HEALTH DATA PRIVACY AND SECURITY IN THE AGE OF WEARABLE TECH: PRIVACY AND SECURITY CONCERNS FOR THE NFLPA AND WHOOP

Terence M. Durkin*

I. Introduction

As the proliferation of new technologies allows for increased amounts of personal data to be collected and stored, increased attention is required for the privacy and security of such data.[1] Perhaps the most significant privacy risks arise from the digitization of medical and personal health information (hereinafter "PHI"), since such data can reveal an individual's most personal and private information.[2] Privacy and security protections already exist for institutions and industries that traditionally handle medical and personal health information,[3] but

*J.D. Candidate, Suffolk University Law School, 2019.

[1] *See* KATHRYN C. MONTGOMERY ET AL., HEALTH WEARABLE DEVICES IN THE BIG DATA ERA: ENSURING PRIVACY, SECURITY, AND CONSUMER PROTECTION 5 (Am. Univ., School of Commc'n. 2017) (discussing a report that found that current regulatory systems fail to provide adequate safeguards over consumers' personal health information collected by wearable technology); Fouzia F. Ozair et al., *Ethical Issues in Electronic Health Records: A General Overview*, PERSP. IN CLINICAL RES. (Jun. 2015), *archived at* https://perma.cc/NVB5-WVQJ (explaining that patients may be susceptible to improper sharing of personal medical data and that medical providers will have to combat these growing ethical concerns).

[2] *See* Ozair, *supra* note 1 (offering some solutions to securing electronic health record information, such as encryption). Encryption allows for sensitive information to remain private and exclusively accessible to authorized parties. *Id.*

[3] *See* Federal Food, Drug, and Cosmetic Act, Pub. L. No. 75-717, 52 Stat. 1040 (1938), (codified as amended at 21 U.S.C. §§ 301-399 (2012)) (prohibiting the movement of adulterated and misbranded food, drugs, devices, and cosmetics through interstate commerce); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996), (codified as amended at 42

gaps in those protections can emerge with the introduction of new technologies.[4]

For instance, wearable technology is one area where gaps in the protection of medical and personal health information have emerged due to technological progress.[5] Despite the modest origins of wearable technology in the form of devices such as pedometers (which track an individual's step count),[6] wearable watches, bands and clothing are now capable of reading, collecting, storing and analyzing data based on an individual's steps, heart rate, calories burned and much more.[7] The increasing capabilities of wearable technology present the public with the question of how to better protect the individual user's privacy.[8] Moreover, lawmakers will have to decide

U.S.C. § 1320d (2012)) (setting forth the Act's purpose, such as improving portability and continuity of health insurance coverage and simplifying the administration of health insurance).

[4] *See Medical and Genetic Privacy*, AM. CIV. LIBERTIES UNION (Nov. 16, 2017), *archived at* https://perma.cc/8ZKS-GH7B (arguing that threats to privacy and autonomy intensify as medical records become increasingly digitized); *see also Privacy & Technology: What's at Stake*, AM. CIV. LIBERTIES UNION (Nov. 16, 2017), *archived at* https://perma.cc/G4UF-BFAW (stating that, because of technological innovations, a person's "digital footprint" is easily discoverable by the government and corporations).

[5] *See* MONTGOMERY, *supra* note 1, at 116 (acknowledging the privacy issues with wearable technology). Wearable technology devices pose threats to privacy as they are being integrated into data digital health and marketing ecosystems that are designed to gather and monetize personal health data. *Id.*

[6] *See* Samuel Gibbs, *10 Most Influential Wearable Devices*, THE GUARDIAN (Mar. 3, 2017), *archived at* https://perma.cc/W77K-R88G (establishing the pedometer, invented in 1780, as one of the most influential wearable devices in history).

[7] *See* Theresa Hegel, *Wearable Tech Trends for 2017*, ADVERT. SPECIALTY INST. (Jan. 5, 2017), *archived at* https://perma.cc/T5DX-GHQM (describing the development of wearable technology into hubs of body sensors that are increasingly efficient at aggregating and integrating data); Libby Plummer, *Super Bowl 50: How Wearable Tech is Changing the NFL*, WEARABLE (Feb. 6, 2016), *archived at* https://perma.cc/8NKC-XXBX (commenting on new technologies that will affect how football is played, as well as efficiency and safety concerns); 50 *Wearable Tech Gamechangers for 2017*, WEARABLE (Jan. 3, 2017), *archived at* https://perma.cc/7MJM-VYSM (listing 50 new technologies that are likely to make headlines in 2017).

[8] *See* Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, 8 LANDSLIDE 1, 2 (2015) (proposing industry solutions to safeguard privacy and security in the absence of express legislation or regulations around consumer privacy and security for wearables).

whether the data collected by these devices will be protected under current legislation or if new legislation will be needed.[9]

One unique area where this issue appears is professional sports.[10] In April 2017, the National Football League Players Association (hereinafter "NFLPA") entered into an agreement with a Boston-based wearable technology company, Whoop.[11] Under the agreement, the officially licensed NFLPA wearable band will be provided to each NFL player with the goal of studying the effects of travel, sleep, scheduling, and injuries on players' recovery.[12]

---

[9] *See* MONTGOMERY, *supra* note 1, at 5 (emphasizing that policy makers must act to protect consumers in today's big data era).

