5-2023

Moving to Digitized Health Care: Why HIPAA Coverage Needs to Be Expanded

CONNECTICUT
LAW REVIEW

VOLUME 55 MAY 2023 NUMBER 3

Comment

Moving to Digitized Health Care: Why HIPAA Coverage Needs to Be Expanded

DONGXUAN JESSICA TANG

The rapid development of personal technology over the past few years has thrust health care online. Most people have used some form of health tracking apps, nutrition apps, or exercise and fitness apps. The expansion of telehealth services and apps during the COVID-19 pandemic accelerated the shift toward online health care. Digitized health care, whether accessed through a mobile app, a web site, or a telehealth service, provides a convenient and efficient means for people to access health care services. But this new access comes with a hidden cost: a risk of unauthorized use of private health information. This Comment discusses the increase in digitized health care, the risks of health care data breaches, and the inability of the Health Insurance Portability and Accountability Act (HIPAA), the nation's most potent health care privacy law, to protect our privacy during this digitized health care boom. This Comment then explores how HIPAA and the regulations implementing it can be amended to provide the protections we need.

COMMENT CONTENTS

Moving to Digitized Health Care: Why HIPAA Coverage Needs to Be Expanded

DONGXUAN JESSICA TANG [*]

INTRODUCTION

Welcome to the age of the "smart." It is 2023, and everything in our lives seems to be "smart"—smart doorbell, smart lock, smart speaker. One clap, and the alarm turns off. A whisper of "Alexa," and music starts playing in the house. Stepping into the kitchen? The lights turn on after sensing our motions. But none of these devices is smarter than our wearable devices—with a few taps, these little factories can collect and store health information and then analyze that data for our benefit.[1] They can tell us everything from how many calories we burned in our last workout, to changes to our heart rate, to the amount of sleep we got last night. They can track our periods, cycles, fertilities, and methods we use to change our cycles, including birth control,[2] and even allow our health care providers to monitor us remotely.[3] These devices record almost everything we do: when we sit, when we stand, how many steps we take to get our morning coffee, the spike in our heart

[*] J.D., University of Connecticut School of Law, May 2023. Thank you to Professor John Cogan, who provided invaluable time and guidance in developing this Comment; to Chris Kriesen and Karem Friedman for your mentorship; to my peers of the *Connecticut Law Review* for your contributions and maintaining the highest editorial standards. Additionally, thank you to all my friends who stood by me. Thank you, my amazing parents, for your unconditional support; my beloved sister Doris, who always has my back; and my wonderful fiancé Ruben, for your continuous encouragement and patience.

[1] Wearable device is defined as "any kind of electronic device designed to be worn on the user's body. Such devices can take many different forms, including jewelry, accessories, medical devices, and clothing or elements of clothing." Kinza Yassar, *Wearable Technology*, TECHTARGET, https://www.techtarget.com/searchmobilecomputing/definition/wearable-technology (last visited Apr. 21, 2023).

[2] Hannah Norman & Victoria Knight, *Should You Worry About Data from Your Period-Tracking App Being Used Against You?*, KFF HEALTH NEWS (May 13, 2022), https://kffhealthnews.org/news/article/period-tracking-apps-data-privacy/; *see also Spot On Period Tracker*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/get-care/spot-on-period-tracker (last visited Apr. 21, 2023) (explaining the different functions of the application). This is an even bigger problem following *Dobbs v. Jackson Women's Health Organization*, 142 S. Ct. 2228, 2242 (2022) (overturning Roe v. Wade, 410 U.S. 113 (1973), and finding that the Constitution does not provide a right to an abortion). In states where abortion is banned or severely restricted, these apps can expose users to criminal liability. Rina Torchinsky, *How Period Tracking Apps and Data Privacy Fit into a Post-*Roe v. Wade *Climate*, NPR (June 24, 2022, 3:06 PM), https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps.

[3] Adam Hayes, *Wearable Technology*, INVESTOPEDIA (July 10, 2022), https://www.investopedia.com/terms/w/wearable-technology.asp.

rates when we complete a workout, the calories we have burned, and so on.[4] Besides wearable devices, there are also pages after pages of applications on Apple's App Store and the Google Play store to help us monitor our health through our smartphones.[5] These applications allow us to input the food we ate to track calories and the workout we did to monitor our heart rates.

