Note

Addressing the HIPAA-potamus Sized Gap in Wearable Technology Regulation

*Paige Papandrea**

INTRODUCTION

You wake up at 7:00 AM, half an hour late. You rush to get ready, first throwing on your Apple Watch[1] and then showering. Your watch records your heart rate at 112 beats per minute and counts exactly seventeen steps from your bedroom to your bathroom. You run to catch the bus at 7:30 AM—your watch tracks your location as you run exactly 0.3 miles to the bus stop. Your heart rate is 155 beats per minute, you ran exactly 600 steps to get there, and burned around twenty-two calories, all tracked by your watch. You sit down, also recorded on your watch. You arrive at work at 8:00 AM, sprint up the three flights of stairs, and quickly sit at your desk. Your watch measures your heart rate at 169 beats per minute, updates how many flights of stairs you

* J.D. Candidate 2020, University of Minnesota Law School. I owe thanks to many people for their roles in my Note's publication. First and foremost, thank you to Professor Amy Monahan for the guidance and advice in writing my Note. I also owe a special thanks to Professor Christopher Soper for his mentorship throughout law school and his willingness to be a much-needed listening ear during the Note-writing process. To the wonderful *Minnesota Law Review* editors and staff, especially those staff members who checked my numerous citations, thank you all for your hard work. Thank you to my father, Rick Papandrea, and Roger Strode for providing the physician's and health care lawyer's perspectives, respectively, on my Note topic. To Eric, Sam, Frances, Bryan, Corissa, and Connor, thank you for being my rocks throughout law school. Finally, thank you to Cole, whose love and support over the past year undoubtedly made this a better Note.

1. This section discusses the types of data collected by a hypothetical Apple Watch. These types of data include heart rate, steps, distance traveled by foot, calories burned, flights of stairs taken, time spent sitting, time spent standing, general activity level, exercise length and type, and GPS location. *See* Joseph Keller, *Apple Watch and Activity Tracking: Everything You Need to Know!*, IMORE (Mar. 1, 2019), https://www.imore.com/apple-watch-and-activity-tracking-what-you-need-know [https://perma.cc/E2ZY-8KNL].

have climbed in the Apple HealthKit,[2] and records the precise moment you sat at your desk. Over the next nine hours of work, your watch records almost everything you do: when you sit, when you stand, how many steps you take to get your morning coffee, your every trip to the bathroom, the spike in your heart rate when your boss asks you to come into her office. After work, you complete a quick workout and the exact workout length, calories burned, steps taken, and minute-by-minute heart rate are recorded by your watch.

At the end of the day, your watch tells you your general activity level, how many calories you burned (and how they were burned), and total time standing. You can also view your heart rate throughout the day, your total steps taken, and distance covered by foot. If you had a different type of wearable technology, you may have recorded your blood pressure,[3] monitored your insulin levels,[4] or tracked your sleep patterns.[5] Although this health information is similar to, and in many cases more personal than, information collected by doctors and certain types of insurers, it generally has no privacy or security protections under federal law.[6] This leaves most wearable technology companies free to impose weak data security measures and sell or

2. Apple's HealthKit is an iOS platform that allows a wide range of fitness, health, and medical data to be shared across different Apple apps and devices. *See* Ryan Faas, *Get to Know iOS 8: HealthKit and Apple's New Health App*, MACWORLD (Oct. 6, 2014), https://www.macworld.com/article/2691952/get-to-know-ios-8-healthkit-and-apple-s-new-health-app.html [https://perma.cc/KRM5-KFH4].

3. *See* Hugh Langley, *Fighting the Silent Killer: Blood Pressure Is Wearable Tech's Next Challenge*, WAREABLE (Aug. 28, 2018), https://www.wareable.com/health-and-wellbeing/wearable-blood-pressure-tech-559 [https://perma.cc/UU3A-3K9Q] (discussing different wearable technology devices that can monitor blood pressure).

4. *See* Michael Sawh, *The Holy Grail: What You Need to Know About Wearables and Glucose Monitoring*, WAREABLE (June 18, 2019), https://www.wareable.com/health-and-wellbeing/wearables-glucose-monitoring-6476 [https://perma.cc/2Y9C-25TG] (discussing devices like the Dexcom monitor, which pairs with Fitbits to help users manage diabetes).

5. *See* Conor Allison, *Best Sleep Trackers: We Compare Fitbit, Wearable and Bedside Devices*, WAREABLE (Aug. 29, 2019), https://www.wareable.com/health-and-wellbeing/best-sleep-trackers-and-monitors [https://perma.cc/9NS2-5AMF] (discussing different wearable technology that tracks users' sleep patterns and habits).

6. See *infra* Part II.B for a discussion of the types of data from wearable technology that are currently protected by HIPAA.

share their users' health information without legal liability. Similarly, if they experience a data breach in which individuals' health information is compromised, then wearable technology users have no right to a remedy.[7]

Despite the significant risks posed by wearable technology, it remains wildly popular.[8] It is also wildly unregulated,[9] with a few limited exceptions, and no stranger to data breach and privacy controversies.[10] Given the types of health information collected by wearable technology, the Health Insurance Portability and Accountability Act of 1996, better known as HIPAA, appears to be the likeliest candidate for wearable technology regulation.[11] However, HIPAA's rules on health information privacy and security currently only apply to "covered entities" such as physicians and insurance companies and their "business associates,"[12] leaving the vast amounts of personal health information collected by wearable technology virtually unprotected.