[10] *See* Tom Goldman, *What's Up Those Baseball Sleeves? Lots of Data, and Privacy Concerns*, NPR (Aug. 30, 2017), *archived at* https://perma.cc/59PU-CCV8 (questioning how increasing amounts of data will be used in baseball); Jeremy Venook, *The Upcoming Privacy Battle over Wearables in the NBA*, THE ATLANTIC (Apr. 10, 2017), *archived at* https://perma.cc/TYB5-UXUQ (analyzing the benefits and risks of increasing the use of wearables in the NBA); Emily Waltz, *Rocky Start for Wearables in Professional Sports Games*, IEEE SPECTRUM (Apr. 15, 2016), *archived at* https://perma.cc/A8WB-WRPN (outlining certain league policies towards the in-game use of wearables).

[11] *See* Bloomberg News, *NFL Players to Use Wearable Device to Monitor Readiness to Play*, HEALTH DATA MGMT. (Apr. 24, 2017), *archived at* https://perma.cc/2K8E-UAJG (noting that the deal between the NFLPA and Whoop is part of a growing trend of sports data being gathered from biometric devices); Arthur Caplan & Lee H. Igel, *Big Whoop About NFL Players Using Wearable Tech, Selling Personal Health Data*, FORBES (Apr. 27, 2017), *archived at* https://perma.cc/R2JD-UBQ7 (identifying issues about privacy that result from the deal between the NFLPA and Whoop); Rajiv Leventhal, *NFL Strikes Deal To Give Players Control of Wearable Data*, HEALTHCARE INFORMATICS (Apr. 28, 2017), *archived at* https://perma.cc/VPY5-5G3Z (explaining the deal between the NFLPA and "human performance company Whoop"); Tom Taylor, *Football's Next Frontier: The Battle over Big Data*, SPORTS ILLUSTRATED (June 27, 2017), *archived at* https://perma.cc/76Y2-ZWXF (identifying risks to players' privacy, autonomy, and confidentiality in the deal between the NFLPA and Whoop).

[12] *See* Bloomberg News, *supra* note 11 (explaining that the Whoop strap measures data 100 times per second and transmits the information to mobile and web applications for analysis); Leventhal, *supra* note 11 (describing the band as a lightweight, waterproof, and screenless device that is worn on the wrist, forearm, or upper arm); *see also NFL Player Contract*, NFL COLLECTIVE BARGAINING AGREEMENT 2011, 145 *archived at* https://perma.cc/F528-PRNM (stipulating in Article 25: "In any League Year, a Club's Active and Inactive Lists shall not exceed 53 players"); *see also* Marc Lillibridge, *The Anatomy of a 53-Man Roster in the NFL*, BLEACHER REPORT (May 16, 2013), *archived at* https://perma.cc/G7SW-MPZE (explaining the NFL rule that teams are allowed to have fifty-three players on their

According to Whoop, the data will provide players, trainers, and coaches with a detailed analysis of the player's body preparedness, while ensuring that each player owns and controls his own data.[13] The more advanced wearable technology becomes, the more personal the data will be that is collected.[14]

This note analyzes how privacy and security issues affect wearable technology companies and their users. As a case study, this Note will analyze the agreement between the NFLPA and Whoop: Section II discusses the history of health data protection legislation,[15] Section III discusses the history of wearable technology and health data,[16] Section IV analyzes how current law applies to the agreement between the NFLPA and Whoop, [17] and Section V proposes modifications and additions to current law that may address privacy and security concerns.[18]

II. History of Health Data Protection Legislation

This section examines the laws that may be implicated by the development of new wearable technologies, including The Food, Drug, and Cosmetic Act;[19] the Stored Communications Act;[20] and the Health Insurance Portability and Accountability Act and the Health

active roster, forty-six of which can actually dress for the game); *see also NFL Standings - 2018*, ESPN (Feb. 7, 2019), *archived at* https://perma.cc/GJ29-FUDX (listing the thirty-two teams in the NFL as of 2018 by division).

[13] *See* Bloomberg News, *supra* note 11 (declaring that players will own and control their own data, with the ability to sell it or keep it private); Kelly J. O'Brien, *Boston Startup Scores in Deal that Will Give its Wearable to Every NFL Player*, BOSTON BUS. J. (Apr. 25, 2017), *archived at* https://perma.cc/5H2G-SXVQ (noting that Whoop will "co-own" player health data).

[14] *See* Goh, *supra* note 8, at 1 (emphasizing the volume and sensitivity of data that will be collected as more wearable devices and sensors are introduced into clothes, shoes, and accessories).

[15] *See infra* Section II.

[16] *See infra* Section III.

[17] *See infra* Section IV.

[18] *See infra* Section V.

[19] *See infra* Section II, A (focusing on FDA regulation of medical devices).

[20] *See infra* Section II, B (narrowing the regulatory focus to electronic communications).

Information Technology for Economic and Clinical Health Act.[21]

A. FDA & Medical Devices

The Food and Drug Administration ("FDA") has broad authority to regulate products marketed to the public.[22] Recently, however, the Administration has taken a "hands-off approach" to the technology industry to foster the development of new products without oppressive regulation.[23] The FDA is limited to the regulation of "medical devices," due to the Food, Drug and Cosmetic Act ("FDCA").[24] The statute defines medical devices as "any product intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, or intended to affect the structure or any function of the body."[25] Accordingly, the

[21] *See infra* Section II, C (noting the congressional response to the digitization of medical records).

[22] *See What We Do*, U.S. FOOD & DRUG ADMIN. (Apr. 4, 2017), *archived at* https://perma.cc/QC7M-8DF7 (articulating that the responsibility of the FDA is to protect the public health by ensuring the safety, efficacy, and security of drugs, biological products, and medical devices).