Wearable devices are widespread, with about thirty percent of U.S. adults using them.[6] Among such users, nearly half (47.33%) use their devices every day, and a majority (82.38%) are willing to share their health data with providers.[7] To put these percentages in context, the American adult population is around 260 million;[8] thirty percent of this population means that about 78 million adults own wearable devices in the United States. However, data breaches happen all the time, leaving millions vulnerable.[9] In addition, this supposedly private data is often sold. SafeGraph, a data broker, sells the location data of people who visit abortion clinics, potentially exposing them to criminal liability in states where abortion is banned or severely restricted.[10]

Despite the significant risk posed by data breaches, wearable devices remain largely unregulated, which could result in identity theft and reputational damages for their users.[11] Even though other countries have

---

[4] *See* Paige Papandrea, Note, *Addressing the HIPAA-potamus Sized Gap in Wearable Technology Regulation*, 104 MINN. L. REV. 1095, 1095–96 (2019).

[5] *App Store: Health & Fitness*, APPLE, https://apps.apple.com/us/genre/ios-health-fitness/id6013 (last visited Apr. 21, 2023); *Google Play*, GOOGLE, https://play.google.com/store/apps/category/HEALTH_AND_FITNESS (last visited Apr. 21, 2023).

[6] Ranganathan Chandrasekaran et al., *Patterns of Use and Key Predictors for the Use of Wearable Health Care Devices by US Adults: Insights from a National Survey*, J. MED. INTERNET RSCH., Oct. 2020, 473, 476.

[7] *Id.*

[8] There are around 330 million people in the U.S. population. Of the 330 million, around 22.2% are children. This means that around 260 million are adults. *Quick Facts: United States*, U.S. CENSUS BUREAU (Jul. 1, 2021), https://www.census.gov/quickfacts/fact/table/US/PST045221.

[9] *See* Aaron Drapkin, *Data Breaches that Have Happened in 2022 and 2023 So Far*, TECH.CO (Apr. 11, 2023), https://tech.co/news/data-breaches-updated-list (tracking the latest data breaches).

[10] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022, 12:46 PM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood; Geoffrey A. Fowler & Tatum Hunter, *For People Seeking Abortions, Digital Privacy is Suddenly Critical*, WASH. POST (June 24, 2022, 4:23 PM), https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/.

[11] *See* Anna Mizzi, Note, *Profiting on Your Pulse: Modernizing HIPAA to Regulate Companies' Use of Patient-Consumer Health Information*, 88 GEO. WASH. L. REV. 481, 484 (2020) (exploring the idea of using HIPAA as a solution to regulating consumer health interactive analysis companies); *see also* Papandrea, *supra* note 4, at 1097 (stating that wearable devices are "wildly unregulated, with a few limited exceptions, and no stranger to data breach and privacy controversies" (footnote omitted)). The Federal Trade Commission (FTC) describes medical identity theft as incidents in which "someone uses another person's name or insurance information to get medical treatment, prescription drugs or surgery." FED. TRADE COMM'N, MEDICAL IDENTITY THEFT: FAQS FOR HEALTH CARE PROVIDERS AND HEALTH PLANS 1 (2011), https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.

expanded protection for all consumer data,[12] the United States has yet to do so. The Health Insurance Portability and Accountability Act (HIPAA) is the nation's most potent health care privacy law.[13] However, HIPAA was enacted in 1996 and related regulations from the Department of Health and Human Services (HHS) were last significantly amended in 2013.[14] HIPAA can no longer keep up with today's fast-developing technology advancements. The lack of oversight puts Americans at risk of data and privacy breaches.[15]

This Comment explores the gap between HIPAA and wearable devices—why wearable devices fall outside the realm of HIPAA—and provides a solution to this problem. Although some scholars have already raised this issue,[16] this Comment proposes a unique solution to the problem of wearable devices falling beyond the scope of HIPAA. Others have suggested changes to how HIPAA is regulated by expanding the definition of covered entities.[17] However, simply amending HHS regulations to include wearable devices under the Act's "covered entities" will not provide the solution, either to wearables or universally for all health care technologies. With the rapid development of technology, any new definition will soon be outdated because there will be new health technologies on the market every few months and new health apps developed every day. The digital health data privacy problem is much bigger than simply wearables. There are also websites that collect user data—for example, over-the-counter pregnancy tests can ask users to input data regarding their cycles to a website.[18] All personal data collected is already sensitive information at the point of collection, but the "covered entities" definition does not address this issue.

