Intersect, Vol 10, No 3 (2017)

Wary About Wearables: Potential for the Exploitation of Wearable Health Technology Through Employee Discrimination and Sales to Third Parties

Nayanika Challa, Stephen Yu, and Sanjay Kunchakarra
University of Chicago and University of Pennsylvania

Abstract

The wearable health technology market is booming due to its potential to capitalize on the acquisition of real-time health metrics and effect positive lifestyle changes. However, dangers arise from the continuous monitoring, tracking, and recording of user data, as it allows wearable health technology companies to potentially exploit user data through third-party sales. There remain ambiguous characterizations of wearable health devices as either electronic communication services or remote computing services and wearable health data as either content or non-content under the Stored Communications Act (SCA). In 2012, the FTC revealed that twelve health and fitness apps sold user data to seventy-six different third parties, bringing the issue of health data transmission to the forefront. Here, we investigate the potential misuse of wearable health technology data for inappropriate monitoring, informal screening, and potential discriminatory actions against employees. We evaluate the shortcomings of the Americans with Disabilities Act (ADA), Equal Employment Opportunity Commission (EEOC), and Genetic Information Nondiscrimination Act (GINA) in clearly delineating the role of wearable health data.

Background

Wearable technology is revolutionizing healthcare, as individuals are becoming more aware of their health and demanding the data in order to improve their well-being and prevent future illness. Fitness bands and watches address step tracking, sleep monitoring, and heart rate tracking, which serve as proxies for a consumer's current state of health (Duffy, 2015). But wearable technology extends far beyond fitness devices, as evidenced by the European group Semeoticons' Wize Mirror project, which plans to use "multispectral cameras, gas sensors, and 3-D scanners to collect data in such areas as weight gain or loss, blood oxygen levels and stress, and then highlight potential risk factors" (DeRenzo, 2016). If digitized and integrated into electronic medical systems, wearables can potentially relay more complicated metrics such as diet, posture, ultraviolet light exposure, skin temperature, and respiratory rate, alerting medical personnel in real time when life threatening changes occur (Edwards, 2015).

As wearable devices gain traction over the next five to ten years, their potential will only be realized if they engage consumers, convert raw data into insights, and focus on improving consumer health. The increased presence of wearables in the market is not conjectural. In the past three years, there has been a 500% increase in the number of fitness bands and activity trackers sold (Danova, 2014). According to Transparency Market Research, in its emerging stages, the wearable technology market was $750 million in 2012 and is expected to reach $5.8 billion in 2018, a 40.8% compound annual growth rate (Latest Trend in the Wearable Technology Industry, 2015). Similarly, the research firm Market and Market predicts that the wearable industry will continue to grow at exceptional rates to eventually reach $11.61 billion by the end of 2020 (Shedd et al., 2015). Activity tracker startups like Fitbit and technology giants like Apple, which comprise "more than 80 percent of the health-related wearable technology market are helping drive a new digital health-conscious movement into a $2.8 trillion health care industry. Research firm Gartner estimates that more than 1.4 billion health and fitness units will ship by 2020, up from roughly 300 million today" (Overfelt, 2015). This booming industry of wearable technology heralded by Fitbit now has plenty of competitors, including Jawbone, Garmin, Nike, and Misfit (Brody, 2015). Although these devices have gained traction among all age groups, they seem to particularly attract young adults "motivated enough to want a device and able to afford it," according to Dr. Mitesh S. Patel and colleagues at the University of Pennsylvania (Patel et al., 2015). As technological advancements and increased competition lead to more affordable prices and more effective monitoring systems, the number of consumers who own a wearable device is expected to rise.

It is clear that wearables represent a major step in the penetration of healthcare technology. These devices allow users to track their daily activities and fitness progressions. Sleep patterns, calories burned, and

steps taken can all be tracked and recorded by the device and parent digital health company without any action by the user; however, this convenience does not come without a price. A decentralized legal framework underlying wearable health technology allows for its greater exploitation by parent digital health technology companies and employers.