[23] *See* Adam Satariano, *FDA 'Taking a Very Light Touch' on Regulating the Apple Watch*, BLOOMBERG (Mar. 30, 2015), *archived at* https://perma.cc/RGW5-HFBM (announcing the FDA's policy to give the technology industry leeway to develop new products without aggressive regulation).

[24] *See* Federal Food, Drug, and Cosmetic Act, Pub. L. No. 75-717, 52 Stat. 1040 (1938), (codified as amended at 21 U.S.C. §§ 301-399 (2012)) (defining and outlining medical devices intended for human use).

[25] *See* Definitions; generally, 21 U.S.C. § 321(h)(2)-(3) (2012) (defining "device").

> (h) The term "device" . . . . means an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is . . . .
> (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
> (3) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 520(o) [21 USCS § 360j(o)].

FDA can only regulate consumer wearables if they meet the statutory definition of medical devices.[26]

In response to the rapid expansion and broad use of mobile phone applications, the FDA has been forced to clarify its regulation of certain mobile devices.[27] While an overarching software policy has not been issued, the FDA has classified some software applications that meet the definition of a device and therefore fall under certain regulatory requirements of the FDA.[28] Mobile phone applications will be regulated if they are intended to 1) be used as an accessory to a regulated medical device; or 2) transform a mobile platform into a regulated medical device.[29]

The extension of FDA regulatory power, however, will not extend to applications that are considered "low risk."[30] Whether these devices and associated apps will be considered medical devices, depends on the "intended use" of the product.[31] The FDA defines "intended use" as the "objective intent of the persons legally responsible for the labeling of devices" that is shown through "labeling claims, advertising matter, or oral or written statements."[32] Still, the distinction between medical devices and general health and wellness

---

Id.

[26] *See* Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1649 (2015) (explaining how the definition of "device" limits regulation by the FDA).

[27] *See* U.S. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 7 (2015) (distinguishing which mobile applications are considered medical devices).

[28] *See id.* at 6 (detailing that stand-alone software used to analyze medical device data is traditionally regulated as an accessory to a medical device or as medical device software).

[29] *See id.* at 8 (emphasizing that the intended use of a mobile application determines whether it meets the definition of a "device").

[30] *See id.* at 12 (noting that the FDA intends to exercise enforcement discretion over certain medical devices because they pose a low risk to patients).

[31] *See* Vincent J. Roth, *The mHealth Conundrum: Smartphones & Mobile Medical Apps—How Much FDA Medical Device Regulation is Required?*, 15 N.C. J. OF L. & TECH. 359, 371-72 (2014) (distinguishing between medical devices intended to be used for medical purposes and medical devices intended to be used to promote or encourage general health or wellness).

[32] *See* Meaning of intended uses, 21 C.F.R. § 801.4 (2018) (defining objective intent of persons labeling devices).

products is not always clear.[33] Ultimately, the primary purpose of the FDA is not to safeguard individual privacy, but to protect public health.[34] In the end, it is unlikely that the FDA will treat consumer wearables as medical devices as most are advertised to promote health and not to treat medical conditions.[35]

B. The Stored Communications Act (SCA)

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA").[36] One of the sections of the ECPA was the Stored Communications Act ("SCA"), which created protections for electronic communications, extended privacy protections to e-mails and information stored by third parties, and established rules about when entities may disclose their customers' communications records.[37] Section 2702 of the SCA governs when providers can and cannot disclose information to commercial third parties, applying only to persons or entities that provide electronic communication service or remote computing service.[38]

Two determinations govern whether the SCA applies to consumer wearables: 1) if the health apps provide either electronic communication service or a remote computing service; and 2) if so,

---

[33] *See* Langley, *supra* note 26, at 1649 (providing an example of a medical devices used by an overweight person to assist with exercise and weight management or to treat the medical condition of obesity).

[34] *See* Langley, *supra* note 26, at 1650 (suggesting that the FDA does not provide a viable solution to privacy problems regarding consumer wearables since the FDA appears unwilling to regulate purely commercial products).

[35] *See* Langley, *supra* note 26, at 1649-50 (recognizing that the FDA could still regulate health-app companies that provide software for wearables); *see also* Roth, *supra* note 31, at 372 (suggesting that new technological progress may warrant a new paradigm).

[36] *See* Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986), (codified as amended at 18 U.S.C. §§ 2701-2712 (2012)) (preventing authorized government access to private electronic communications).

[37] *See* Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2012) (addressing the disclosure of electronic communications stored with technology providers).

[38] *See* Stored Communications Act § 2702 (listing persons or entities that cannot divulge the contents of communications, such as those providing an electronic communication, providing remote computing service, or a provider of remote computing service).

whether the communications are considered content or non-content.[39] "Electronic communications" are defined by the SCA as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[40] "Remote computing service," on the other hand, is defined by the SCA as "the provision to the public of computer storage or processing services by means of an electronic communications system."[41]

Under section 2702(c) of the SCA, providers "may divulge a record or other information pertaining to a subscriber to or customer of such service . . . . to any person other than a government entity" with no restriction.[42] Additionally, providers can sell the data without notifying the individual or obtaining the individual's consent if the data are considered "non-content."[43] The data will be protected only if it is considered "content," and the definition of "content" appears to hinge on whether the user intended the communication.[44] It is very unlikely that data collected and stored by wearable technology would be considered content, or that the wearer of that device would consider such content to be communication.

