO Review, (Jan. 7, 2016) *at* http://www.beckershospitalreview.com/healthcare-information-technology/fitbit-accounts-targeted-by-online-fraudsters.html.
[56] Jayanthi, *supra* note 55.
[57] Biostatistics includes data such as when the Fitbit wearer goes to sleep or how many steps the wearer took in a day.
[58] Jayanthi, *supra* note 55.

store, or transmit PHI, and is thus not subject to HIPAA liability, security researcher, Axelle Apvrille, alleged that she was able to hack a Fitbit bracelet in only 10 seconds from as far as 15 feet away.[59] This shows the vulnerability of wearables and should be a warning to Apple since its Apple Watch is able to store much more sensitive data, such as PHI. Apple should attempt to mitigate potential security and privacy risks with the Apple Watch and corresponding apps (HealthKit and Apple Health App) in order to prevent a modern day "Ford Pinto moment" from happening.[60]

III. CHANGES FROM THE HITECH ACT AND HIPAA OMNIBUS RULES

Although HIPAA Privacy and Security rules were stringent on their own, HITECH and HIPAA Omnibus Rules established and expanded additional security procedures focusing on electronic data. HITECH, part of the American Recovery and Reinvestment Act of 2009, works hand-in-hand with HIPAA regarding privacy and security concerns associated with the electronic transmission of health information.[61] HITECH expanded the reach of HIPAA compliance to business associates, as well as imposed a nationwide security breach notification law for entities that possess ePHI.[62] Through several provisions, HITECH strengthens the civil and criminal enforcement of the HIPAA rules.[63]

---

[59] Alexandra Burlacu, *Experts Warn It Just Takes 10 Seconds to Hack Fitbit Fitness Trackers: Here's Fitbit's Response*, (Oct. 24, 2015) *at* http://www.techtimes.com/articles/98427/20151024/experts-warn-it-just-takes-10-seconds-to-hack-fitbit-fitness-trackers-heres-fitbits-response.htm.

[60] Teena Maddox, *The Dark Side of Wearables: How they're Secretly Jeopardizing your Security and Privacy*, TechRepublic, *at* http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/ (last visited Feb. 16, 2016) (quoting Conan Dooley, a senior security engineer with Box, who compared the current security problems of wearables with the Ford Pinto's exploding gas tank scandal that changed the standards for the entire auto industry).

[61] HHS.gov, *at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (last visited Dec. 4, 2015).

[62] Heidi Echols, Maura Ward, Karen Sealander, Bernadette Broccolo & Stephen Bernstein, *HITECH ACT: Analysis of Policy Implications, Requirements of Health IT Provisions*, Health Care Pol'y Rep. (BNA), 17 HCPR 336, (March 2, 2009).

[63] HHS.gov, *supra* note 61.

A. The HITECH Act and HIPAA Omnibus Rules

The 2013 HIPAA Omnibus Rules included a provision that mandated the Privacy Rule would now apply to business associates who handle PHI for a covered entity by explicitly stating that liability extends down the chain of information technology to include covered entities, business associates, and subcontractors.[64] In addition, the Omnibus Rules state that business associates are responsible for complying with HIPAA's Security Rule.[65] Most significant, the Omnibus Rules modified the definition of "business associate" to include health information organizations and any "other person that provides *data transmission services* with respect to protected health information . . . and that requires access on a routine basis to such protected health information."[66] The expansion of "data transmission services" is important because it raises the question of whether these services include devices like the Apple Watch and medical health apps. Apps that transmit PHI from patient to physician most likely fall under this umbrella, but the issue of PHI storage on personal devices is still unclear even with the expansion of "business associate." However, a narrow exception is granted to entities and Internet service providers that only provide transmission services of PHI.[67] Thus, if an app merely transmits PHI it may escape breach liability. One could argue that because the Apple Watch, together with the iPhone, is capable of "maintaining" PHI that it should be subject to HIPAA regulation, but the Apple Watch would have to be used by a covered entity or business associate in order to become HIPAA-protected.