Sale To Third Parties

Stored Communications Act (SCA)

The Stored Communications Act (SCA) "addresses voluntary and compelled disclosure of stored wire and electronic communications and transactional records held by third-party internet service providers" (Minc, n.d.). In relation to the wearables industry, the SCA's applicability depends on two factors. First, the SCA will only apply to the associated health apps "if they provide either an electronic communication service or a remote computing service to the public. Second, if the health apps provide one of these services, the level of protections afforded to the wearable's communications will depend on whether the communications are considered content or non-content" (Minc, n.d.). For instance, health apps, like the Apple Watch, provide users with both an electronic communication service as well as a remote computing service. The watch serves as an electronic communication service, as it allows users to voluntarily share heart rate and exercise data with a friend. However, the watch also serves as a remote computing service, because it is continuously collecting and storing this same data when worn by the user. It is currently unclear whether a company can be simultaneously considered a provider of an electronic communication service and a remote computing service. In any scenario, for wearables, these health apps at least fall under one of these categories, thereby mandating the need for SCA compliance.

The most pressing issue here is the subtle difference between content and non-content. Content refers to the substance and meaning underlying a communication, such as spoken words or written words in emails, whereas non-content refers to the records such as telephone numbers and email addresses. If wearable data are considered content, then they will receive limited disclosure protections of section 2702(b). However, if wearable data are considered non-content, then health apps would not violate section 2702 (Voluntary disclosure of customer communications or records) by selling the data without proper notification to the individual. This is because subsection 2702(c) provides exceptions for disclosure of customer records (SCA subsection 2702(c)). The difficult question of "whether a user's heart rate obtained through a wearable is the content of a communication or is more like a customer record" elicits no clear answer (Langley, 2015). Health information data generated from wearable devices blur the line between content and non-content, which ultimately paves the course for potential exploitation.

The problem with wearable health data being considered as non-content arises from the fundamental way the devices function, which relies on the continuous collection and storage of information about the device user. "Similar to location data, the user's health data are generated automatically - the user cannot simply choose to stop his heart rate" (Langley, 2015). Thus, except when a user intentionally shares his health data with another user, any generated data can easily be considered a customer record. Moreover, health data that is voluntarily shared can also potentially be considered non-content, similar to location sharing. The Electronic Communications Privacy Act (ECPA) was enacted as an amendment to the SCA and provided new provisions prohibiting access to stored electronic communications (18 U.S.C § 2510-22). While seemingly fitting for the current wearables data dilemma, the ECPA was created in 1986 with regard to wire taps from telephone calls and did not contemplate modern communication technology (U.S Department of Justice, n.d.). Furthermore, there is a loophole in the ECPA that allows companies to "freely disclose customer records, but not contents of a communication, to third parties" (Langley, 2015). Based on the current statutory definition of the ECPA, it seems likely that health data would be considered customer records instead of content of a communication.

This is alarming by any means and portrays the necessity for regulation on non-content, at least in the case of health data, which tends to be sensitized. Although the SCA currently holds the basic framework to protect private data generated from wearables, "the content problem reveals why the SCA has not kept up with modern technology" (Langley, 2015). Modernizing the ECPA by explicitly including sensitive health data or wearable health technology in its statutory definition could prove beneficial to addressing the commercial wearable problem.

Proof of Exploitation

Wearables generate vast amounts of user health data by continuously monitoring and storing information about the user. The information is then wirelessly transmitted to a mobile app, which then sends the data through a cloud operating system to be further stored and analyzed. "In many respects, those data's value is based on their potential to be used for the greater good, such as disease prevention. From a commercial standpoint, marketers want these data to gain insight into individual preferences as a means of offering personally targeted products" (Langley, 2015). In some situations, these goals are achieved as with the use of continuously generated patient health data, such as with blood pressure measurements to construct more personalized and tailored interventions for people with hypertension (Milani, 2016).