7. Since the mid-2000s, the risk of data breaches has increased. *See* John Biglow, Note and Comment, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943, 943, 946 (2016) (stating that since 2005, 4789 publicly-known data breaches resulted in 896,258,345 compromised records and that 781 of these breaches occurred in 2015 alone).

8. See *infra* Part I.B for a discussion of the widespread use of wearable technology.

9. *See, e.g.*, Nina Kostyukovsky, *Regulating Wearable Devices in the Healthcare Sector*, AM. B. ASS'N (Sept. 27, 2018), https://www.americanbar.org/groups/health_law/publications/aba_health_esource/2014-2015/may/devices/ [https://perma.cc/NTT5Q6VK] ("Wearable device manufacturers are not ordinarily exposed to HIPAA liability, because they are not Covered Entities."); Colin Lecher, *The FDA Doesn't Want to Regulate Wearables, and Device Makers Want to Keep It That Way*, THE VERGE (June 24, 2015), https://www.theverge.com/2015/6/24/8836049/fda-regulation-health-trackers-wearables-fitbit [https://perma.cc/32WY-9TDF] (describing how the Food and Drug Administration will not regulate wearable technology).

10. *Cf.* Liz Sly, *U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging*, WASH. POST (Jan. 29, 2018), https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html [https://perma.cc/NE7X-7SCG] (discussing how Fitbit use accidentally revealed the locations of military bases).

11. This Note will exclusively focus on the regulation of wearable technology to protect users' private health information. Regulation of wearable technology for purposes of device safety, device effectiveness, general user privacy, or other purposes are separate issues not covered in this Note.

12. See *infra* Part I.A.1 for a discussion of "covered entities" and "business associates."

This Note argues that HIPAA's existing framework, although well suited for the protection of health data in its traditional forms, must be modernized to reflect the reality that personal health information is created, collected, stored, and transmitted by devices far-removed from the four walls of a doctor's office. Part I discusses HIPAA and its regulatory protections of health information, which are limited by its application to only "covered entities" and their "business associates." It also outlines the current state and uses of wearable technology. Part II highlights pertinent issues with wearable technology, the massive gaps in HIPAA coverage of health information collected or transmitted by wearable technology, and the other laws and regulations that fail to cover it. Part III proposes expanding HIPAA's definition of "covered entities" to include wearable technology companies, so that the health information collected and transmitted by wearable technology is adequately regulated and protected. It provides model language for this expansion and also addresses why other potential solutions, unrelated to HIPAA, are inadequate.

I. HIPAA AND THE EMERGENCE OF WEARABLE TECHNOLOGY

Medical privacy is such a foundational aspect of the health care system that it was written into the Hippocratic Oath.[13] Congress recognized the importance of medical privacy when it passed HIPAA in 1996, citing the increased risks of unauthorized disclosure of medical information posed by electronic communication.[14] What Congress did not contemplate, however, was the emergence of non-medical entities that collect, store, and transmit private medical information. This Part introduces HIPAA's key regulatory components and wearable technology as one type of non-medical device that interacts with health information. Section A outlines the limited application of HIPAA's

13. MARGARET BRAZIER & EMMA CAVE, MEDICINE, PATIENTS AND THE LAW 83 (5th ed. 2011) ("Whatever, in connection with my professional practice, or not in connection with it, I see or hear in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." (quoting the Hippocratic Oath)).

14. *See Protecting Our Personal Health Information: Privacy in the Electronic Age: Hearings Before the S. Comm. on Labor & Human Res.*, 105th Cong. 2–5 (1997) (statements of Sen. Bill Frist, Member, S. Comm. on Labor & Human Res., and Donna E. Shalala, Secretary, U.S. Dep't of Health and Human Servs.).

regulatory framework to traditional health care entities and the regulatory protections afforded to patients' health information. Section B discusses the popularity of wearable technology, the types of health data it collects, and its user benefits.

A. HIPAA, ITS LIMITED APPLICATION, AND ITS REGULATORY FRAMEWORK

Congress enacted HIPAA with the original purpose of improving "the portability and continuity of health insurance."[15] However, public concerns about health information privacy and rapidly developing electronic technology led Congress to incorporate provisions into HIPAA that allowed the Secretary of the Department of Health and Human Services (HHS) to promulgate rules for health information privacy and security.[16] HHS primarily accomplished this goal by enacting the HIPAA "Privacy Rule,"[17] the HIPAA "Security Rule,"[18] the HIPAA "Enforcement Rule,"[19] and the HIPAA "Breach Notification Rule."[20] However, the protections afforded by the HIPAA Privacy, Security, Enforcement, and Breach Notification rules do not apply to all types or uses of health data. This Section discusses HIPAA's limited application and its regulatory framework in turn below.

15. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 136.

16. *Id.* § 264; *HIPAA for Professionals*, U.S. DEP'T OF HEALTH & HUM. SERVICES (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/index.html [https://perma.cc/MQQ8-GTUX].

17. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. §§ 160, 164); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. §§ 160, 164).

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

19. HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390 (Feb. 16, 2006) (codified at 45 C.F.R. §§ 160, 164).

20. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Heath Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164). The Breach Notification Rule was included in a final rule promulgated by HHS that implemented a number of provisions in the Health Information Technology for Economic and Clinical Health (HITECH) Act. *Id.*; *Omnibus HIPAA Rulemaking*, U.S. DEP'T OF HEALTH & HUM. SERVICES. (Oct. 30, 2015), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html [https://perma.cc/RD6B-58T5].