C. The Health Insurance Portability and Accountability Act (HIPAA) & the Health Information Technology for Economic and Clinical Health ("HITECH") Act

Most recently, in 1996, Congress responded to the increased digitization of data in the healthcare industry by passing the Health Insurance Portability and Accountability Act ("HIPAA").[45] This Act

[39] *See* Stored Communications Act § 2702 (allowing *voluntary* disclosure in limited circumstances).
[40] *See* Stored Communications Act § 2510(15) (defining electronic communication service as applied to the Stored Communications Act).
[41] *See* Stored Communications Act § 2711(2) (defining remote computing service).
[42] *See* Stored Communications Act § 2702(c)(6) (listing one of the providers in subsection (a) that may divulge customer records).
[43] *See* Stored Communications Act, 18 U.S.C. §§ 2702(c)(6) (2012) (allowing content of communications not covered in subsection (a)(1) or (a)(2) to be disclosed to non-governmental agencies).
[44] *See* Graf v. Zynga Game Network, Inc., 750 F.3d 1098, 1106 (9th Cir. 2014) (arguing that Congress intended the word "contents" to mean a person's intended message to another).
[45] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996), (codified as amended at 42 U.S.C. § 1320d (2012))

essentially codified the Hippocratic Oath,[46] intending to ease the growing concern among patients regarding the confidentiality of personal health information in an outdated paper record system.[47] Accordingly, HIPAA mandated nationwide security standards and safeguards for the use of electronic health care information and the creation of privacy standards for protected health information.[48]

Decades later, to promote the adoption and meaningful use of health information technology, Congress reinforced HIPAA when it passed the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009.[49] Additionally, the HIPAA Omnibus Rules enacted after the HITECH Act added and expanded

(explaining the purpose of the Act was to improve the industry of health insurance coverage).

[46] *See* Langley, *supra* note 26, at 1647 (declaring that in passing HIPAA, "[c]ongress essentially codified the Hippocratic Oath" by protecting individuals' privacy of personal health information); *see also* Peter Tyson, *The Hippocratic Oath Today*, PBS (Mar. 27, 2001), *archived at* https://perma.cc/H6BB-STYB (providing the modern version of the Oath in which doctors swear to "respect the privacy of my patients, for their problems are not disclosed to me that the world may know.").

[47] *See* James Blake Hike, *An Athlete's Right to Privacy Regarding Sport-Related Injuries: HIPAA and the Creation of the Mysterious Injury*, 6 IND. HEALTH L. REV. 47, 51 (2009) (adding that the Act sought to address concerns, such as where patient medical information was going and who had access to it); Timothy Newman & Jennifer Kreick, *The Impact of HIPAA (and Other Federal Law) on Wearable Technology*, 18 SMU SCI. & TECH. L. REV. 429, 431 (2015) (explaining that HIPAA regulations incorporate privacy and security protections for individually identifiable health information).

[48] *See* INST. OF MED. OF THE NAT'L ACAD., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 63 (Sharyl J. Nass et al. eds., 2009) (laying out a brief history of HIPAA and its goals of making health care more efficient); *see also* OFFICE OF CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVICES, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE 8 (2012) (providing guidance about methods and approaches to re-identifying PHI in accordance with HIPAA).

[49] *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009), (codified as amended at 42 U.S.C. § 17938 (2009)) (creating incentives related to health care information technology); *see also* Newman & Kreick, *supra* note 47, at 432 (explaining that concerns regarding the privacy and security of electronic health information persisted after the passing of the HITECH Act, which prompted Health and Human Services to strengthen certain HIPAA provisions).

security procedures focusing on electronic data.[50] Most notably, the new laws and regulations expanded the application of HIPAA to cover "business associates" of covered entities and strengthened the civil and criminal enforcement of HIPAA rules.[51]

Pursuant to HIPAA, the U.S. Department of Health and Human Services ("HHS") promulgated regulations that can be separated into the "Privacy Rule"[52] and the "Security Rule."[53] Both Rules aim to protect the privacy of the individual's personal health information by limiting disclosure of such information.[54] The reach of the regulations, however, extends only to individuals, organizations, and agencies that meet the definition of "covered entity" or "business associate."[55] The regulations only apply to these individuals, organizations, or agencies if they maintain or transmit personal health information PHI, which includes any individually identifiable information that relates to an individual's physical or mental health or has provision of or payments for healthcare.[56]

Under the HHS regulations, a "covered entity" is defined as 1)

---

[50] *See* Cristina M. Mares, *To Cover or Not to Cover? The Relationship Between the Apple Watch and the Health Insurance Portability and Accountability Act*, 18 DEPAUL J. HEALTH CARE L. 159, 170 (describing the changes resulting from the HITECH Act and the HIPAA Omnibus Rules).

[51] *See id.* at 172 (discussing the impact of the HITECH Act on HIPAA); *see also* Langley, *supra* note 26, at 1648 (noting the expanded jurisdictional element of HIPAA to include "business associates" of covered entities).

[52] *See* 45 C.F.R. §§ 160.101 & 164.104 (2018) (outlining the standards for privacy and security rules); *see also* MAURICIO PAEZ, 2-32 CORPORATE COMPLIANCE PRACTICE GUIDE § 32.03 (Carol Basri ed., 2018) (highlighting that the Privacy Rule regulates the use and disclosure of personal health information in any form held by covered entities and their business associates).

[53] *See* 45 C.F.R. §§ 160.103 & 164.306 (2018) (stating the general provisions for security and privacy); *see also* PAEZ, *supra* note 52 (describing how the Security Rule complements the Privacy Rule by dealing specifically with electronic personal health information).

[54] *See* Langley, *supra* note 26, at 1648 (clarifying that numerous safeguards protect all individually identifiable health data once an organization is deemed a covered entity under HIPAA).

