WRISTWATCHES OF RUIN: FITNESS WEARABLES AND THE HIPAA PRIVACY RULE

Dana Holmstrand and Samuel P. Taylor

INTRODUCTION

You wake with a start as your wrist buzzes. Tapping your Fitbit to quiet it, you open your phone to see how the wearable has assessed last night's sleep quality. Your Fitbit accompanies you on your morning jog, cheerfully providing real time heart rate updates urging you to go faster and counting calories as fast as you burn them. Your Fitbit captures your brisk walk to the metro as steps rise toward the elusive 10,000 that you strive for each day. Your choice to take the stairs rather than the elevator is evidenced by an increased respiratory rate—also captured by Fitbit. You slide into your desk already excited to log those breakfast calories in the Fitbit app. The quantified self is already at work, and it is not even 9:00 am.

These vignettes show the many ways fitness wearables generate unique health information, which the companies then sell and share with third parties often unbeknownst to users. The amount of information is vast and valuable. An estimated 20% of Americans use some kind of fitness wearable,[1] a device that collects information that would otherwise only be available in a hospital. Advertisers, insurers, lenders, and employers seek to capitalize on this unique information to sell more product, insure healthier clients, and surveil employees, all without the user's awareness of their data's use.[2]

This Essay aims to shed light on the laws and regulations that allow this sale and invasive use of health information. First, we will discuss the inherent sensitivity of health information by discussing the kinds of information fitness wearables collect and the harms if such information is exposed. Next, we will explain why the current U.S. health privacy framework fails to cover fitness wearables and the enforcement problems this creates. Finally, we offer broad principles that legislators and regulators should adopt when seeking to close the fitness wearable loophole.

---

[1] Emily Vogels, *About one-in-five Americans use a smart watch or fitness tracker*, PEW RESEARCH CENTER (Jan. 9, 2020), https://www.pewresearch.org/fact-tank/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker.

[2] A.J. Perez, *Use a fitness app to track your workouts? Your data may not be as protected as you think*, USA TODAY (Aug. 16, 2019), https://www.usatoday.com/story/sports/2019/08/16/what-info-do-fitness-apps-keep-share/1940916001.

HEALTH INFORMATION IS UNIQUELY SENSITIVE

The right to privacy, from both private and public actors, is necessary for a fulfilling personal life.[3] Fundamental to that right is the ability to control to whom, when, or if we disclose private information.[4] The increasingly networked world and the Internet of Things (IoT) has made it easier for revealing information to flow from users to the wider world,[5] and IoT devices that collect health information risk the wide dissemination of information that is particularly sensitive.

Compare health information with credit card purchase history. A quick review of someone's purchases may reveal the geographic location of the cardholder.[6] It may also imply socio-economic status: a purchaser who frequents secondhand clothing stores or who has purchased retread tires may be considered less economically secure, in turn lowering their credit score.[7] Health information is even more revealing. Rather than just reflecting how an individual interacts with wider society or their credit score, health information can reveal facts about the data subject that are entirely internal: the strength of a person's heart or the quality of their lungs. A routine physical, among the least invasive medical practices, collects intimate details of the patient's life—substance abuse, sexuality, and mental health conditions—information not readily gleaned by the naked eye.[8] The trust relationship between a doctor and patient reflects this sensitivity: patients open up to their physicians because they believe their information will remain private.[9] Additionally, we construct physical and psychological markers that reflect and honor the sensitivity of information that passes from patient to physician: closed doors, individual examination rooms, and the patient's power to determine who is in the room. Fitness wearables invert this relationship trading on the

---

[3] Standards for Privacy of Individually Identifiable Health Information, 65 FED. REG. 82462, 82464 (Dec. 28, 2000) [hereinafter *Health Privacy Rule*] (citing JANNA MALAMUD SMITH, PRIVATE MATTERS: IN DEFENSE OF THE PERSONAL LIFE 240–41 (1997)).

[4] *Id.*

[5] *See generally* Stephanie Jernigan et. al, *Data Sharing and Analytics are Driving Success with IoT*, 58 MIT SLOAN MANAGEMENT REV. 1 (Fall 2016).