1. HIPAA Only Extends Its Regulatory Protections to "Personal Health Information" Held by "Covered Entities" and Their "Business Associates"

Although HIPAA may appear to protect all of an individual's health information, the accompanying regulatory language limits its protections to "protected health information" (PHI). Simply put, health information must be coupled with personal identifiers to constitute PHI and receive protection under HIPAA's various regulatory rules.[21] For example, "if [a] vital signs dataset includes [a personal identifier], then the entire dataset must be protected since it contains an identifier."[22] Personal identifiers include things such as names, biometric identifiers, and "[a]ny other unique identifying number, characteristic, or code."[23]

The protection and regulation of PHI by HIPAA only applies to "covered entities"[24] and "business associates."[25] Covered entities include health plans, health care clearinghouses, and health care providers who transmit "any health information in electronic form in connection with a transaction covered by this subchapter."[26] These most commonly include individuals or entities such as doctors, clinics, pharmacies, and health insurance companies.[27]

21. PHI consists of any individually identifiable health information transmitted or maintained by covered entities and their business associates. 45 C.F.R. § 160.103 (2017). Health information is any information, including genetic information that regardless of form or medium, "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." *Id.* If health information identifies the individual, or there is a reasonable basis to believe it could be used to do so, it is considered individually identifiable. *Id.*

22. *HIPAA PHI: List of 18 Identifiers and Definition of PHI*, U.C. BERKELEY, https://cphs.berkeley.edu/hipaa/hipaa18.html [https://perma.cc/6YFA-RPL9].

23. 45 C.F.R. § 164.514 (2017).

24. *Id.* § 164.500(a) ("[T]he standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.").

25. *Id.* § 160.102(b).

26. *Id.* § 160.103.

27. *Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUM. SERVICES (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/R9VP-WREJ].

Business associates of covered entities are also under HIPAA's purview when they interact with PHI.[28] Business associates are "a person or entity that performs certain functions or activities that involve the use or disclosure of [PHI] on behalf of, or provides services to, a covered entity."[29] HHS expanded the definition of "business associates" in 2013 to include subcontractors of business associates.[30] Therefore, business associates of covered entities and subcontractors of business associates, those "to whom a business associate has delegated a function, activity, or service the business associate has agreed to perform for a covered entity or business associate," are subject to HIPAA's Privacy and Security Rule's compliance obligations.[31]

2. HIPAA's Regulations that Protect Patient Health Information

In response to the growing concerns surrounding health information privacy, HHS promulgated the HIPAA Privacy, Security, Enforcement, and Breach Notification rules. These rules govern how covered entities and their business associates transmit, maintain, use, and otherwise interact with PHI. This Section describes the rules and their various protections in turn.

28. 45 C.F.R. § 160.102(b) (2017).

29. *Business Associates*, U.S. DEP'T OF HEALTH & HUM. SERVICES (May 24, 2019), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [https://perma.cc/65TK-Q9X9]. Business associates perform certain functions and activities for covered entities and provide certain services. 45 C.F.R. § 160.103 (2017). These functions and activities include claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. *Business Associates*, *supra*. Business associates provide services that are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. *Id.*

30. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Heath Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg., 5566, 5573 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164); *Final HIPAA Amendments Expand HIPAA Net: Business Associates Now Required to Enter Business Associate Agreements with Subcontractors*, DUANE MORRIS (Jan. 23, 2013), https://www.duanemorris.com/alerts/final_HIPAA_amendments_expand_HIPAA_net_4724.html [https://perma.cc/ZXT7-CGXZ].

31. *Business Associates*, *supra* note 29; *see also* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Heath Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. at 5573; DUANE MORRIS, *supra* note 30.

a. The HIPAA Privacy Rule

The HIPAA Privacy Rule's purpose includes "protect[ing] and enhanc[ing] the rights of consumers" with regards to their health information, improving the quality of U.S. health care by "restoring trust in the health care system," and "improv[ing] the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection."[32] The Privacy Rule safeguards any PHI that is held by a covered entity or business associate[33] and "define[s] and limit[s] the circumstances" in which PHI can be used or disclosed.[34] This entitles individuals to certain rights concerning their PHI, such as the right to know who has received their records[35] and to place restrictions on who can access their information.[36]

Generally, PHI cannot be used or disclosed unless the Privacy Rule requires or permits it or the individual authorizes it.[37] The Privacy Rule requires disclosure only when the individual requests access to it or when HHS is investigating the entity's HIPAA compliance.[38] However, covered entities may use or disclose PHI without the individual's authorization in circumstances ranging from "treatment, payment, [and] health care operations" to "public health activities."[39] The Privacy Rule

32. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000) (codified at 45 C.F.R. §§ 160, 164).

33. 45 C.F.R. § 160.103 (2017). Generally, covered entities cannot release PHI without the patient's prior authorization. *Id.* § 164.514. See *supra* Part I.A.1 for a discussion of "covered entities" and "business associates."

34. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/8K4H-JCGQ].

35. 45 C.F.R. § 164.528.

36. *Id.* § 164.510.

37. *Id.* § 164.502(a).