[55] *See Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SRVS. (June 16, 2017), *archived at* https://perma.cc/4SWX-KLBH (explaining that entities that do not meet the definition of a covered entity or business associate do not have to comply with the HIPAA Rules).

[56] *See* Mares, *supra* note 50, at 162 (asserting that federal privacy laws have a limited reach regarding PHI stored on consumers' personal devices).

a health plan; 2) a health care clearinghouse; or 3) a health care provider that transmits any health information in electronic form.[57] A "business associate" is defined as any person or entity that creates, receives, maintains or transmits PHI on behalf of a covered entity.[58] Further, covered entities that work with business associates must create a written business associate agreement ("BAA") that requires the business associate, through its relationship with the covered entity, to comply with HIPAA.[59] It is possible for a covered entity to be a business associate of another covered entity.[60] For instance, health care providers and health plans often use the services of a variety of other persons or business to carry out health care activities and functions.[61]

The Privacy Rule requires covered entities and business associates to establish appropriate safeguards to protect PHI.[62] Furthermore, the Privacy Rule sets limits and conditions on the uses and disclosures of PHI without the individual's authorization.[63] Covered entities and business associates are liable for unauthorized disclosure of PHI regardless of whether the disclosure was intentional or due to negligence,[64] and such organizations must ensure the confidentiality, integrity and availability of all electronic personal health information ("ePHI") that they create, receive, maintain or transmit.[65] Accordingly, the regulations require these entities to protect against any reasonably anticipated threats or hazards to security or integrity of any ePHI created, received, maintained or transmitted

[57] *See* 45 C.F.R. § 160.103 (defining "covered entity").
[58] *See* 45 C.F.R. § 160.103 (declaring the meaning of "business associate").
[59] *See* Mares, *supra* note 50, at 163 (2016) (describing the agreement as establishing specifically what the business associate has been engaged to do).
[60] *See* 45 C.F.R. § 160.103 (2018) (recognizing what is required to be a business associate of another covered entity).
[61] *See Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SRVS. (July 26, 2013), *archived at* https://perma.cc/GD6X-BNFW (emphasizing that business associate agreements must contain the elements specified at 45 CFR § 164.504(e)).
[62] *See* PAEZ, *supra* note 52 (noting that the Privacy Rule requires covered entities to comply with certain administrative requirements).
[63] *See* Mares, *supra* note 50, at 165 (explaining the limited protection of PHI stored on wearable devices such as the Apple Watch).
[64] *See* Mares, *supra* note 50, at 165 (explaining the various interests in personal health information).
[65] *See* Mares *supra* note 50, at 166 (emphasizing the breadth of requirements for covered entities and business associates).

by them.[66] If wearable device manufacturers or companies using wearable devices were to be considered either "covered entities" or "business associates," they would be required to adhere to HIPAA regulations.

III. Premise

A. Wearable Technology & Health Data

From the humble origin of the pedometer, wearable technology today is capable of reading and collecting a variety of measurements, including sensitive vital sign information.[67] The devices collecting this information now come in the form of watches, glasses, belts, shirts, shoes and jewelry.[68] Additionally, these devices have the ability to be worn 24/7 – while sleeping, exercising and showering.[69] While many of the advanced features included on today's wearable technology were originally used for medical purposes, the devices have become more functional, focusing more on ordinary daily lifestyle, health, and exercising.[70] In fact, today's wearables often have little to do with medical necessity and more to do with tracking health and fitness levels.[71]

In addition to individual consumers, employers are utilizing these devices to encourage healthy lifestyles for their workers.[72] Pharmaceutical and biotechnology companies are also beginning to

[66] *See* Mares, *supra* note 50, at 166 (highlighting the requirement of health care providers to implement stringent security measures to protect patient information).
[67] *See* Langley, *supra* note 26, at 1642 (emphasizing how companies are collecting an enormous amount of individual data).
[68] *See* Joanna Stern, *Where to Wear Your Technology? Torso to Toe*, WALL STREET J. (Jan. 7, 2014), *archived at* https://perma.cc/C42C-CR5G (describing the new crop of wearable technology that can be worn all over the human body).
[69] *See* Langley, *supra* note 26, at 1644 (describing wearable technology as computerized clothing or accessories that can be worn on the user's body).
[70] *See* Langley, *supra* note 26 (noting the medical devices such as blood-pressure monitors, heart-rate monitors, and stress detectors as being wearable technology).
[71] *See* Langley, *supra* note 26 (highlighting that today's wearable technology has little to do with medical necessity but rather aim to recreationally track health and fitness levels).
[72] *See* Mares, *supra* note 50, at 162 (discussing the balancing effort of protecting personal health information without hindering innovation).

utilize wearable technology for research trials.[73] Still, the data that is being collected, stored, and transmitted by today's wearable technology in both consumer and professional environments is becoming increasingly personal.[74]

The technology has advanced beyond simply monitoring health and wellness and will likely face increased scrutiny and complex regulation that may create additional liability for developers and subscribers.[75] The increased use of biometrics, which is automated methods of identifying or recognizing individuals based on one or more unique characteristics, increases the value of the collected data.[76] Such data may be exploited for financial and commercial gain, which would create additional concerns for regulators and lawmakers, not to mention the consumers themselves.[77]

According to the International Data Corporation, shipments of wearable devices increase from 104 million in 2016 to 125 million in 2017.[78] By 2021, the market is expected to double to 240 million units shipped.[79] These growth projections only enhance the complexity and severity of privacy and security concerns carried by wearable devices.[80] Moreover, the increasing sophistication of technology will impact the application of current legislation on new technologies such