---

[12] Through the General Data Protection Regulation (GDPR), Europe has already expanded protection for consumer data , but the United States has yet to follow. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1, 33 (EU) (recognizing that "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right").

[13] *Information is Powerful Medicine*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/information-is-powerful-medicine/index.html (last visited Apr. 21, 2023) (describing the potency of HIPAA and listing rights under HIPAA, ranging from control over medical records to personal representatives and notice of privacy practices).

[14] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C.); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164); *see also HIPAA Updates and HIPAA Changes in 2023*, HIPAA J. (Mar. 9, 2023), https://www.hipaajournal.com/hipaa-updates-hipaa-changes/.

[15] FED. TRADE COMM'N, *supra* note 11.

[16] *See generally* Mizzi, *supra* note 11 (exploring the idea of expanding HIPAA); *see also* 45 C.F.R. § 160.103 (2021) (defining "covered entity" as a health plan, health care clearinghouse, or "health care provider who transmits any health information in electronic form in connection with a transaction").

[17] *See generally* Papandrea, *supra* note 4 (explaining how HIPAA should be expanded to include covered entities).

[18] *See, e.g.*, FIRST RESPONSE PREGNANCY HUB, https://firstresponsepregnancyhub.socialmedialink.com/ (last visited Apr. 22, 2023) (inviting users to "participate in surveys and questionnaires").

Therefore, HHS needs to remove the "covered entities" requirement entirely and regulate HIPAA so that all health data is monitored at the point of collection.

This Comment consists of two parts. The first part provides an overview of the privacy dangers posed by wearable technologies and health apps, and the lack of oversight of HIPAA. The paper then discusses how HHS can alter its regulation of HIPAA to combat this problem and proposes a unique and workable solution. While this discussion is limited to wearables, the proposed solution could also cover other technologies and processes for obtaining and transmitting personal health data, providing broader protection from data and privacy breaches. Wearables pose a big problem, but they are not the only health care technologies that put out data and privacy at risk. User-input websites and other medical monitoring devices can also expose our personal information,[19] so this Comment's solution addresses the regulation of health care technologies as a whole.

I. PROBLEMS OF WEARABLE TECHNOLOGIES AND HIPAA REGULATION

Fueled by COVID-19, more and more health records are stored digitally.[20] Known as electronic health records (EHR),[21] these systems provide great convenience to our lives. However, their shortcomings are also significant—they are vulnerable to data breaches that can result in loss of sensitive information, identity theft, reputational damage, and financial harm.[22] According to a study published in the BMJ that analyzed twenty-four of the most popular EHR apps in the Google Play store, seventy-nine percent of widely used health apps share user data, risking users' privacy.[23] These data are not just shared with app developers but also with outside or third-party companies that use consumer data for sales and marketing.[24] Many companies sell personal health data to third parties; this even includes hospitals, as HIPAA does not require patient consent to share or sell

---

[19] *See, e.g.*, Drapkin, *supra* note 9; Kirsty Needham & Clare Baldwin, *China's Gene Giant Harvests Data from Millions of Women*, REUTERS (July 7, 2021, 5:00 PM), https://www.reuters.com/investigates/special-report/health-china-bgi-dna.

[20] *See* John Glaser, *It's Time for a New Kind of Electronic Health Record*, HARV. BUS. REV. (June 12, 2020), https://hbr.org/2020/06/its-time-for-a-new-kind-of-electronic-health-record (explaining how the COVID-19 pandemic has presented "the U.S. health care system with a mind-boggling array of challenges," including "[s]orting through large amounts of information and finding the nuggets that apply to a particular patient's situation").

[21] *Id.*

[22] Nir Menachemi & Taleah H. Collum, *Benefits and Drawbacks of Electronic Health Record Systems*, 4 RISK MGMT. HEALTHCARE POL'Y 47, 51–52 (2011).

[23] Quinn Grundy et al., *Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis*, BMJ, Mar. 23, 2019, at 4.