38. *Id.* § 164.502(a)(2). Upon the individual's request, covered entities must also provide an accounting of the disclosures of the individual's PHI. *Id.*

39. *Id.* §§ 164.502(a)(1), .512(b). PHI may also be disclosed without an individual's authorization for the following reasons or situations: (1) "[t]o the individual"; (2) "[i]ncident to a use or disclosure otherwise permitted or required"; (3) where the individual has the opportunity to agree or object; and (4) as part of a "limited data set" for research, public health, or health care operations purposes. *Id.* §§ 164.502(a)(1), .510, .512(b), .514(e)(1).

expressly prohibits the sale of PHI[40] or the use of PHI in marketing[41] without prior authorization.

b. The HIPAA Security Rule

The HIPAA Security Rule sets national standards for the protection of electronic health information[42] and does so through its proscribed data security measures.[43] Once the covered entity or business associate has a patient's PHI, it must (1) "[e]nsure the confidentiality, integrity, and availability" of the information; (2) protect the information against "any reasonably anticipated threats or hazards"; (3) protect against unpermitted or unnecessary "reasonably anticipated uses or disclosures" of the information; and (4) ensure its workforce is compliant with the Security Rule.[44]

Aside from the aforementioned general requirements, the HIPAA Security Rule also requires covered entities and business associates to implement specific administrative, physical, and technical safeguards to protect the PHI.[45] The HIPAA Security Rule specifically allows for flexibility in its implementation—covered entities and business associates "may use any security measures that allow [it] to reasonably and appropriately implement the standards and implementation specifications."[46] This means "smaller and less complex operations can institute more

40. *Id.* § 164.502(a)(5)(ii). Any authorization "must state that the disclosure will result in remuneration to the covered entity." *Id.* § 164.508(a)(4).

41. *Id.* § 164.508(a)(3). The HIPAA regulations define "marketing" as a "communication about a product or service that encourages recipients of the communication to purchase or use the product or service." *Id.* § 164.501. However, this definition contains several notable exceptions. These include communications such as refill reminders, face-to-face communications, and communications regarding an individual's treatment. *Id.* §§ 164.501, 164.508(a)(3).

42. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (codified at 45 C.F.R. §§ 160, 162, 164) ("The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information.").

43. *See* 45 C.F.R. § 164.306.

44. *Id.* § 164.306(a).

45. U.S. DEP'T OF HEALTH & HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 16 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/B2K8-6Z83].

46. 45 C.F.R. § 164.306(b).

cost-conscious means to remain lawful under HIPAA and can change with new technologies."[47]

c. The HIPAA Enforcement Rule

The HIPAA Enforcement Rule created enforcement mechanisms for the HIPAA Privacy and Security Rules.[48] Individuals may file complaints with the Secretary of HHS if they believe a covered entity or business associate isn't complying with the HIPAA Privacy and Security Rules.[49] The Secretary investigates these complaints and may impose civil penalties against the violating entity.[50] Criminal penalties can be imposed by the Department of Justice for more egregious HIPAA violations.[51] Most important to this Note is what the HIPAA Enforcement Rule does not contain: a private right of action for those whose PHI has been compromised.[52] This limits patients' and consumers' federal remedies to merely filing complaints with the HHS Secretary. While there is no federal private right of action under

47. Alexis Guadarrama, Comment, *Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry*, 55 HOUS. L. REV. 999, 1008 (2017).

48. The HIPAA Enforcement Rule also sets out requirements and procedures for compliance reviews, investigations, and hearings. *See, e.g.*, 45 C.F.R. §§ 160.308, .312–.314, .504–.552 (2017). These aspects of the Rule are less pertinent to this Note and are therefore omitted from the discussion of the HIPAA Enforcement Rule in Part I.A.2.c.

49. 45 C.F.R. § 160.306(a) (2017).

50. *Id.* §§ 160.400–.408.

51. Memorandum Op. for the Gen. Counsel of the Dep't of Health & Human Servs. & the Senior Counsel to the Deputy Attorney Gen., 29 Op. O.L.C. 76, 76 (2005), https://www.justice.gov/sites/default/files/olc/opinions/attachments/2015/05/28/op-olc-v029-p0076.pdf [https://perma.cc/8C2W-927P]. Under this recent DOJ guidance, any provider "who violates the privacy rule by knowingly using or obtaining individually identifiable health information or discloses it to someone else may be punished by a fine, prison time, or both." Anne M. Murphy et al., *Criminal Prosecution for Violating HIPAA: An Emerging Threat to Health Care Professionals*, STAT (July 2, 2018), https://www.statnews.com/2018/07/02/criminal-prosecution-violating-hipaa/ [https://perma.cc/S5KB-BA37]. The violating individual only needs to have "knowledge of the facts that constitute the offense," knowledge that their actions violate HIPAA is not required. *Id.* (quoting the Department of Justice's Office of Legal Counsel's guidance to the Department of Health and Human Services).

52. *De Facto Private Right of Action Under HIPAA: Is Ohio Next?*, THOMPSON HINE (Dec. 16, 2014), https://www.thompsonhine.com/publications/de-facto-private-right-of-action-under-hipaa-is-ohio-next [https://perma.cc/GRR9-BSZM].

HIPAA, state private causes of actions are not preempted by HIPAA[53] and at least ten states allow plaintiffs to use HIPAA as a standard of care in negligence claims brought under existing state privacy torts.[54]

Since 2003, the HHS Office of Civil Rights (OCR) has "received over 213,561 HIPAA complaints and has initiated over 975 compliance reviews."[55] The OCR resolved 98% of the cases, the majority of which did not present a case for enforcement.[56] Only sixty-five cases resulted in settlement or imposition of civil monetary penalties by the OCR, totaling $102,681,582.[57] As of July 31, 2018 the OCR has referred 760 cases to the DOJ for potential criminal HIPAA violations.[58]

d. The HIPAA Breach Notification Rule and Other Protections Under the HITECH Act

In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), as part of the American Recovery and Reinvestment Act.[59] The HITECH Act was "designed to promote the widespread adoption and use of health information technology,"[60] but electronic health information privacy and security concerns drove HHS to

53. *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, 102 A.3d 32, 35 (Conn. 2014).