[73] *See* Mares, *supra* note 50, at 175 (highlighting 299 clinical trials using wearables).
[74] *See* Langley, *supra* note 26, at 1645-46 (describing how wearables collect data about the user and wirelessly send the information to smartphones and applications).
[75] *See* Newman & Kreick, *supra* note 47, at 430-31 (noting Fitbit's announcement that it would comply with HIPAA when collecting even more sensitive information).
[76] *See* Sharon Roberg-Perez, *The Future is Now: Biometric Information and Data Privacy*, 31 A.B.A. ANTITRUST 3 (2017) (explaining that behavioral characteristics such as one's heartbeat can be used to identify individuals based on data).
[77] *See* Langley, *supra* note 26, at 1646 (illustrating how marketers could use the data to personally target products and sports equipment manufacturers could use the data to offer clothes depending on fitness activity).
[78] *See Worldwide Wearables Market to Nearly Double by 2012, According to IDC*, IDC (June 21, 2017), *archived at* https://perma.cc/82YS-CD9A (projecting the rate of growth in the wearables market).
[79] *See id.* (noting that watches will account for a majority of the growth while wristbands will see a slower development).
[80] *See* Roberg-Perez, *supra* note 76, at 64 (explaining that companies looking into biometric information should closely monitor legal developments and jurisdictional differences in regulation since "things are bound to get more and more interesting").

as wearables.[81]

B. The Agreement—NFLPA & Whoop

In April of 2017, the NFLPA became the first players' association in professional sports to partner with a wearable technology company.[82] The company that the NFLPA partnered with, Whoop, is marketed as the first product engineered to unlock human performance.[83] Under the deal, the players were provided easy access to, ownership of, and the option to commercialize their health data.[84] Notably, the players will own and control their individual data, and design their own custom licensed bands.[85]

Under the agreement, the NFLPA and Whoop will study how travel, sleep schedules, injuries, and other factors affect recovery, and will generate reports in order to advance player safety and maximize athletic performance.[86] Additionally, NFL players will have the ability to commercialize their data through the NFLPA's licensing program.[87] Yet, these features raise concerns about players' privacy and security of their personal health information that is generated,

[81] *See* Roth, *supra* note 31, at 406 (noting the complexity of the regulatory environment and the guesswork involved when complying with FDA regulations).
[82] *See WHOOP Strikes Landmark Deal as the Officially Licensed Recovery Wearable of the NFL Players Association*, NAT'L FOOTBALL LEAGUE PLAYERS ASS'N (Apr. 24, 2017), *archived at* https://perma.cc/S6LT-AN4P [hereinafter "*WHOOP Strikes Landmark Deal*"] (outlining the deal struck between the NFLPA and WHOOP).
[83] *See* Will Ahmed, *Our Mission: Unlock Human Performance*, WHOOP (Nov. 19, 2017), *archived at* https://perma.cc/RX2K-W6XE (admitting that the data collected by Whoop is unprecedented in both sophistication and scale).
[84] *See WHOOP Strikes Landmark Deal*, *supra* note 82 (explaining that this arrangement is the first time that a professional sports players association has partnered with a wearable technology company).
[85] *See WHOOP Strikes Landmark Deal*, *supra* note 82 (noting that players will have custom designed bands for personal use and commercial sale).
[86] *See WHOOP Strikes Landmark Deal*, *supra* note 82 (emphasizing that such study will produce data that can translate into physiological and financial opportunities for the players).
[87] *See WHOOP Strikes Landmark Deal*, *supra* note 82 (describing this arrangement as the first step in harnessing the exciting new innovative and holistic monitoring technology).

gathered, stored, and transmitted by the Whoop strap.[88] The application of current laws, such as the FDCA, the SCA, HIPAA and HITECH, to the agreement between the NFLPA and Whoop will be difficult to predict, but must nonetheless be explored.[89]

IV. An Analysis: How Does Current Law Apply to the NFLPA and WHOOP?

The Whoop Strap is a good example of how new technologies are creating difficult regulatory and legal environments for consumers, developers and manufacturers, and this section discusses if and how the Agreement between the NFLPA and Whoop may be affected by the FDCA,[90] the SCA,[91] HIPAA and the HITECH Act.[92]

A. FDA & Medical Devices

As discussed above, the FDA's authority under the FDCA is limited to the regulation of "medical devices."[93] For wearable devices like the Whoop Strap to be considered "medical devices," they must be intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease.[94] Furthermore, the Whoop strap will be considered a medical device if

[88] *See WHOOP Strikes Landmark Deal*, *supra* note 82 (pointing out, however, that Whoop has developed "27 levels of privacy" to make sure that data is safe and secure); *but see* Frank Sivilli, *HIPAA Breach Affects Thousands of Current, Former NFL Players*, MEDCITYNEWS (June 2, 2016), *archived at* https://perma.cc/8BUV-9GAC (noting that the trainer's paper and computer records dated back thirteen years and reportedly included current and former players' protected health information as well as that of the attendees of the annual Scouting Combine). These records were breached despite safety measure. *Id.;* Hoala Greevy, *HIPAA Compliance and the NFL (National Football League)*, PAUBOX (Apr. 5, 2017), *archived at* https://perma.cc/RNR3-339X (stating an incident where a laptop was stolen).
[89] *See infra* Section V.
[90] *See infra* Section V, A.
[91] *See infra* Section V, B.
[92] *See infra* Section V, C.
[93] *See* Federal Food, Drug, and Cosmetic Act, Pub. L. No. 75-717, 52 Stat. 1040 (1938), (codified as amended at 21 U.S.C. §§ 301-399 (2012)) (acknowledging that sponsors of medical devices are among one of the classes of subjects listed that the FDA has authority over under the FDCA).
[94] *See id*. (detailing what must exist for something to be deemed a medical device).