[24] *Id.* at 5–10.

anonymous data.[25] In addition, state and local governments can access this data for their own purposes.[26]

Even if health apps claim that they will keep data private, ninety-one percent of people consent to legal terms and services conditions without reading them, according to a Deloitte survey.[27] Even when consumers want to combat this problem by reading privacy policies and "shop for privacy terms" when they choose a product, many electronic health technology companies reserve the right to unilaterally amend their terms of service and their privacy policies.[28] This means that they can make one-sided changes that undermine the market for privacy, leaving users vulnerable.[29] Unfortunately, no law currently restricts such unilateral amendments.

HIPAA, a landmark federal law that expanded protections for some personal health data,[30] offers a potential solution to the sale of health data, consumer's blind consent, and companies' unilateral amendments. Since HIPAA's enactment in 1996, HHS has updated its regulation of the Act many times. Effective in 2003, HHS added the Privacy Rule, which mandates that "health plans, health care clearinghouses, and certain health care providers must guard against misuse of individuals' identifiable health information and limit the sharing of such information."[31] Effective in 2005, HHS added the Security Rule, which set the standards that covered entities must meet to protect electronic health data that they hold or transfer.[32] The most significant update was to incorporate the requirements of the 2009 Health Information Technology for Economic and Clinical Health

---

[25] *Id.*; 45 C.F.R. § 164.502 (2021); Nicole Wetsman, *Hospitals Are Selling Treasure Troves of Medical Data — What Could Go Wrong?*, VERGE (June 23, 2021, 2:22 PM), https://www.theverge.com/2021/6/23/22547397/medical-records-health-data-hospitals-research.

[26] This has been a problem in the health care field since the 1990s. Even though HIPAA has been amended to address this problem, "[n]o explicit right to privacy is guaranteed by the Constitution of the United States; in fact, the word 'privacy' does not appear." INST. OF MED., HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY 146 (Molla S. Donaldson & Kathleen N. Lohr eds., 1994).

[27] DELOITTE, 2017 GLOBAL MOBILE CONSUMER SURVEY: US EDITION 12 (2017), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf.

[28] Leah R. Fowler et al., *Uncertain Terms*, 97 NOTRE DAME L. REV. 1, 26 (2021).

[29] *Id.* at 27.

[30] Congress enacted HIPAA as a major health reform law following the failure of President Clinton's health reform efforts. *Health Care Reform Initiative*, CLINTON DIGIT. LIBR., https://clinton.presidentiallibraries.us/health-reform-initiative (last visited Apr. 22, 2023). It contains multiple parts, which affect everything from group health insurance to tax law. Title II of HIPAA includes provisions to establish standards and requirements for the electronic transmission of certain health information. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 261, 110 Stat. 1936, 2021 (1996) (codified as amended at 42 U.S.C. § 1320d).

[31] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182, 53182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 164).

[32] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164).

(HITECH) Act,[33] which expanded the Security Rule to include business associates of covered entities.[34] Despite these changes, HIPAA still has a major flaw: limited coverage.

Currently, HHS regulations do not cover consumer health data. Even though health care is becoming rapidly digitized, consumer health data, like that commonly found in wearables, is not included among HHS's limited definition of "covered entities."[35] Covered entities only include health plans,[36] health care clearinghouses,[37] and health care providers who electronically store or use health data in connection to transactions.[38] After the HITECH Act,[39] HIPAA also applies to business associates of covered entities,[40] an addition which has helped to strengthen the security of HIPAA protections. However, the definition of covered entity is still far from

---

[33] Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, §§ 13001–13424, 123 Stat. 115, 226–79 (codified as amended in scattered sections of 42 U.S.C.); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164) (regulations incorporating the HITECH Act into the enforcement for HIPAA).

[34] 42 U.S.C. § 17931. The definition of covered entity has been the subject of debate. Even though the HITECH Act expanded the reach of the Security Rule, its coverage is still limited. *See* 45 C.F.R. § 160.103 (2021).

[35] *See To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, NAT'L INSTS. OF HEALTH, https://privacyruleandresearch.nih.gov/pr_06.asp (last visited Apr. 22, 2023).