However, abuse and misuse of this health data also occurs in the industry. "According to Federal Trade Commission (FTC) findings, health apps are in fact transmitting sensitive health information to third parties. On May 7, 2014, the FTC released a study, which found that twelve

different health and fitness apps transmitted user data to seventy-six different third parties, including advertisers" (Federal Trade Commission, 2014). The data transmitted encompassed a wide range of metrics and information including exercise routines, dietary habits, and symptom searches. Most alarming was that in a subset of cases, "even names and addresses were being transmitted" (Scelsi, 2015). To complicate matters, a FTC examination of twelve health and fitness apps found that these apps lacked privacy policies that disclose what data is collected, how it is used, and who it is shared with (Scelsi, 2015). Although the FTC did not reveal the names of the health apps it investigated, the study adequately showed that wearable health data privacy concerns are legitimate.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, is largely responsible for the protection and privacy of sensitized health data. It relates that Private Health Information (PHI) can be shared with covered entities such as a health care provider, a health plan, or one of their business associates such as a pharmacy benefits manager (§160.103). HIPAA contains forward-looking statements, as evidenced by its distinction between "Required specifications" and "Addressable specifications", the latter providing flexibility and latitude for covered entities (U.S. Department of Health & Human Services, n.d.). However, there remains cause for concern. While HIPAA "solved the privacy problem of wearables in the medical field, it remains an ineffective source of protection in the commercial sphere" (Langley, 2015). Non-providers and individuals do not fall under HIPAA's jurisdiction.

Moreover, because data collected by wearables can be transferred through a chain of covered and non-covered entities, this same data can pass in and out of HIPAA coverage, thereby circumventing the law at different entities. This may pose a problem for new wearable health technology firms entering the market, as they may not be aware of their needing to comply with HIPAA if they provide data to covered entities (Barash, 2015). "HIPAA was enacted, in part, to ensure confidentiality in all health care information" (Langley, 2015). To this end, HIPAA required the Department of Health and Human Services to adopt standards, known collectively as the Administrative Simplification Provisions, with respect to the electronic exchange, privacy, and security of private health information (Langley, 2015). Furthermore, a Business Associate is also regulated by Privacy, Security, and Breach Notification Rules established through HIPAA and modified by the Health Information Technology for Economic and Clinical Health (HITECH) Act, an extension of HIPAA (HIPAA Basics for Providers: Privacy, Security, and Bread Notification Rules). HIPAA's Privacy Rule requires that covered entities have appropriate safeguards, both physical and digital, on hard copy and verbal PHI, sets limits on the disclosure of PHI, and gives patients the rights to

access their PHI (Office of the Federal Register, 2013; Other Modifications to the HIPAA Rules, n.d.). Under the Security Rule, Business Associates must implement administrative safeguards, such as in risk analysis, along with physical and technical safeguards (S 1814, 110th Cong, 1st Sess). Under the Breach Notification Rule, breaches of unsecured PHI must be reported without unreasonable delay and no later than 60 days after discovery (U.S. Department of Health & Human Services, n.d.). Once an organization is deemed a covered entity, numerous safeguards must be erected to protect all individually identifiable health information data. While these rules serve to regulate a budding industry, the sheer complexity associated with data falling in and out of HIPAA coverage results in a highly fragmented and incomplete system.