54. *See* THOMPSON HINE, *supra* note 52. It is much more difficult, however, to use HIPAA as a standard of care in a negligence per se claim. *See, e.g.*, Sheldon v. Kettering Health Network, 40 N.E.3d 661 (Ohio Ct. App. 2015) (holding that HIPAA could not be used as the standard of care where there was no state tort for negligent process and the plaintiff's claim was essentially that the defendant violated HIPAA).

55. *Enforcement Highlights*, U.S. DEP'T OF HEALTH & HUM. SERVICES (July 31, 2019), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html [https://perma.cc/MJ67-W68C].

56. The OCR found no eligible case for enforcement in 133,637 of the 210,131 completed cases. *Id.*

57. *Id.*

58. *Id.*

59. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (codified in scattered sections of Titles 16 and 42 of the U.S. Code).

60. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Heath Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg., 5566, 5568 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164).

strengthen HIPAA provisions as well.[61] In 2013, HHS announced a final omnibus rule, which amended HIPAA regulations in accordance with the HITECH Act.[62] The HITECH Act supplemented HIPAA's existing health data protections by implementing measures such as mandatory penalties for violations[63] and breach notification requirements.[64]

These breach notification requirements are better known as the HIPAA Breach Notification Rule, which provides that in the event of a breach of unsecured health information, the responsible covered entity must notify all affected individuals.[65] Large breaches may require the covered entity to inform the appropriate media[66] and the Secretary of HHS.[67]

B. THE CURRENT STATE OF WEARABLE TECHNOLOGY AND ITS USES AND BENEFITS

Wearable technology has been popular for decades. However, the wearable technology discussed in this Note, such as fitness trackers and watches, took off in the early 2010s.[68] It did

61. Timothy Newman & Jennifer Kreick, *The Impact of HIPAA (and Other Federal Law) on Wearable Technology*, 18 SMU SCI. & TECH. L. REV. 429, 432 (2015).

62. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Heath Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164); *Final HIPAA Amendments*, *supra* note 30.

63. 42 U.S.C. § 1320d-5 (2012).

64. 45 C.F.R. § 164.404(a)(1) (2017).

65. *Id.* ("A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach."). In cases of breaches involving business associates of covered entities, the business associate must notify the covered entity, who in turn must notify the affected individuals. *Id.* § 164.410.

66. *Id.* § 164.406 ("For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall . . . notify prominent media outlets serving the State or jurisdiction.").

67. *Id.* § 164.408 (stating that a covered entity shall notify the Secretary in breaches involving 500 or more individuals).

68. Many commentators dubbed 2014 the "Year of Wearable Technology" due to the immense popularity of devices made by companies such as Fitbit, Nike, Samsung, and Google. *See*, *e.g.*, Ewan Spence, *2014 Will Be the Year of Wearable Technology*, FORBES (Nov. 2, 2013, 11:43 AM), https://www.forbes.com/sites/ewanspence/2013/11/02/2014-will-be-the-year-of-wearable

not take long for their popularity to explode: global sales of wearable technology reached 121 million units in 2018 and analysts predict this number will near 200 million by 2021.[69] Interest in wearable technology is equally high—71% of those aged sixteen to twenty-four want wearable technology and 64% of global internet users "have worn a piece of wearable tech already or are 'keen to do so in the future.'"[70] Wearable technology is predicted to become one of the globally best-selling consumer electronics products, behind only smartphones.[71]

Today's wearable technology specifically refers to devices that "incorporate[ ] smart sensors that measure the wearer's personal data."[72] These devices track troves of personal information, including heart rate, sleep patterns, calorie expenditure, blood pressure, and geolocational information and share this information with computers and smartphone devices.[73] The latest version of the Apple Watch can even take an electrocardiogram (EKG),[74] further blurring the line between wearable technology as a consumer good and wearable technology as a medical good. The EKG feature received clearance from the U.S. Food and

-technology/#32132dcac466 [https://perma.cc/T4GS-MTB4].

69. Rob Corder, *Sales of Wearable Technology Rose to 121 Million Units in 2018*, WATCHPRO (Mar. 20, 2019), https://www.watchpro.com/sales-of-wearable-technology-rose-to-121-million-units-in-2018/ [https://perma.cc/5RVP-2PP8].

70. Victor Lipman, *71% of 16-to-24-Year-Olds Want 'Wearable Tech.' Why Don't I Even Want To Wear a Watch?*, FORBES (Sept. 22, 2014, 4:48 PM), https://www.forbes.com/sites/victorlipman/2014/09/22/71-of-16-24s-want-wearable-tech-why-dont-i-even-want-to-wear-a-watch/#3c35578370bf [https://perma.cc/FJ5M-KYXG].

71. Nyshka Chandran, *It's Confirmed: Wearables Are the 'Next Big Thing*,*'* CNBC (Sept. 22, 2015, 7:28 PM), https://www.cnbc.com/2015/09/22/after-smartphones-wearable-tech-poised-to-be-next-big-thing.html [https://perma.cc/CFU6-LDR6].

72. Shivali Best, *What Is Wearable Technology? Everything You Need To Know About the Popular Gadgets*, MIRROR (May 3, 2018, 9:12 AM), https://www.mirror.co.uk/tech/what-wearable-technology-everything-you-12461665 [https://perma.cc/573B-JJ8B].

73. *See supra* INTRODUCTION; *see also* Grant Arnow, Note, *Apple Watch-ing You: Why Wearable Technology Should Be Federally Regulated*, 49 LOY. L.A. L. REV. 607, 610 (2016).