it is intended to affect the structure or any function of the body.[95]

In addition to the strict limitations of authority granted to the FDA under the FDCA, the FDA's decision to take a "hands-off approach" to new technologies like wearables makes it even more unlikely that such devices will be regulated by the FDA.[96] The software used by Whoop to gather, analyze, and store players' data will only be regulated if intended to be used as an accessory to a regulated medical device or to transform a mobile platform into regulated medical device.[97] Ultimately, the "intended use" of a product is crucial in determining whether a product will be considered a medical device.[98] From Whoop's own description of its product, we can see that its "intended use" is to advance player safety and maximize athletic performance.[99] However, while the distinction between medical devices and general health and wellness products are not always clear, the FDA's primary purpose is to protect public health and not safeguard privacy.[100] Thus, it is unlikely that the Whoop Strap would be considered a "medical device" or that the FDA would regulate such products to protect public health.[101] Therefore, alternative routes of regulation are necessary.

B. The SCA

As discussed above, the Stored Communications Act was

[95] *See* 21 U.S.C. § 321 (h)(2)-(3) (2012) (defining device as an "instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article").

[96] *See* Satariano, *supra* note 23 (noting the agency's decision to allow the industry to develop new products without aggressive regulation).

[97] *See* U.S. FOOD & DRUG ADMIN., *supra* note 27 (explaining when and how "mobile medical apps" meet the definition of device in section 201(h) of the Food, Drug, and Cosmetic Act)

[98] *See* Roth, *supra* note 31, at 406 (distinguishing products used for medical purposes and those used to promote general health or wellness).

[99] *See WHOOP Strikes Landmark Deal*, *supra* note 82 (describing the deal between the NFLPA and Whoop and the purposes of NFL players wearing the Whoop Strap).

[100] *See* Langley, *supra* note 26, at 1647 (suggesting that the FDA does not provide the appropriate avenue to solving privacy issues).

[101] *See* Langley, *supra* note 26, at 1647 (stating that the FDA is unable to provide effective oversight to wearables since such devices are being used as consumer products rather than medical devices).

enacted in order to protect electronic forms of communications.[102] In order for the Act to apply to consumer wearables like the Whoop Strap, the software must provide either electronic communication services or remote computing services.[103] Furthermore, if the software does provide such services, then the communications must be considered "content."[104] The Whoop Strap does not provide its users "electronic communication" service because it does not provide them with the ability to send or receive wire or electronic communications.[105] However, Whoop may provide remote computing services, which are defined as the provision of "computing storage or processing services by means of an electronic communications system."[106]

Even if Whoop's services were considered remote computing services, however, the SCA does not apply to its wearable bands because the communications transmitted are not considered "content."[107] If NFL players used the Whoop Strap, the users would only wear the bands and utilize Whoop's platform in order to transmit health data that may help enhance their performance.[108] Accordingly, health data information regulation may be the only avenue to ensure protection and privacy of NFL players' personal health information

[102] *See* Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2012) (criminalizing the unlawful access to, and disclosure of, stored communications)

[103] *See* Stored Communications Act § 2711 (defining remote computing service as the provision to the public of computer storage or processing services by means of an electronic communications system).

[104] *See* Stored Communications Act § 2702 (establishing the prohibitions on disclosure of customer communications or records).

[105] *See* Stored Communications Act § 2510(15) (Defining: [An] "electronic communication" [is] "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.").

[106] *See* Stored Communications Act § 2711(2) (providing definitions for the statute that governs privacy).

[107] *See* Graf v. Zynga Game Network, Inc., 750 F.3d 1098, 1106 (9th Cir. 2014) (emphasizing that whether a communication is considered "content" turns on whether the user intended the communication).

[108] *See WHOOP Strikes Landmark Deal*, *supra* note 82 (describing the deal between the NFLPA and Whoop and the purposes of NFL players wearing the Whoop Strap).

under the agreement between the NFLPA and Whoop.[109]

C. HIPAA

With thirty-two teams in the NFL, and up to fifty-three players on each team, the NFL and the NFLPA are responsible for the PHI of almost 1,700 athletes.[110] The risk associated with this responsibility was evident in 2016 when thousands of players' healthcare records were breached after a laptop was stolen from the car of a Washington Redskins trainer.[111] In an official statement from the NFL to the NFLPA, it was admitted that while the stolen laptop was password protected, it's hard drive was not encrypted.[112] Despite industry-wide pushes for electronic health record adoption and migration away from paper records, privacy and security of such records cannot be increased without accompanying encryption and privacy measures.[113]

In light of the nationwide security standards and safeguards imposed by HIPAA, the HITECH Act, and the HIPAA Omnibus Rules regarding electronic health care information, breaches such as the one described above may have implications with HHS.[114] First, HIPAA attempted to ease concerns regarding the confidentiality of PHI by mandating nationwide security standards and safeguards for the use of ePHI and creating privacy standards.[115] More recently, the HITECH

---

[109] *See infra* V, C. (discussing the implications of HIPAA on the agreement between the NFLPA and Whoop).

[110] *See NFL Player Contract*, supra note 12, at 145 (reinforcing the number of players per team); *see also* Marc Lillibridge, *supra* note 12 (explaining that forty-six are active and dressed for the game); *see also NFL Standings*, *supra* note 12 (restating that 32 teams are in the NFL).

[111] *See* Sivilli, *supra* note 88 (articulating that breaches are possible).