The Omnibus Rules also strengthened HITECH Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to the Department of Health and Human Services (HHS).[68] Now, when a breach occurs, the presumption is that the information has been compromised, and the person or entity responsible for the breach has the burden of proving that the breach has a low probability of risk.[69] Another major change is that patients can now ask

---

[64] *New rule protects patient privacy, secures health information*, HHS.gov (Jan. 17, 2013), *at http://www.hhs.gov/about/news/2013/01/17/new-rule-protects-patient-privacy-secures-health-information.html#.*
[65] *Id.*
[66] 45 C.F.R. § 160.103 (3)(i) (2014) (emphasis added).
[67] Joyce L.T. Chang, *The Dark Cloud of Convenience: How the New HIPAA Omnibus Rules Fail to Protect Electronic Personal Health Inform*ation, 34 Loy. L.A. Ent. L. Rev. 119, 143 (2013-2014).
[68] *New rule protects patient privacy, secures health information*, *supra* note 64.
[69] 45 C.F.R. § 164.402(2) (2013).

for a copy of their electronic medical records in an electronic form,[70] thus allowing for the swifter, more efficient storage and transmission of PHI, classified as electronic protected health information.[71] Theoretically, this change would lead to the presumption that ePHI would be transmitted to patients through apps and then stored on their personal devices. Once more, the weak security of wearables is highlighted creating further questions of why the storage of PHI on a user's personal device has not been addressed. Lastly, the Omnibus Rules established that the individual consumer does not have a private right of action under HIPAA; all HIPAA privacy and security violations must be reported to HHS who then decides whether or not to investigate the charges.[72] The "no private right of action" rule may be somewhat of a safety net for companies like Apple and app developers because it closes the floodgates of insurmountable litigation that could destroy technology companies due to bankruptcy, specifically smaller companies. This is a good change because it may prevent the filing of frivolous lawsuits.

B. The Liability of Apple and App Developers

The looming possibility of HIPAA and HITECH regulation may be overwhelming to app developers, but because these federal laws do not yet apply, do Apple and app developers still face any liability regarding security breaches of PHI stored on the Apple Watch, iPhone, or healthcare apps? The answer to this question is, it depends. As noted, healthcare apps such as MyChart and Athenahealth are covered under HIPAA and HITECH because they are promoted as a means for providers to have a more uniform and centralized method of communication that is secure and complies with HIPAA requirements.[73] However, when PHI is merely stored on the user's Apple Watch or when the user uploads PHI to a healthcare app, privacy and security concerns arise because strict adherence to HIPAA's rules are not required or recommended. In order to escape some liability of potential privacy and security weaknesses of consumer health data, Apple has implemented "specific privacy parameters" with its HealthKit framework. Because HealthKit allows apps to obtain health data from the user's device, the user must explicitly give each app permission to "read and write data" to the HealthKit by granting

---

[70] *New rule protects patient privacy, secures health information*, *supra* note 64.
[71] Chang, *supra* note 67 at 123.
[72] *Id.* at 126.
[73] Drey, *supra* note 3.

or denying permission separately for each type of data.[74] An example that Apple gives is that a user may allow an app to read the "step count" data but prevent it from reading the blood glucose level.[75] Perhaps this is a way of Apple releasing itself from any liability if the consumer loses an Apple device.

These "privacy parameters" give the consumer power over what information she is comfortable sharing and storing, as well as puts the consumer on notice of any privacy implications. Although the consumer is allowed to grant and deny the type of data stored, consumers still have no way of knowing the security levels of these apps. Consumers are basically putting all of their trust into these third-party apps while simultaneously releasing Apple from any liability. However, consumers are most likely not concerned with the privacy or security of shared data on these apps and are unaware of any serious consequences of a potential breach. The average consumer probably does not think of her health data on her Apple Watch to be sensitive information like she would of her medical records in a doctor-patient setting. Apple also emphasizes that HealthKit data is only kept locally on the user's device.[76]

Lastly, to help app developers become aware of privacy concerns, as well as comply with any privacy and security regulations, Apple provides potential healthcare app developers with links directly to healthIT.gov. This website provides privacy and security guidelines for both HIPAA covered apps and non-HIPAA apps.