[6] Connie Prater, *What electronic payments reveal about you to lenders*, CREDITCARDS.COM (Jan. 13, 2009), https://www.creditcards.com/credit-card-news/credit-card-purchase-privacy-1282/#:~:text=Law%20enforcement%20agencies%20can%20subpoena,a%20crime%20victim%20or%20suspect.

[7] *Id.*

[8] Joel J. Heidelbaugh, *The Adult Well-Male Examination*, 98 AM. FAM. PHYSICIAN 729, 731 (Dec. 15, 2018).

[9] *Health Privacy Rule*, *supra* note 3, at 82467 (Dec. 28, 2000).

moral and social value placed on health and wellness to nudge users into disclosing personal health information.[10]

While fitness wearables like Fitbits and WHOOP may not collect the same swath of personal information as a routine physical, they still present concerns about personal health information because they collect a surprising amount of data. Fitbit's Charge 4 wrist strap passively collects heart rate data, activity, and sleep.[11] When paired with Fitbit's app, the Charge 4 can be used to track a user's menstrual cycle.[12] Similarly, WHOOP straps passively collect heart rate and sleep but also offer respiratory rate tracking.[13]

This information is valuable not just to the user and health companies but to hostile actors. In 2019, Google partnered with major U.S. hospital network Ascension to provide cloud computing capabilities and artificial intelligence services.[14] Project Nightingale, as the partnership is dubbed, is a HIPAA-compliant business associate agreement, allowing Ascension to send fully identifiable information to Google.[15] Google then uses this information to train machine-learning programs to develop a healthcare platform for Ascension.[16] At the same time, Google acquired Fitbit and the data of its 29 million users.[17] Google says that it will not merge the Fitbit user data with other data for advertising purposes, but given Google's track record of unauthorized sharing of personal data, there is cause for skepticism.[18] Even if Google honors its promise, the vast amount of

---

[10] Amy Roeder, *The Scarlet F*, HARV. PUB. HEALTH (Spring 2017), https://www.hsph.harvard.edu/magazine/magazine_article/the-scarlet-f.

[11] FITBIT, *Charge 4*, https://www.fitbit.com/global/us/products/trackers/charge4?sku=417BKGY (last visited Feb. 6, 2021).

[12] *Id.*

[13] WHOOP, *Experience*, https://www.whoop.com/experience/ (last visited Feb. 6, 2021); Mark Van Deusen, *Knowing Your Baseline, Case Studies in Respiratory Rate in Time of COVID-19*, WHOOP (Oct. 26, 2020), https://www.whoop.com/thelocker/case-studies-respiratory-rate-covid-19/.

[14] Gregory Barber & Megan Molenti, *Google Is Slurping Up Health Data—and It Looks Totally Legal*, WIRED (Nov. 11, 2019), https://www.wired.com/story/google-is-slurping-up-health-dataand-it-looks-totally-legal.

[15] Christina Farr & Jennifer Elias, *Google's hospital data-sharing deal raises privacy fears — here's what's really going on*, CNBC (Nov. 12, 2019), https://www.cnbc.com/2019/11/12/google-project-nightingale-hospital-data-deal-raises-privacy-fears.html.

[16] Barber, *supra* note 14.

[17] Rick Osterloh, *Google Completes Fitbit Acquisition*, GOOGLE (Jan. 14, 2021), https://blog.google/products/devices-services/fitbit-acquisition/.

[18] Barber, *supra* note 14.

health information that Google is processing makes it a ripe target for cyberattack.

Paul Ohm, a privacy and cybersecurity scholar at Georgetown University Law Center, describes "databases of ruin," the hypothetical collection of data held by third parties that, if revealed, could ruin a data subject's life.[19] Google's health information databases risk bringing the database of ruin out of the hypothetical and into the actual. The prospect of an adversary gaining access to either the Ascension data or the Fitbit data is bad enough, but when both are held by one entity, the damage is much greater. The two sets of health information could be accessed by an adversary, who would then have even greater insight into each user.[20] Linking one anonymized database to another unlocks information, which in turn could unlock even more. Cyberattacks of this kind should be at the forefront of any proposed change to the Privacy Rule keeping in mind the sophistication and subtlety with which these attacks can occur.[21]