[36] "For HIPAA purposes, health plans include the following: Health insurance companies, HMOs, or health maintenance organizations, Employer-sponsored health plans, Government programs that pay for health care, like Medicare, Medicaid, and military and veterans' health programs." *Are You a Covered Entity?*, CTRS. FOR MEDICARE & MEDICAID SERVS. (May 26, 2022, 10:37 AM), https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.

[37] Healthcare clearinghouses are processors that analyze claim data between healthcare providers and insurance payers. *Healthcare Clearinghouse: What It Is and How It Can Help*, SMART DATA SOLS. (Sept. 9, 2020), https://sdata.us/2020/09/09/what-is-a-healthcare-clearinghouse/.

[38] 45 C.F.R. § 160.103 (2021); *see also Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Apr. 8, 2023). These health care providers broadly include doctors, nurses, hospitals and so on. Under HIPAA, HHS has adopted a definition of "standard transactions" to manage covered entities. The definition includes payment and remittance advice, claims status, eligibility, coordination of benefits, claims and encounter information, enrollment and disenrollment, referrals and authorizations, and premium payments. § 160.103. These transactions are governed under the same standard to ensure uniformity across board. *Transactions Overview*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview (last visited Apr. 22, 2023).

[39] The HITECH Act was enacted in 2009 as part of the American Recovery and Reinvestment Act (ARRA). It encourages the adoption of health technologies and allows patients to actively participate in health programs. It strengthens the privacy and security protections of HIPAA by expanding the definition of covered entities to include business associates and introducing tougher sanctions for violations. *What is the HITECH Act?*, HIPAA J., https://www.hipaajournal.com/what-is-the-hitech-act/ (last visited Apr. 22, 2023).

[40] 45 C.F.R. § 164.502(e) (2021). According to HHS, a business associate "is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity." *Business Associates*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last visited Apr. 22, 2023).

sufficient—unless an app or wearable transmits your health data to a covered entity or a business associate, HIPAA does not protect your data.

II. HOW HHS SHOULD CHANGE ITS REGULATION OF HIPAA

While HIPAA currently cannot address its electronic health privacy problem—wearable technologies do not fall under "covered entities"—HHS could modify how it regulates the statute. The definition of "covered entities" is part of the regulations issued by HHS, and so HHS can change its ways of regulating HIPAA to combat this issue.[41] Since this solution does not need to go through Congress, these amendments are relatively simple, and this solution is workable.

Although the proposed solution reaches beyond wearable technologies, it is particularly helpful in addressing the troubling problems that wearables pose. As mentioned, wearable technology is one of the most widespread usages of electronic health data, so it is important to address this issue. Since the OCR likely does not have the personnel and resources to monitor and enforce HIPAA violations on the millions of these devices we own, HHS needs to change the way it defines "covered entities."

The most important thing to note is that simply redefining "covered entities" is inadequate. Any expansion of HIPAA regulations should tackle the perpetual problem of technology developing at a much faster rate than the legal system can address. Some scholars have suggested expanding HIPAA's covered entities to include the makers of wearable devices.[42] However, if HHS simply expanded HIPAA regulations to make these companies covered entities, the law would still fail to address still newer technologies. Every time a new health technology hits the market, HIPAA regulations would need to be expanded again to cover the novel device.

Instead, HHS needs to remove its list of "covered entities" from its regulations and instead control all health data at the point of collection from a user, regardless of the "entity" collecting it. This will ensure that the Act does not become outdated in just a few months when new technologies come out. This approach also reclassifies what HIPAA covers by the type of data—it must cover *all* health data provided by a private user. Right now, the covered entities use the HIPAA Privacy Rule as a guideline for personal health information (PHI).[43] PHI is the only guidance that entities have regarding which types of data are protected and which are not. This allows

---

[41] 45 C.F.R. § 160.103 (2021). In the HITECH Act's revisions of HIPAA, Congress deferred to HHS's definition of "covered entities" rather than codifying its own definition. 42 U.S.C. § 17921(3) ("The term 'covered entity' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.").

[42] *See generally* Mizzi, *supra* note 11; Papandrea, *supra* note 4 (explaining that HIPAA needs to be expanded to include wearables).

[43] *What is PHI?*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/answers/hipaa/what-is-phi/index.html (last visited Apr. 22, 2023).

for a picking and choosing of which personal data to protect and which to enable providers to sell.