IV. THE INCREASING USE OF WEARABLES IN MEDICAL RESEARCH AND THE WORK PLACE

The Apple Watch and Fitbit are two wearables that have recently received a lot of attention from corporations looking to encourage healthy lifestyles from their employees. Pharmaceutical and biotechnology companies have also begun enlisting wearables and other gadgets in their research trials in an effort to bring drugs to the market faster.

Companies such as BP and Target are giving their employees wearable devices to track their activity levels as part of "wellness programs." Monitoring employee activity levels incentivizes employees to lead a healthier lifestyle because the fitness data may be tied into health

---

[74] The HealthKit Framework, *at* https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/ (last updated Nov. 19, 2015).
[75] The HealthKit Framework, *supra* note 74.
[76] *Id.*

insurance policy premiums or other incentive programs to reduce health care costs.[77] However, privacy concerns arise because the data transmitted from the wearable to the corporation may be more sensitive than simply how many steps were taken in a week or an employee's caloric intake. This may be particularly concerning because as wearable devices begin to gather more and more personal and biometric data, security risks may grow since consumer-grade devices do not always have strict encryption and other security protections to safeguard personal data.[78] Consequently, companies may be exposed to data leaks or theft. Depending on the type of employee data that is generated to employers, companies will need to be aware of any health information that might be considered sensitive data. Because a company such as Target or BP is generally not considered to be a covered entity or business associate, HIPAA compliance will not be required, however, standard industry security procedures should be implemented in order to reduce the risk of any foreseeable data breaches. On the other hand, if employee data is collected and used by health insurance companies, HIPAA privacy and security compliance is required since health insurance companies are considered covered entities.

Similarly, pharmaceutical and biotechnology companies are increasingly using wearables during research trials. In outfitting trial participants with wearbables, companies are beginning to accumulate precise information and gather "round-the-clock data" in hopes of streamlining trials and better understanding whether a drug is working.[79] In addition, wearables could help pharmaceutical makers prove to insurance companies that their treatments are effective, therefore reducing health costs.[80] According to the National Institutes of Health's records, there have been at least 299 clinical trials using wearables.[81] Pharmaceutical and biotechnology companies are considered covered entities pursuant to HIPAA because they transmit health information in electronic form from these wearable devices.[82] Consequently, pharmaceutical and biotechnology companies are subject to handling, storing, and transmitting PHI in accordance with the requisite laws and

---

[77] Olivia Solon, *Wearable Technology Begins to Creep Into the Workplace*, Health IT Law & Industry Rep. (BNA), 7 HITR 16, (Aug. 6, 2015).
[78] *Id*.
[79] Anna Edney and Caroline Chen, *Big Pharma Hands Out Fitbits to Collect Better Personal Data*, Health Care Pol'y Rep. (BNA), 23 HCPR 1419, (Sept. 14, 2015).
[80] *Id.*
[81] *Id.*
[82] Rachel V. Rose, *How Does HIPAA and the HITECH Act Impact Medical Device and Pharma Companies?* Becker's Health IT & CIO Review, (Jan. 11, 2013), *at* http://www.beckershospitalreview.com/healthcare-information-technology/how-does-hipaa-and-the-hitech-act-impact-medical-device-and-pharma-companies.html.

regulations.[83] Generally, under HIPAA, patients (research subjects) have a right to access their PHI from a clinical trial.[84] Thus, once a patient has her ePHI stored on her own personal device, such as an Apple Watch, any possible HIPAA liability no longer applies. Although HIPAA liability does not apply once PHI is given to the patient, privacy and security concerns were not as prevalent in the past because PHI was generally given in paper form, thus limiting the risk of third-party acquisition. However, ePHIs create a more ominous environment for data breaches because they may be reached remotely from anywhere in the world. Unfortunately, any breach or loss of PHI once it is in a patient's possession would generally be the fault of the patient; most likely due to patient negligence or lack of security measures.