The amount of regulation begs the question of whether wearable devices can be HIPAA compliant. The first point of concern manifests in the difference between HIPAA compliance and Business Associate compliance. The former applies to an entity, such as a covered entity. The latter does not mean that the covered entity is compliant when using a Business Associate's device. To further complicate matters, the device itself, including its software and hardware, cannot be HIPAA compliant, although it can support HIPAA compliance through features promoting de-identification and generalization such as encryption. Thus, covered entities can comply with HIPAA by including the device in a compliance program (Barash, 2015). While the efficacy here is unclear, it is evident there are gaps in the regulation of compliance among businesses. While HIPAA may not apply directly to wearable devices, it "may apply to wearables and their collection of health-related data when related to the operation of a group health plan" (Lazzarotti, 2015). This is the case if the health apps associated with wearables are considered covered entities. To reiterate, "[c]overed entities means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic format in connection with a transaction covered by the HIPAA" (§ 160.103). Employers will be required to consider the consequences of these privacy and security standards, including whether "(i) changes are needed in the plan's Notice of Privacy Practices, (ii) business associate agreements are needed with certain vendors, and (iii) the plan's risk assessment and policies and procedures adequately address the security of PHI in connection with these devices" (Lazzarotti, 2015). However, for the purpose of consumer wearables, health apps are not seen as covered entities since they do not provide medical care, transmit information between entities in the health care system, or provide health care services. Instead, wearables allow people to personally collect data and monitor their own lives as they see fit. Since wearable health apps are not defined as covered entities, they are exempt from HIPAA regulation. Thus, it is worth noting that while "HIPAA may have solved the privacy problem of wearables in the health sector by limiting covered entities

disclosure of patient information, it is completely ineffective against consumer wearables" (Langley, 2015).

While the HIPAA statute covers the vast majority of health care business taking place in the United States, there are gaps that can potentially be exploited. According to Leon Rodriguez, Director of the Office for Civil Rights, U.S. Department of Health and Human Services, "[t]he HIPAA statute really covers three types of what we call covered entities…Excluded from that definition can be providers who don't transmit health information transactions electronically, typically, for example, in a private-pay sort of enforcement. So there clearly are health care providers out there who are not currently subject to the HIPAA statute" (Your Health and Your Privacy: Protecting Health Information in the Digital World, n.d.). Thus, in the absence of covered entities, data provided by wearable devices such as heart rate, respiration level, or skin temperature are not considered protected under HIPAA and can potentially be distributed. There may be a statutory difference between the same data, with the difference lying in whether it was collected by a covered entity or by an individual collecting his own data through a wearable in the hopes of monitoring his personal health. "As long as the health data are not stored and shared with any HIPAA-covered entity or business associate, the exchange of that data are not susceptible to HIPAA regulation at all" (Langley, 2015). Currently, "the vast bulk of wearable health data is tracked and stored outside of these covered entities and is therefore not subject to HIPAA protections. Accordingly, consumers, developers, businesses, and manufacturers are in uncharted territory" (Bromberg, 2014). HIPAA, then, is not the answer for consumer privacy protection in the case of wearables.

The existing federal legal framework is inadequate in preventing the exploitation of sensitized digital health data by parent companies of wearable health technology. There are currently no laws or governing bodies explicitly preventing health app and wearable companies from selling collected user health data to third parties. Consumer privacy suffers as parent companies of these devices profit from the sale of sensitive health information at the expense of individual users.

Employee and Insurance Discrimination

As companies accumulate data points on employees, they face impactful decisions based on undisclosed personal health data. For example, an employee could be penalized for having a relatively inactive week and subsequently be deemed a health risk by an insurance provider, thereby having to pay higher premiums (Langley, 2015). This sparks the controversy of actuarial underwriting. When evaluated on underwriting factors, people who demonstrate a propensity toward an increased risk of loss can be provided with different premiums and coverage options "so long as these disparities are cost justified, non-invidious and do not operate as a subterfuge" (Kirsch, n.d.). The entirety of the insurance

industry rests on the concept of actuarial fairness in pricing and coverage, which prevents adverse risk selection and the subsequent potential for insurance markets to collapse. In the case of HIV, because the legal system has ruled that HIV screenings can be considered sound underwriting practices, insurers can deny coverage or charge different premiums based on the results of such testing (Kirsch, n.d.). *Health Ins. Ass'n v. Corcoran* and *Life Ins. Assoc. of Mass. v. Comm'r of Ins.* in conjunction reveal that HIV is a sound underwriting practice, as the afflicted are expected to live for shorter amounts of time and are more susceptible to illnesses throughout the course of their lives (Health Ins. Assn vs. Corcoran, 1998). This allows for the denial or modification of coverage and premiums. Thus, we see that, at least in regard to HIV, adverse selection is upheld. The generation of data and subsequent tests may streamline the screening process for insurance providers, resulting in cost differentials and coverage discrepancies.