[112] *See* Greevy, *supra* note 88 (providing the text of NFLPA Executive Director's letter stating that "the backpack contained a password protected, but unencrypted, laptop that had copies of the medical exam results for NFL Combine attendees from 2004 until present").

[113] *See* Sivilli, *supra* note 88 (addressing how the breach provided the Department of Health and Human Services an opportunity to make a decisive statement on the adoption of electronic health records and rights of privacy for patients, and emphasizing that over 112 million Americans had their health data breached in 2015 alone).

[114] *See* Nass, *supra* note 48, at 2 (noting the policy goal of ensuring proper protection while allowing the flow of information needed to promote high-quality health care).

[115] *See* Nass, *supra* note 48, at 63 (laying out a brief history of HIPAA).

Act of 2009 and the HIPAA Omnibus Rules prompted HHS to strengthen HIPAA provisions focusing on electronic data and expanding the reach of HIPAA to "business associates" of covered entities.[116] Accordingly, disclosing protected health information will be regulated by HHS, depending on the designation by HHS of the entity that discloses the information.[117] To determine whether the Privacy Rule or Security Rule would apply to the NFLPA or Whoop, it must first be determined whether either organization is a "covered entity" or a "business associate."[118]

Under the NFL's 2011 Collective Bargaining Agreement ("CBA"), each club is required to have certain board-certified medical personnel who must comply with all federal, state and local requirements governing the medical profession in the city where the Club is located.[119] Under the language of the CBA, each NFL club and the NFLPA would likely be considered a "covered entity," which includes health plans, health care clearinghouses and health care providers.[120] Under HIPAA regulations, "health care providers" are defined as "providers of services, providers of medical or health services, and any other person or organization that furnishes, bills or is paid for health care in the normal course of business."[121] Thus, under the language of the CBA, it appears that individual NFL clubs and the NFLPA as a whole could be considered "covered entities."

In the agreement between the NFLPA and Whoop, Whoop would likely be considered a "business associate" of the NFLPA and/or individual NFL clubs since Whoop creates, receives, maintains

---

[116] *See* Mares, *supra* note 50, at 171 (discussing the impact of the HITECH Act on HIPAA); *see also* Langley, *supra* note 26, at 1648 (noting the expanded jurisdictional element of HIPAA to include "business associates" of covered entities).

[117] *See* Nass, *supra* note 48, at 2 (explaining that the Privacy Rule sets forth detailed regulations regarding the types of uses and disclosures of individuals' personally identifiable health information permitted by covered entities).

[118] *See Covered Entities and Business Associates*, *supra* note 55 (stating that if an entity does not meet the definition of covered entity or business associate, it does not have to comply with the HIPAA Rules).

[119] *See NFL Player Contract*, *supra* note 12, at 172 (highlighting section titled "Players' Rights to Medical Care and Treatment").

[120] *See* 45 C.F.R. § 160.103(1)(i)-(ii) (2018) (defining "covered entity").

[121] *See* 45 C.F.R. § 160.103(4)(i) (stating that a health care provider is not considered a business associate).

and/or transmits PHI on behalf of clubs.[122] Whoop not only provides the wearable band that collects the data, but it also analyzes that data and provides analysis about the players' health and recovery.[123] However, one crucial question is whether the data created, gathered, analyzed and exchanged between the NFL players and Whoop is truly PHI.

According to the regulations, PHI includes any individually identifiable information that relates to an individual's physical or mental health or has provision of or payments for healthcare.[124] This could be information relating to: 1) an individual's past, present, or future physical or mental health or condition; 2) the provision of healthcare to the individual; or 3) past, present, or future payment for the provision of health care to the individual.[125] While it may be argued that the information gathered by Whoop is simply fitness-oriented, there is no denying that the data is more complex and detailed than ever before.[126] Thus, organizations like Whoop and the NFLPA must not only keep the relevant laws and regulations in mind when introducing new technologies like the Whoop Strap, but, at some point, the law must also respond to the increased risk that such detailed and personal data presents when left unprotected.[127]

V. Conclusion

While HIPPA provides the most conducive avenue to protect the data collected on wearable devices such as the Whoop Strap, all three laws are equally as important for facilitating effective and meaningful regulation of this new and growing industry. Although the

[122] *See* 45 C.F.R. § 160.103 (noting that "business associate" does not include health care providers, plan sponsors, government agencies, or a covered entity participating in an organized health care arrangement that performs a function or activity).
[123] *See WHOOP Strikes Landmark Deal*, *supra* note 82 (outlining the deal struck between the NFLPA and WHOOP).
[124] *See* Mares, *supra* note 50, at 162 (asserting that federal privacy laws have a limited reach regarding PHI stored on consumers' personal devices).
[125] *See* OFFICE OF CIVIL RIGHTS, *supra* note 48 (outlining what constitutes regulated PHI).
[126] *See* Newman & Kreick, *supra* note 47, at 430 (noting Fitbit's announcement that it would comply with HIPAA when collecting even more sensitive information).
[127] *See* Bloomberg, *supra* note 11 (explaining that the Whoop strap measures data 100 times per second and transmits the information to mobile and web applications for analysis).

agreement between Whoop and the NFLPA distinguishes ownership and marketing rights of the data, the increasing sensitivity of that data will still create risks of disclosure. Ultimately, the wearable tech industry, professional sports organizations, and ordinary consumers must be aware of the inherent risks that come with such advanced technology. State legislatures across the county, the United States Congress, and federal agencies must ensure that protections are enforced for sensitive data such as PHI. Let us hope that such action occurs before, rather than in response to, the next breach or disclosure of PHI.