V. WHAT IS THE SOLUTION?

At first glance, it seems that the most rational solution would be to merely expand HIPAA and HITECH's reach to include storage of PHI on Apple Watches and its related apps. Unfortunately, this solution is more complicated because there is not a clear line between what is considered PHI and what is not. However, the potential widespread use of the Apple Watch and other similar devices by healthcare professionals and consumers will most likely encourage privacy and security regulation from government watchdogs, as well as impact the wearable and app industry.

Apart from government concern, technology companies and mobile app developers have vocalized their growing concerns about how possible privacy implications may affect their industry. To help address some of the major health privacy questions that this industry has regarding development of their products, the Center for Democracy & Technology (CDT) held an event in January of 2015 called "Always On."[85] This event brought together leading experts in government, academia, advocacy, and industry to explore the regulatory and social challenges facing the "digital patient."[86] This forum recognized the importance of user privacy, but also stressed that the repeated emphasis on privacy has slowed potential medical progress.[87] The big question was, and still is, "[h]ow much is privacy really worth?"[88]

---

[83] *Id.*
[84] 45 C.F.R. § 164.524 (2014).
[85] Michelle De Mooy, *Always On: Taking the Privacy Pulse of Today's Digital Patient*, Center for Democracy & Technology (CDT) (Jan. 30, 2015) *at* https://cdt.org/blog/always-on-taking-the-privacy-pulse-of-todays-digital-patient/.
[86] *Id.*
[87] *Id.*
[88] *Id.*

Although each expert that attended "Always On" had different arguments for why or why not the wearable and technology industry should be regulated, all experts agreed that HIPAA is outdated and that new legislation should be designed to reflect today's rapidly advancing technological environment.[89] It is rather surprising that in a day and age where society relies almost entirely on technology that one of the largest and most important privacy and security laws has not also been "updated" to reflect this way of life. Perhaps privacy and security regulation has not been at the forefront of Congress's agenda because it feels as though HIPAA is pervasive enough as it is. Maybe this should be an issue for state police power rather than that of federal regulation.

The biggest hurdle for technology companies and mobile app developers is the cost of complying with HIPAA Privacy and Security Rules if regulation is expanded to storage of PHI on wearables and apps. Although Apple has the financial means to engage legal counsel, many app developers are small and lack the funding necessary to be able to hire legal counsel to ensure compliance with such complicated federal laws. A potential solution to this dilemma is that the technology industry could adopt its own straightforward "rules of best practice" to eliminate confusion over regulation as well as make compliance less expensive.[90] Nevertheless, these "rules of best practice" will most likely have to conform, mirror, or be even stricter than HIPAA Privacy and Security Rules; consequently creating the same hurtles to compliance.

As noted, the FDA is currently withholding regulation to this industry, but because the FDA has a limited reach that only extends to claims of accuracy of "medical devices," most likely the privacy and security issues of the storage of PHI on wearables will not be part of its overall regulation scheme. Similarly, the FTC would be expected to regulate claims of accuracy made by creators of wearable devices and health apps as opposed to privacy and security issues.[91]

Another possible solution could be expanding the definition of PHI to include non-personally identifiable information. This would include data such as a person's daily activities (the amount of time spent sitting, standing, or moving), workout data (heart rate, calories burned), and other exercise-related statistics.[92] This would erase the blurry line between which data constitutes PHI and which data does not. Under this solution,

---

[89] De Mooy, *supra* note 85.
[90] *Id.*
[91] Michael D. Williamson, *Regulations on Wearable Devices Could be Coming, Privacy Advocate Says*, Health Care Pol'y Rep. (BNA), 23 HCPR 826, (May 27, 2015).
[92] Drey, *supra* note 3.