Data gathered by wearables has its merits but is not without its share of pitfalls. According to PricewaterhouseCoopers, "70 percent of consumers say they would wear employer-provided wearables streaming anonymous data to a pool in exchange for a reduction in their health insurance premiums. For employers, wearable technologies allow for great efficiencies by tracking employee productivity, improving security and even improving the accuracy of healthcare" (Bevitt, 2015). A residual effect of the massive amount of generated data is the potential alienation of and discrimination against certain subsets of the workforce. Even under the best of intentions, employers will know the physical activity of employees, which is problematic when an employee, who may know that he should be more active but may find it very difficult to be so, is targeted by the employer. Underscoring an employee's lack of activity to colleagues could result in a decrease in team involvement. "Alternatively, employees may view wearables as just another metric against which they will be measured and learn how to 'game the system' and come out on top, reducing the quality of the data collected" (Bevitt, 2015). Workforce programs that incorporate wearables are in their nascent stages and are known to fall under the category of Health Contingent Wellness Programmes under HIPAA, since they reward employees for meeting a standard related to a health factor (Health-Contingent Wellness Programs, n.d.). Health contingent wellness programs are regulated by HIPAA in that they must be designed to promote health or prevent disease, and alternatives must be provided for people who cannot reach the reward standard. These programs are also under the regulation of the Americans with Disabilities Act (ADA), which prohibits disability-related inquiry or discrimination. The issue here is that programs requiring a wearable device could generate data suggesting a disability for an employee, which otherwise may not have been revealed (Bevitt, 2015). According to the Equal Employment Opportunity Commission (EEOC) which implemented the ADA, voluntary employee health and wellness programs allow

employers the opportunity to conduct medical examinations or inquire about disabilities (U.S. Equal Employment Opportunity Commission, n.d.). This effectively allows employers to screen employees under the guise of an employee health program. It is no surprise, then, that the ADA's requirements of wellness programs are facing serious pressure to change.

While current laws regulating wearable devices are limited, the Genetic Information Nondiscrimination Act (GINA) works to prohibit group health plans and health insurers from denying coverage to a healthy individual or charging that person higher premiums based solely on a genetic predisposition to developing a disease in the future. GINA also prohibits employers from using genetic information as a basis when making hiring, firing, job placement, or promotion decisions. Under GINA, genetic information is considered personal health information and is protected under HIPAA. GINA, HIPAA, and HITECH laws help to protect patients from being discriminated against based on their genetic information/predispositions through employer sanctioned health data analytics (Scelsi, 2015).

However, the potential for personal data exploitation, employee discrimination, and actuarial underwriting is significant despite employers noble intentions to improve the health and efficiency of the workforce through wearable devices and health data analytics. Some employees foresee these possibilities, which prompts their hesitancy in sharing health data with employers. "They worry that the information could negatively affect their insurance premiums, chances for promotions or opportunities for raises," according to Jim Huffman, senior vice president and head of U.S. Health and Wellness Benefits for Bank of America (Martin, 2015). Since the Equal Employment Opportunity Commission has sued companies in the past for wellness programs that allegedly violated federal anti-discrimination laws when they coerced employees to participate, companies are keen to prevent employee complaints. Eric Dreiband, a partner with law firm Jones Day, stressed the importance of "maintaining a secure 'firewall' between the data collected by wearable technology and personnel records. The goal is to keep staff health and fitness data away from supervisors or other decision makers, so that it cannot inadvertently affect employee pay or promotions" (Martin, 2015). If this data is not kept separate, the government could be alerted to investigate and file a lawsuit.