74. Angela Chen, *Why an Apple Watch with EKG Matters*, THE VERGE (Sept. 12, 2018, 1:27 PM), https://www.theverge.com/2018/9/12/17850660/apple-watch-series-4-ekg-electrocardiogram-health-2018 [https://perma.cc/XA54-3UBZ].

Drug Administration (FDA), allowing it to be used as a medical device.[75]

While information such as data collected from the Apple Watch's EKG feature or heart rate can easily be identified as information that would be considered PHI under HIPAA, even geolocational information could constitute PHI in certain circumstances.[76] For example, location data can reveal when and where users go to the doctor's office, identifying at least the physician group visited, and even to the bathroom, indicating particular health problems.[77] Because the user's name and other personal information is stored on the wearable technology, this information could represent PHI.[78]

Personal benefits to wearable technology users include access to personal health information and prompts to develop more healthy habits. Fitbit trackers count steps and allow users to compete with one another in challenges.[79] Apple Watches provide hourly reminders to stand and targeted daily goals for activity.[80] Wearable technology that makes a "meaningful impact" on users' behaviors is likely to be more popular amongst consumers,[81] and devices such as these can encourage habits that help

75. *Id.*

76. For a discussion of HIPAA's definition of health information and PHI, see *supra* note 21 and accompanying text.

77. *See* Alexandra Troiano, Note, *Wearables and Personal Health Data: Putting a Premium on Your Privacy*, 82 BROOK. L. REV. 1715, 1731 (2017).

78. Under HIPAA, PHI consists of any personally identifiable health information that, regardless of form or medium, "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103 (2017). An individual's name is a "personal identifier" necessary to make health information PHI under HIPAA. *See supra* note 23 and accompanying text.

79. *See Fitbit Adventures*, FITBIT, https://www.fitbit.com/challenges/adventures [https://perma.cc/P7TZ-HH2W] (describing how Fitbit users can engage in daily or weekly challenges against other users).

80. *See Apple Watch Series 5: Ultimate Workout Partner*, APPLE, https://www.apple.com/apple-watch-series-5/workout/ [https://perma.cc/7U6Z-FUKK] (describing how the Apple Watch sets targeted goals for movement, exercise, and standing).

81. *Cf.* Endeavor Partners, *Inside Wearables: How the Science of Human Behavior Change Offers the Secret to Long-Term Engagement*, MEDIUM (Apr. 21, 2017), https://medium.com/@endeavourprtnrs/inside-wearable-how-the-science-of-human-behavior-change-offers-the-secret-to-long-term-engagement-a15b3c7d4cf3 [https://perma.cc/N9HA-DNQN] ("Products and services that provide utility but fail to have a meaningful impact on users' behaviors and

reduce premature mortality risks.[82] These devices may have significant medical benefits too. Widespread use of wearable technology will allow physicians to more regularly monitor their patients to provide increased quality of care[83] and may reduce medical care costs.[84]

II. THE NEED FOR PROPER REGULATION OF WEARABLE TECHNOLOGY

Although wearable technology provides numerous benefits, it remains essentially unregulated and leaves its users and the healthcare system vulnerable to harm. Wearable technology compromises users' privacy and exposes them to higher risks of hacking. Currently, HIPAA can provide protection to wearable technology users in very limited circumstances, but this extremely narrow application creates a massive gap in health information protection. While HIPAA's current language fails to cover PHI obtained from wearable technology in all circumstances, other laws and regulations do not regulate wearable technology and users' PHI as well as an amended HIPAA would. This Part will address each of these issues in turn.

A. PRIVACY ISSUES WITH WEARABLE TECHNOLOGY AND ITS VULNERABILITY TO HACKING

Wearable technology presents many privacy risks to consumers, and by extension, the healthcare system. Users' data is

habits—such as an activity tracker that provides data but doesn't inspire action—end up failing in the market. Users quickly abandon wearables that don't help them make positive changes.").

82. *See* Alpa Patel et al., *Leisure Time Spent Sitting in Relation to Total Mortality in a Prospective Cohort of US Adults*, 172 AM. J. EPIDEMIOLOGY 419, 419 (2010) ("There is a growing body of evidence showing that reducing the amount of time spent sitting [may relate] to total mortality . . . .").

83. *See* Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1192–93 (2014) ("Patients and providers can then use this data to better tailor care, to better coordinate care . . . . Constant monitoring might give providers more lead-time to respond to life-threatening conditions, or even predict them ahead of time, and could reduce hospital readmission rates.").

84. *Id.* at 1195 (explaining that mobile technologies, which include wearable technology, can reduce costs "typically by preventing more acute, expensive episodes of care. For example, mobile technologies could reduce the number of hospital visits, physician visits, and other expensive face-to-face consultations. Mobile apps might also enable us to better manage chronic diseases, which account for roughly 75% of all U.S. health spending").

extremely difficult to anonymize—meaning that even where individual identifiers are stripped from user data, users can almost always be identified.[85] For example, if the wearable technology tracks users' gaits, the user can "be 100 percent identified" because individual gaits are totally unique.[86] Even without gait information, 95% of adults can be identified by their physical activity data collected via wearable technology.[87] Additionally, many types of wearable technology pair with mobile health and fitness applications, leaving users at risk of improper third-party data sharing.[88] While HIPAA's Privacy Rule prohibits the sale of PHI,[89] equivalent personal health information collected or transmitted by wearable technology can generally be sold without legal consequences.[90] This means wearable technology users also have no right to know how often and to whom their PHI was sold, leaving them unaware of how their privacy may be compromised.