In addition, every time individuals enter health data into their wearables (e.g., measuring heartbeat), that information only becomes PHI when the individual can be identified.[44] It is important to understand the distinction between anonymous data and de-identified data.[45] Anonymous data "does not contain any identifiable information and there is no way to link the information back to identifiable information," while de-identified data "does not contain any identifiable information, but there is a way to link the information back to identifiable information."[46] So what is considered PHI? HIPAA has set out eighteen identifiers—if the patient data contains any of the eighteen identifiers, it is considered PHI.[47] If none of these identifiers are present, it is considered anonymous and not

---

[44] Danielle Kelvas, *Understanding What Is and Is Not PHI*, HIPAA EXAMS, https://www.hipaaexams.com/blog/understanding-what-is-and-is-not-phi/ (last visited Apr. 22, 2023).

[45] R. Bert Wilkins, *Do You Know Me?: The Subtle Distinction Between "Anonymous" and "De-identified" Data in Clinical Research*, WCG IRB, https://www.wcgirb.com/insights/do-you-know-me-the-subtle-distinction-between-anonymous-and-de-identified-data-in-clinical-research/ (last visited Apr. 22, 2023).

[46] *Id.*

[47] 45 C.F.R. § 164.514(b)(2)(i) (2021). The identifiers are:

> 1. Names
> 2. Geographic subdivisions smaller than a state (except the first three digits of a zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000)
> 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death and all ages over 89 and all elements of dates (including year) indicative of such age (except that such ages and elements may be aggregated into a single category of age 90 or older)
> 4. Telephone numbers
> 5. Fax numbers
> 6. Electronic mail addresses
> 7. Social security numbers
> 8. Medical record numbers
> 9. Health plan beneficiary numbers
> 10. Account numbers
> 11. Certificate/license numbers
> 12. Vehicle identifiers and serial numbers, including license plate numbers
> 13. Device identifiers and serial numbers
> 14. Web Universal Resource Locators (URLs)
> 15. Internet Protocol (IP) address numbers
> 16. Biometric identifiers, including finger and voice prints
> 17. Full face photographic images and any comparable images
> 18. Any other unique identifying number, characteristic, or code (excluding a random identifier code for the subject that is not related to or derived from any existing identifier).

Id.; *see also HIPAA Identifiers: Anonymizing Data*, STANFORD MED., https://med.stanford.edu/irt/security/stanfordinfo/hipaa.html (last visited Apr. 22, 2023).

"protected."[48] As a practical matter, however, anonymous does not mean that it is de-identified. The data can still be traced back to the individual.[49] This poses a major issue because data can be sold or breached at the point of collection, and some data never becomes PHI because the individual only puts in general data considered to be anonymized. In fact, many data brokers take advantage of this loophole and sell consumer profiles containing anonymous medical information.[50]

For example, when an individual inputs data into a period tracker anonymously, that data is not PHI. At this point, the individual is anonymous, and the app company can sell the data. However, the buyers of anonymous health data can supplement it with other data "culled from social media interactions, retail stores, web trackers, online transactions, mobile phone location trackers, fitness wearables, and so on," and "subsequently leverage their sophisticated algorithms and the breadth of their triangulation databases to re-identify the data"[51] (and potentially expose that person to criminal liability post-*Dobbs*).

Because of this risk, HIPAA regulations should protect as PHI all health data at the point of collection, regardless of the eighteen identifying markers. This would ensure that no matter how the data is collected or through which device it is collected, private health information would be considered PHI that cannot be sold. Expanding HHS regulations to remove "covered entities" and instead protect all health data at the point of collection can ensure that these regulations also apply to other new forms of technology, beyond just wearables.[52]

Of course, many consumers turn to telehealth or wearables for their convenience and affordability. Although exposing more companies to liability under HIPAA can possibly deter innovation of new health technologies and make health care less affordable or privacy agreements more tedious, it is important to enforce privacy regulations more rigorously. The need for improved health data privacy calls for bold solutions. In 2021, health data service provider GetHealth left user records from over 61 million fitness trackers from both Apple and Fitbit exposed online.[53] However, it is

---

[48] § 164.514(b).