Data exposure to authorized viewers should also be concerning. On June 19, 2020, PGA golfer Nick Watney, a WHOOP strap user, noticed his respiratory rate was higher than usual.[22] Watney had read that WHOOP had analyzed user data to determine that respiratory rate increases were correlated with positive COVID-19 diagnoses.[23] Despite testing negative a few days earlier, Watney got tested for COVID-19 again—his test came back positive.[24] WHOOP parlayed Watney's story into a deal with the PGA to supply 1,000 WHOOP straps to the PGA.[25] It is not just athletic associations partnering with WHOOP; lifestyle brand Tory Burch purchased 700 WHOOP straps for a "new employee wellness initiative to advance health and resilience during the COVID-19 pandemic."[26]

---

[19] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1746 (2010).
[20] *Id.* at 1746–48.
[21] Brian Krebs, *SolarWinds: What Hit Us Could Hit Others*, KREBS ON SECURITY (Jan. 21, 2021), https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/.
[22] Mark Van Deusen, *Knowing Your Baseline, Case Studies in Respiratory Rate in Time of COVID-19*, WHOOP (Oct. 26, 2020), https://www.whoop.com/thelocker/case-studies-respiratory-rate-covid-19/.
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *WHOOP Partners with Tory Burch to Optimize Employee Health and Well-Being*, YAHOO! (Oct. 14, 2020), https://news.yahoo.com/whoop-partners-tory-burch-optimize-130000215.html?soc_src=social-sh&soc_trk=ma.

When fitness wearables are provided by employers, they present a particular set of concerns. The confluence of the U.S. norm of employment-at-will, employer provided healthcare, and COVID-19 create an environment where employees may unwittingly provide health information to their employers, ultimately to their detriment. At-will employment, the doctrine that allows either employee or employer to terminate their employment relationship for any reason, is the default employment relationship in every state but Montana.[27] Fifty-five percent of American workers also receive their healthcare from their employer.[28] This data suggests there is a significant portion of the American workforce who are terminable for any reason and who also cost their employer thousands of dollars every year through healthcare costs.[29] In the wake of the COVID-19 pandemic, these employees may find themselves consenting to wellness and workplace health tracking programs that provide their employer with un-aggregated data.[30] COVID-19 may prove to be a catalyst for the widespread adoption of fitness wearables as a means of surveilling employees, even post-pandemic.

It is not difficult to imagine how employers could use this information to skirt existing laws. For instance, long term monitoring of heart rate data may lead an employer to believe that an employee is likely to suffer from a heart attack in the near future.31 The Americans with Disabilities Act prohibits employers from terminating employees due to certain health conditions, including heart attacks and the missed work that comes with treating these conditions.32 With long-term health monitoring via fitness wearables, employers can see which employees are more likely to develop a serious health condition and terminate those employees

---

[27] Mayer G. Freed & Daniel D. Polsby, *Just Cause for Termination Rules and Economic Efficiency*, 38 EMORY L.J. 1097, 1097 (1989); MONT. CODE. ANN. § 39-2-904(1)(b) (2009).

[28] CENSUS BUREAU, *Percentage of People by Type of Health Insurance Coverage and Change from 2017 to 2018*, https://www.census.gov/content/dam/Census/library/visualizations/2019/demo/p60-267/Figure_1.pdf (last visited Feb. 6, 2021).

[29] Sarah O'Brien, *Employers to spend about $10,000 on health care for each worker*, CNBC (Aug. 9, 2017), https://www.cnbc.com/2017/08/09/employers-to-spend-about-10000-on-health-care-for-each-worker.html.

[30] Ohm, *supra* note 19, at 1704 ("Data can either be useful or perfectly anonymous but never both.").

[31] Robert Shmerling, *How's your heart rate and why it matters*, Harv. Health Publishing (Mar. 25, 2020), https://www.health.harvard.edu/heart-health/hows-your-heart-rate-and-why-it-matters.

[32] DEP'T HEALTH AND HUM. SERV., *Your Rights Under the Americans with Disabilities Act* (June 2006), https://www.hhs.gov/sites/default/files/ocr/civilrights/resources/factsheets/ada.pdf.

before the condition manifests. As unscrupulous as this conduct appears, employment-at-will permits this seemingly arbitrary termination, and employee health surveillance enables it.