almost all personal data will be considered PHI. Although this solution seems to include too much information, it would create more ease of determining HIPAA regulation. Similarly, if practitioners and patients are using apps to share PHI between each other, perhaps hospitals could implement a policy requiring such data be "de-identified" so that the patient information does not identify the individual and there is no reasonable basis to believe that the information can be used to identify an individual.[93] De-identified information is "neither individually identified health information nor protected health information" which means that it can be freely used, disclosed, transferred, and stored on a patients wearable with little security concerns.[94] If a patient's Apple Watch were to be hacked, the information stored would not include sensitive data that could result in identity theft or economic harm. This policy may be costly, time consuming, and most likely would require the help of a security Information Technology (IT) team or it may even require the app itself to de-identify PHI, however, this may protect any potential PHI stored on an individual's device from becoming compromised.

Individuals are able to take many of the same security measures that healthcare providers take in order to protect PHI on their mobile devices, however the average person is somewhat lax when it comes to implementing security on her own personal devices.[95] Consumers often fail to take adequate security precautions and believe that merely deleting sensitive files and using a "passcode" to lock devices are sufficient methods of data protection.[96] However, most people are naïve about how easy it is for third-party hackers to infiltrate wearables and other mobile device, not to mention how easy it is to lose a device or have it stolen. The average person may not be aware of the potential consequences that arise with storage of PHI on personal devices and the need to strengthen security on such devices. Although it seems that news of data breaches occur daily, consumers seem to believe that they are immune from any such attack. Therefore, it is imperative to create more awareness of how easy it is to hack or retrieve data from an Apple Watch and other wearable devices, as

---

[93] Scott C. Withrow, HIPAA Compliance: Standards for Electronic Transmission, Privacy, and Security of Health Information 119 (Health Administration Press, 2001).
[94] *Id.*
[95] Peabody, *supra* note 5 at 81; *see also* Blancco Technology Group, *Consumers Risk Data Loss with Lax Approach to Mobile Security*, Business Reporter (Nov. 23, 2015) *at* http://www.blancco.com/en/about-us/in-the-news/consumers-risk-data-loss-lax-approach-mobile-security (finding that many consumers are aware of the risks posed by mobile devices but are not taking preventive steps to protect themselves. A large number of consumers also have a "false sense of security" when storing information on mobile devices).
[96] Blancco Technology Group, *supra* note 95.

well as the ramifications of weak security. Awareness would incentivize consumers to implement some of the security measures that heathcare providers use. Perhaps this could be an endeavor that technology companies could do as a part of using their apps or devices. Similarly, federal or state campaigns could raise awareness of the security concerns of wearables and apps to the general public, which would further both the technology companies' and the government's interests.

Consequently, because of the many different agendas between private technology companies and government entities that are involved in this area of technology, any quick resolution will be unlikely.

VI. CONCLUSION

Although HIPAA and the HITECH Act are pervasive laws, they do not protect individuals who store PHI on their Apple Watch and accompanying apps. This is particularly true now that more and more healthcare providers and their patients are incorporating wearables and healthcare apps into their everyday lives. The technology industry is attempting to grapple with the many security and privacy issues before releasing their products and services; however, the increasing sophistication of hackers makes protecting consumers' data harder and harder. It is clear that there is a need for some type of government regulation or industry guidelines in this area. The many legal implications of data breaches could cripple part of the technology industry, as well as create financial harm to the unaware consumer. Most likely the expansion of HIPAA regulation to the storage of PHI on devices such as the Apple Watch will be the go-to solution, unless industry and government leaders develop an alternative answer. Unfortunately, the privacy and security implications of PHI stored on Apple Watches or other wearable devices will most likely not be regulated until a major breach, or "Ford Pinto moment" occurs.[97]

[97] Maddox *supra*, note 60.