The privacy and exploitation challenges associated with wearable devices are considerable, but it is essential that advances in this space are not derailed on the basis of hypothetical worst-case scenarios. Major benefits are and will continue to be associated with this new technology, but these benefits may be limited if overly preemptive policies are implemented. As investigated above, the fundamental complexity of wearable devices lies in its ability to both store and transfer data. This second ability is not innocuous. Although the data being stored may be harmless, its transfer can violate many privacy laws, such as HIPAA.

Thus, the key to regulating wearables resides in protecting the transfer of data. Moving forward, a multi-phased solution can be implemented to strengthen the regulation of this industry. In the short term, organizations should devote time to understanding how the specific wearable devices work with regard to its ability to store and transfer data. In this interim period, employers should consider hiring a third party to manage any sensitive data collected in order to avoid claims related to knowledge of employee medical issues. Maintaining this secure firewall between those in positions to determine promotions or premiums and the data itself is of utmost importance. In the long term, employers should focus on creating organizational rules and the necessary infrastructure regarding acceptable technology. While controlling the movement of data is certainly a difficult task, it should not be neglected so as to ensure wearable technology can become a valuable asset to healthcare providers and employers in the 21st century.

References

§160.103

18 U.S.C § 2510-22

Barash, L. (2015). *Legal Issues and Risks in Wearable Health Technologies: A Live Webinar, Davis Wright Tremaine's Health Care Webinar Series: What You Need to Know* Retrieved from http://www.privsecblog.com/2015/09/articles/surveillance/dwt-webinar-legal-issues-in-wearable-health-technologies/

Bevitt, A. (2015). Challenges with workplace wearables in the EU and US. *Privacy & Data Protection Journal, 16*(1). Retrieved from https://www.cooley.com/files/Challenges%20with%20workplace%20wearables%20in%20the%20EU%20and%20US%20-%20Ann%20Bevitt.pdf

Brody, J. E. (2015). *Assessing the Fitness of Wearable Tech.* Retrieved from http://well.blogs.nytimes.com/2015/11/16/assessing-the-fitness-of-wearable-tech/

Bromberg, K. (2014). Wearable Health Industry Has To Be Proactive on Privacy. *Law 360*. Retrieved from https://www.cohengresser.com/assets/publications/Wearable_Health_Industry_Has_To_Be_Proactive_On_Privacy_-_Law360.pdf

Danova, T. (2014). *Just 3.3 million fitness trackers were sold in the US in the past year.* Retrieved from at http://www.businessinsider.com/33-million-fitness-trackers-were-sold-in-the-us-in-the-past-year-2014-5

DeRenzo, N. (2016). A Smart Mirror That Could Diagnose Ilness. *United Hemispheres Magazine*, *71*. Retrieved from http://www.hemispheresmagazine.com/2015/12/01/smart-mirror-diagnose-ilness/#CuSFDWhkvWpJKUqs.97

Duffy, J. (2015). *The Best Fitness Trackers for 2016.* Retrieved from http://www.pcmag.com/article2/0,2817,2404445,00.asp

Edwards, C. (2015). *Digital health technology and data are benefiting employees, employers*. Retrieved from http://www.mhealthnews.com/blog/digital-health-technology-and-data-are-benefiting-employees-employers

Federal Trace Commission (2014*). FTC Spring Privacy Series: Consumer Generated and Controlled Health Data Transcript.* Retrieved from https://www.ftc.gov/system/files/documents/videos/spring-privacy-series-consumer-generated-controlled-health-data/ftc_spring_privacy_series_-_consumer_generated_and_controlled_health_data_-_transcript.pdf

Health Ins. Ass'n v. Corcoran 551 NYS 615, 618 (AD 3 Dept. 1990)

Health-Contingent Wellness Programs. (n.d.). *United Healthcare*. Retrieved from http://www.uhc.com/content/dam/uhcdotcom/en/HealthReform/PDF/Provisions/WellnessHealthContingentPrograms.pdf

HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules. Retrieved from https://www.cms.gov/Outreach-and-

Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf

Kirsch. L. *Assessing the Actuarial Basis for Health-Related Underwriting in Medical and Disability Insurance*. Retrieved from http://www.bazelon.org/LinkClick.aspx?fileticket=R9YQS4gzb44%3D&tabid=345

Langley, M. R. Note: Hide Your Health: Addressing the New Privacy Problem of Consumer Wearable. *The Georgetown Law Journal, 103.* Retrieved from https://georgetownlawjournal.org/articles/36/hide-your-health-addressing/pdf

Latest Trend in the Wearable Technology Industry. (2015). Retrieved from http://blog.zensorium.com/latest-trends-in-the-wearable-technology-industry/

Lazzarotti, J. J. (2015). *Wearables, Wellness and Privacy.* Retrieved from http://www.natlawreview.com/article/wearables-wellness-and-privacy

Life Ins. Assoc. of Mass. v. Comm'r of Ins. (1998)/ 403 Mass. 410, 416

Martin, J. A. (2015). *14 ways to improve corporate wellness programs with wearables.* Retrieved from http://www.cio.com/article/2988907/wearable-technology/14-ways-to-improve-corporate-wellness-programs-with-wearables.html

Milani, et al. (2016). New Concepts in Hypertension Management: A Population-Based Perspective. *Progress in Cardiovascular Diseases*, *59*, 289-294. Retrieved from http://www.sciencedirect.com/science/article/pii/S0033062016301074

Minc, A. (n.d.). *What is the Store Communication Privacy Act?* Retrieved from http://www.defamationremovallaw.com/what-is-the-stored-communication-privacy-act/

Office of the Federal Register (US) (2013). *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, A Rule by the Health and Human Services Department.* Retrieved from https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-15

Overfelt, M. (2015). *The price of wearable craze: Personal health data backs*. Retrieved from http://www.cnbc.com/2015/12/12/price-of-wearable-craze-your-health-data-hacked.html

Patel, M. S., Asch, D. A., & Volpp, K. G. (2015). Wearable Devices at Facilitators, Not Drivers of Health Behavior Change. *JAMA*. Retrieved from http://www.telbios.com/wp-content/uploads/2015/01/jvp140141.pdf

S 1814, 110th Cong, 1st Sess

SCA subsection 2702(c)

Scelsi, C. (2015). New Media and Old Metaphor: Care and Feeding of Privacy Policies and Keeping the Big Data Monster at Bay: Legal Concerns in Healthcare in the Age of the Internet of Things. *Nova Law Review, 391*(39). Retrieved from https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=39+Nova+L.+Rev.+391&srctype=smi&srcid=3B15&key=f12b6d13ccac97e3fba0b33026105915

Shedd, J., Tahas, L, & Woebse, E. (2015). *Are Wearable Devices a Privacy Nightmare?* Retrieved from http://www.jdsupra.com/legalnews/are-wearable-devices-a-privacy-nightmare-69302/

U.S Equal Employment Opportunity Commission, Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees Under the Americans With Disabilities Act (ADA). Retrieved from http://www.eeoc.gov/policy/docs/guidance-inquiries.html

U.S. Department of Health & Human Services, Breach Notification Rule. Retrieved from http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

U.S. Department of Health & Human Services, What is the difference between addressable and required implementation specifications in the Security Rule. Retrieved from http://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html

U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, Electronic Communications Privacy Act of 1986. Retrieved from https://it.ojp.gov/privacyliberty/authorities/statutes/1285

Your health and Your Privacy: Protecting Health Information in a Digital World, Hearing on S. HRG 112-867 before the Subcommittee on Privacy, Technology and the Law of the Committee on the Judiciary United States Senate, 112 Cong, 1st Sess. Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-112shrg87166/pdf/CHRG-112shrg87166.pdf