THE UNITED STATES HEALTH PRIVACY REGIME DOES NOT COVER FITNESS WEARABLES

Health information in the United States is protected under the Health Information Portability and Accountability Act (HIPAA), which delegates authority to the Department of Health and Human Services (HHS) to promulgate regulations in support of HIPAA.[33] HHS has done so through the promulgation of the Privacy Rule, which requires a covered entity to make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure or request.[34]

The Privacy Rule defines health information as any information "created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse," that relates to the physical or mental health or condition of an individual, the provision of health care to an individual, or payment for health care to an individual.[35] This information becomes protected health information when it is transmitted or maintained in any form.[36] The information generated by fitness wearables, like respiration, heart rate, and sleep information, would then appear to be protected health information.

Fitness wearables slip past the requirements of the Privacy Rule because of the narrow definition of a "covered entity." HHS has defined a covered entity as health care providers that electronically transmit health information in certain transactions, health insurers, and health care clearinghouses.[37] The Privacy Rule concentrates on the entity collecting the information rather than the information collected. Companies then that collect health information, as defined by HHS, but do not fit within the definition of a covered entity are conspicuously excluded from Privacy Rule requirements and subsequent enforcement.

The Privacy Rule matters because it sets limits on who covered entities can share information with and provides individuals with affirmative rights over their data, including rights of access and

[33] 42 U.S.C. 1320d-2.
[34] 45 C.F.R. §§ 164.502(b), 164.514(d).
[35] *Id.* § 160.03.
[36] *Id.*
[37] 45 C.F.R. § 160.03. *See also* 42 U.S.C. § 1320d.

correction.[38] The Privacy Rule requires that individuals be notified how their health information is used and shared and, importantly, gives individuals the opportunity to choose whether their health information can be used or shared for certain purposes, including marketing and sale.[39] These restrictions do not apply to fitness wearable companies because they are not covered entities. These entities are then not bound to disclose how health information is used and, in fact, are free to share and use user health information with whomever and however they choose. This fear is not theoretical. WHOOP, for instance, informs users they can expect WHOOP to share their health information with payment processors, ad networks, and analytics providers.[40] If WHOOP was considered a covered entity, this type of sharing would not be permitted without user permission. Additionally, WHOOP assures users that if their straps are used in conjunction with their employer's wellness program the employer only receives aggregated data, unless the user consents to providing un-aggregated data to their employer.[41] By leaving out fitness wearables from the definition of covered entity, the Privacy Rule strips users of agency over their health information.

The Privacy Rule also affords individuals who believe there has been a violation of their rights the opportunity to seek redress. The HHS Office of Civil Rights (OCR) is tasked with enforcement of the Privacy Rule and does so through a combination of voluntary compliance, technical guidance, and financial penalties for wrongdoing.[42] OCR is the only entity that is able to pursue companies for violations of the Privacy Rule as HIPAA and subsequent regulations did not create a private right of action.[43] Individuals are able to submit formal complaints with OCR or with state attorneys general if they believe any of the above rights have been violated.[44] Either course of action requires that the violation be by a covered entity. Users of fitness wearable are excluded from this remedy because fitness wearable companies are not covered entities.

Users may be able to pursue action through the Federal Trade Commission under unfair or deceptive acts and practices.

---

[38] 45 C.F.R. §§ 164.524, 164.526.
[39] 45 C.F.R §§ 164.501, 164.508.
[40] WHOOP, *Full Privacy Policy*, https://www.whoop.com/privacy/full-privacy-policy (Sept. 2, 2020).
[41] *Id.*
[42] Steve Alder, *Who Enforces HIPAA*, HIPAA J. (Oct. 25, 2017), https://www.hipaajournal.com/who-enforces-hipaa.
[43] Steve Alder, *Can a Patient Sue for a HIPAA Violation*, HIPAA J. (Nov. 7, 2017), https://www.hipaajournal.com/sue-for-hipaa-violation.
[44] Office for Civil Rights; Statement of Delegation of Authority, 65 Fed. Reg. 82381-01 (Dec. 28, 2000); 42 U.S.C. § 1320d-5(d).