[49] Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143, 179 (2016) (describing how data brokers supplement anonymous health data with other sources to "re-identity" the data).

[50] Wendy A. Bach & Nicolas Terry, *How* Dobbs *Threatens Health Privacy*, HARV. L.: BILL OF HEALTH (Jan. 10, 2023), https://blog.petrieflom.law.harvard.edu/2023/01/10/how-dobbs-threatens-health-privacy/.

[51] Terry, *supra* note 49, at 179; Bach & Terry, *supra* note 50.

[52] After the *Dobbs* decision, this can be crucial because it also applies to OTC pregnancy kits. When individuals take an OTC pregnancy test and go online to acquire information, websites can collect such information and sell it to states where abortion is banned or restricted, exposing users to criminal liability.

[53] Jeremy Fowler, *Report: Fitness Tracker Data Breach Exposed 61 Million Records and User Data Online*, WEBSITE PLANET, https://www.websiteplanet.com/blog/gethealth-leak-report/ (last visited

unclear whether GetHealth, Apple or Fitbit took any significant remedial steps.[54] Companies will take privacy more seriously if they are subject to meaningful consequences for breaching it.

Furthermore, any risk of negative consequences such as deterring innovation is limited because enforcement is limited—HHS's Office for Civil Rights (OCR) has only imposed fines in 130 cases, or 0.4% of those that it found required "changes in privacy practices and corrective actions."[55] Much more often, the OCR "enforce[s] the HIPAA Rules by applying corrective measures"[56]—presumably allowing violators the opportunity to change their conduct without penalty. Although some courts allow plaintiffs to use HIPAA to establish the standard of care in negligence cases,[57] there is no private right of enforcement under HIPAA for breach of privacy. This means that aggrieved individuals in data breach cases cannot sue companies directly, so they cannot hold companies accountable when OCR so rarely employs penalties. However, greater enforcement is simply impractical; the government does not have the resources to litigate thousands upon thousands of valid complaints. Companies thus have little incentive to proactively ensure their conduct complies with HIPAA and may continue innovating with little risk of penalties from OCR.[58]

Therefore, because of the importance of privacy regulations and the limited risk of deterring innovation, HIPAA's regulations must be amended to cover all entities that collect health data.

Apr. 22, 2023); Jill McKeon, *61M Fitbit, Apple Users Had Data Exposed in Wearable Device Data Breach*, HEALTH IT SEC. (Sep. 16, 2021), https://healthitsecurity.com/news/61m-fitbit-apple-users-had-data-exposed-in-wearable-device-data-breach.

[54] *Id*.

[55] *Enforcement Highlights*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Apr. 14, 2023), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[56] *Id*.

[57] *See, e.g.*, Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 175 A.3d 1, 7 (2018) ("We conclude that recognizing a cause of action for the breach of the duty of confidentiality in the physician-patient relationship by the disclosure of medical information is not barred by . . . HIPAA and that public policy, as viewed in a majority of other jurisdictions that have addressed the issue, supports that recognition."). Even so, there do not appear to be many of these cases. On Westlaw, there are only about five hundred negligence cases that used HIPAA to establish the standard of care. This is not a lot at all, considering that OCR has received over 325,577 HIPAA complaints. *Enforcement Highlights*, *supra* note 55. Although these are only the reported cases and actual number of cases can vary, this low number of cases suggests that merely having a state tort enforcement mechanism is not an effective remedy and therefore not an effective deterrent to curb companies' misconduct.

[58] State Attorneys General may also enforce civil penalties for HIPAA violations, 42 U.S.C. § 1320d–5(d), while the U.S. Department of Justice may enforce criminal penalties for HIPAA violations, *id*. § 1320d-6. OCR has made 1,731 referrals to DOJ "for the knowing disclosure or obtaining of protected health information in violation of the Rules." *Enforcement Highlights*, *supra* note 55.

CONCLUSION

HIPAA is currently the only statute that governs the collection and privacy of health data. However, there is a major problem with how HHS regulates HIPAA. Its definition of "covered entities" is too limited because it does not cover wearable devices and cannot adapt with newer health technologies. HIPAA's regulation must be amended to cover health information at the point of collection regardless of the identity of the collector. Doing so will expose companies to more liability and allow HIPAA to keep up with today's rapid changes in technology.