However, it seems unlikely that such claims would result in favorable decisions for users. The FTC recently proposed a settlement with the fertility app Flo Health for allegedly breaking terms of its privacy policy by sharing pseudonymized data about consumers, like their pregnancies, with third parties, including marketing analytics companies.[45] This settlement allows us to extrapolate how the FTC would treat a case against a fitness wearable selling user information. First, the FTC focused on the fact Flo Health had told users it would not share data when in fact it was.[46] This suggests that companies like WHOOP would not be prosecuted because they do disclose to users that they share with third parties for a variety of purposes. Second, the FTC's proposed settlement would require Flo Health to get user consent before sharing their health information.[47] Outside the criticism that notice and choice consent do not effectuate user agency,[48] fitness wearables are already meeting the threshold for consent by seeking approval of terms and conditions before use. A future fitness wearable case then would be unlikely to succeed since fitness wearables are already doing what is required of them – the bare minimum.

PRINCIPLES FOR CLOSING THE COVERED ENTITY GAP

Currently, fitness wearables slip between the cracks, collecting personal health data without being subject to HIPAA's requirements. Even if HIPAA's requirements did apply, the Privacy Rule's reliance on anonymization has been rendered obsolete due to advances of re-identification science.[49] The Privacy Rule does not place limits on the use or disclosure of de-identified health information.[50] The law must change.

First, HHS and Congress should broaden the definition of "covered entity" to focus on *what* is being collected rather than *who* is doing the collecting. By adding a catch-all provision to covered entity to include any business that collects health information that is

[45] Wendy Davis, *Fertility App Must Inform Users about Privacy Prosecution, FTC* Says, MEDIAPOST (Jan. 14, 2021) https://www.mediapost.com/publications/article/359610/fertility-app-must-inform-users-about-privacy-pros.html.
[46] *In re Flo Health. Inc*., FTC File No. 1923133 (Jan. 13, 2021) (consent order); *In re Flo Health. Inc*., FTC File No. 1923133 (Jan. 13, 2021) (complaint).
[47] *In re Flo Health. Inc*., FTC File No. 1923133 (Jan. 13, 2021) (consent order); *In re Flo Health. Inc*., FTC File No. 1923133 (Jan. 13, 2021) (complaint).
[48] A discussion on notice and choice consent is unfortunately outside the scope of this Essay. For a full throated discussion *see generally* Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 125 Harv. L. Rev. 1880 (May 2013).
[49] Ohm, *supra* note 19, at 1769.
[50] 45 C.F.R. § 164.514.

not a health plan, a health clearinghouse, or a healthcare provider, regulators would be able to capture not just fitness wearables, but any future actors that may enter the health information space.[51]

Second, HHS should promulgate regulations outlining destruction principles for collectors of health information. HHS could set periods after which health information would need to be deleted from servers that are dependent on the type of covered entity. For example, health care providers may need a longitudinal health record of an individual that lasts until death. It is hard to imagine why a fitness band would need the same latitude.

Finally, HHS should limit non-covered entity access to health information to trusted researchers in conjunction with removing data anonymization requirements. Recognizing that de-identification is no longer reliable in the world of high-powered computing,[52] HHS could require that researchers access information at the source of the data, while permitting access to the full suite of data. This could increase research outcomes by allowing access to currently prohibited categories like birth date and zip code.[53]

CONCLUSION

The Privacy Rule was created in the wake of widespread adoption of electronic medical records.[54] Electronic records led to an increase in the number of organizations involved in providing healthcare, and this in turn led to a decrease in consumer trust in providing health information to their doctors.[55] We find ourselves at a similar moment as new players enter the healthcare space, and the power of data points to the promise of a healthier future. The Privacy Rule was created not only to simplify the administration of healthcare but to also expand the Fourth Amendment right of privacy of the person.[56] Allowing fitness wearable companies and other non-covered entities to share and collect health information with minimal regulation is a betrayal of the very reasoning underlying HIPAA. We would not let hospitals sell our health information to turn a profit – why should we let our watches?

---

[51] Google has recently announced that their phones will be able to read an individual's heart rate using the built-in camera alone. Ron Amadeo, *Google Pixel phones will soon track heart rate using only the camera,* ARS TECHNICA (Feb. 4, 2021), https://arstechnica.com/gadgets/2021/02/google-pixel-phones-will-soon-track-heart-rate-using-only-the-camera.

[52] Ohm, *supra* note 19, at 1769.

[53] *Id.*

[54] *Health Privacy Rule*, *supra* note 3, at 82463.

[55] *Id.*

[56] *Id.* at 82464.