These privacy concerns are not limited to cheaper or less popular wearable technology—a 2015 study by HP found that all of the top ten most popular smartwatches contained "significant

85. FED. TRADE COMM'N, INTERNET OF THINGS WORKSHOP 170 (2013), https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf [https://perma.cc/UVJ5-HFJD].

86. *Id.* at 170–71 ("[T]he CIO of the CIA said you can be 100 percent identified, as an individual, by your Fitbit data. Why? Because no two persons' gaits or ways of moving are the same. We can almost always figure out who you are based on that kind of incredibly rich detail.").

87. Liangyuan Na et al., *Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets from Which Protected Health Information Has Been Removed with Use of Machine Learning*, J. AM. MED. ASS'N NETWORK OPEN 1, Dec. 21, 2018.

88. A 2014 FTC study of twelve mobile health and fitness applications found that user information was sent to seventy-six third-party companies without user knowledge. FED. TRADE COMM'N, CONSUMER GENERATED AND CONTROLLED HEALTH DATA (2014), https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf [https://perma.cc/67CT-C8QT]. The improperly-shared information included device information, consumer specific identities, unique device IDs capable of allowing third parties to track users' devices across apps, and consumer information such as exercise and dietary habits and symptom searches. *Id.*

89. *See supra* Part I.A.2.a.

90. Wearable technology is generally not under HIPAA's purview because wearable technology companies are not covered entities. *See supra* Part I.A.1. However, there are some circumstances in which wearable technology companies covered by HIPAA. *See infra* discussion of the "who provides it" and "limited voluntary compliance" HIPAA coverage gaps in Part II.B.

vulnerabilities" and presented privacy concerns.[91] This study also highlighted wearable technology's heightened risk of hacking: all of the smartwatches used poor authentication methods and lacked proper encryption, but 70% of the watches lacked any encryption whatsoever for their firmware.[92] This leaves users susceptible to security attacks such as "eavesdropping" and spyware, data injection, phishing, and "brute force attack[s]" that can decipher user data and take control of the device.[93]

Wearable technology's vulnerability to hacking and the type of information it collects creates severe consequences for consumers and providers in the healthcare system. Wearable technology collects many types of health information from its users, which is uniquely sensitive information as compared to other types of data at risk in high-profile data breaches.[94] Apple's new Health Records API, currently still in beta, lets users share their health record data, including "conditions, lab[] [results], medications" and more, with watchOS (Apple Watch) apps.[95] Apple Watches and other similar devices are also prime targets of hackers because of electronic health record's high black market value.[96] If hackers obtain medical records or other personal information, they can misuse the user's medical identity to obtain

91. *HP Study Reveals Smartwatches Vulnerable to Attack*, HP (July 22, 2015), https://www8.hp.com/us/en/hp-news/press-release.html?id=2037386#.Vi18G7crLIU [https://perma.cc/8D45-CCJE].

92. Ke Wan Ching & Manmeet Mahinderjit Singh, *Wearable Technology Devices Security and Privacy Vulnerability Analysis*, 8 INT'L J. NETWORK SECURITY & ITS APPLICATIONS 19, 22 & 22 fig.1 (2016).

93. *Id.* at 23 tbl.1.

94. While not all wearable technology would store personal health information that could be used for medical identity theft, the Apple Watch now supports apps that allow you to access your medical records. *iPhone Users Can View Their Health Records Through the Apple Health App*, HIPAA J. (Jan. 26, 2018), https://www.hipaajournal.com/iphone-users-can-view-health-records-apple-health-app/ [https://perma.cc/QHM4-R9M2]. Medical records contain information that can be used in medical identity theft, which has more severe privacy and financial consequences than financial identity theft. *See* Claire Wilka, Note, *The Effects of* Clapper v. Amnesty Int'l USA*: An Improper Tightening of the Requirement for Article III Standing in Medical Data Breach Litigation*, 49 CREIGHTON L. REV. 467, 484 (2016).

95. *HealthKit*, APPLE, https://developer.apple.com/healthkit/ [https://perma.cc/3AC9-3NN7].

96. *How Wearables Could Put Doctors in HIPAA Hot Water*, MDLINX: PHYSICIAN SENSE (Mar. 28, 2019), https://www.mdlinx.com/internal-medicine/article/3586 [https://perma.cc/B3UV-CPJ9].

medical care.[97] Aside from the financial consequences of medical identity theft,[98] it can also result in improper medical care as "[t]he thief's own medical treatment, history, and diagnoses can get mixed up with your own electronic health records . . . ."[99] Unlike financial identity theft, where credit cards can be cancelled, "[b]iometric data such as fingerprints or eye scans, health information, and genetic data cannot be exchanged."[100] Because wearable technology collects such health information, its vulnerability to hacking increases the likelihood for medical identity theft and the consequences thereof.

B. HIPAA'S WEARABLE TECHNOLOGY DATA PROTECTION GAPS

Most wearable technology and its associated applications fall outside of HIPAA's scope. Wearable technology must be used or provided by a covered entity, such as a health care provider, and transmit PHI to fall under HIPAA.[101] Therefore, when an individual purchases and uses wearable technology to manage their health, HIPAA does not apply; however, where a health care provider or insurer provides the individual with the device,

97. Wilka, *supra* note 94, at 476.

98. *See* Sam Draper, *How Data Breach Is Inevitable in Wearable Devices*, WEARABLE TECHS. (Oct. 5, 2018), https://www.wearable-technologies.com/2018/10/how-data-breach-is-inevitable-in-wearable-devices/ [https://perma.cc/X2SC-23CJ] (describing how medical identity theft can lead to increased health insurance costs or even policy cancellation).

99. Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REP. (Aug. 25, 2016), https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ [https://perma.cc/XK4J-ER5M] ("About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft . . . .").

100. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harm*, 96 TEX. L. REV. 737, 757–58 (2018).

101. *Compare* Adam H. Greene, *When HIPAA Applies to Mobile Applications*, MOBI HEALTH NEWS (June 16, 2011, 3:15 AM), https://www.mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications [https://perma.cc/MB6D-AGVB] ("An application that assists a physician with following up with patients would need to be designed to allow the physician to comply with HIPAA."), *with id.* (stating that an application that allowed individuals to track their medication schedules and send their information to their physician would not fall under HIPAA because there is no covered entity involved). Greene's article deals exclusively with mobile applications that track health data, but given the similarities and overlap between mobile applications and wearable technology, which collect larger amounts of personal health information, the same reasoning would very likely apply.

the wearable technology must comply with HIPAA.[102] This leaves massive gaps in HIPAA coverage of personal health information.

1. The "Who Provides It" HIPAA Coverage Gap

A large number of Americans use wearable technology,[103] which collects sensitive information ranging from daily activity to EKG results.[104] While information like this would be covered under HIPAA if it was collected by a covered entity, technology designed for patient-use, independent of covered entity involvement, is not affected by HIPAA.[105] This Note will refer to this gap in HIPAA coverage as the "who provides it" gap.

The "who provides it" gap is best illustrated by insurance programs such as those created by UnitedHealthcare.[106] UnitedHealthcare's Motion program is an employer-sponsored program that allows employers to offer free or discounted wearable devices and insurance discounts to insured employees that track their exercise.[107] Under the Motion program, employers can either directly provide the wearable device to applicable employees, allow employees to sync their existing wearable devices to

102. U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 45, at 9.

103. A 2016 "digital health consumer adoption survey" conducted by Rock Health found that "[n]early a quarter of Americans own a wearable, up from 12% in 2015." Ashlee Adams et al., *50 Things We Now Know About Digital Health Consumers*, ROCK HEALTH (2016), https://rockhealth.com/reports/digital-health-consumer-adoption-2016/ [https://perma.cc/6GWN-QGMH]. Other recent studies have found that 33% of Americans use wearable technology. Shelagh Dolan, *The Wearables in US Healthcare Report: 3 Untapped Opportunities Wearables Present to Health Insurers, Providers, and Employers*, BUS. INSIDER (Sept. 30, 2018, 9:12 AM), https://www.businessinsider.com/9-30-2018-wearables-in-healthcare-b-2018-9 [https://perma.cc/UXY6-PEE7].

104. *See, e.g.*, Arnow, *supra* note 73; Chen, *supra* note 74.

105. Scott Rupp, *App Association Requests Clarity on HIPAA Regulations for Mobile App Developers*, NUEMD (Oct. 2, 2014), https://www.nuemd.com/news/2014/10/02/app-association-requests-clarity-hipaa-regulations-mobile-app-developers [https://perma.cc/X3E4-KYD3].

106. N.L., *Will Wearable Devices Make Us Healthier?*. ECONOMIST (Jan. 2, 2019), https://www.economist.com/the-economist-explains/2019/01/02/will-wearable-devices-make-us-healthier [https://perma.cc/LDK4-3N7Q].

107. Caroline Hroncich, *Fitbit Offers New Wearables to UnitedHealthcare Participants*, EMPLOYEE BENEFIT NEWS (May 14, 2019), https://www.benefitnews.com/news/fitbit-offers-new-wearables-to-unitedhealthcare-participants [https://perma.cc/Q2FG-2C4B].

the program, or provide discounted wearable devices to employees who reach certain fitness goals.[108] Generally, insurance companies financially benefit from having healthier insureds, as the costs for their health care decrease. The Motion program has been very popular with insureds: 45–65% of those eligible to participate in the program registered to do so.[109] Other insurers, such as Blue Cross Blue Shield, Humana, and Aetna, have offered similar incentives to policyholders.[110]

Where a covered entity like UnitedHealthcare (or its related employer-sponsored health plans) provides users with wearable technology, two distinct issues with the "who provides it" gap are exposed. First, where wearable technology is provided by insurers, HIPAA applies because insurers are one type of covered entity. However, HIPAA will not apply to the same types of wearable technology if the consumer directly purchases it. This is the surface level issue in the "who provides it" gap.

Second, even where HIPAA applies because the wearable technology was provided by insurers, there is still an alarming gap in HIPAA coverage. HIPAA may only apply to the *insurers*, because they fall under the definition of covered entities, and not to the wearable technology companies. This means that the data collected from the Fitbits and Apple Watches in UnitedHealthcare's Motion program must be used, stored, and transmitted by UnitedHealthcare in a HIPAA-compliant fashion. However, the same data collected from these devices is not protected under HIPAA while it is collected, used, stored, or transmitted by the wearable technology company unless that company has

108. *Id.*; Michael Potuck, *Promotion to Earn Free Apple Watch with UnitedHealthcare Rolling Out to All Eligible Customers*, 9 TO 5 MAC (Nov. 14, 2018), https://9to5mac.com/2018/11/14/free-apple-watch-with-unitedhealthcare/ [https://perma.cc/4CJU-XMER]; *UnitedHealthcare Motion*, UNITEDHEALTHCARE, https://www.uhc.com/employer/programs-tools/unitedhealthcare-motion [https://perma.cc/6GZS-UYLX].

109. *UnitedHealthcare Motion*, *supra* note 108.

110. Diana Manos, *Health Plans Take Steps to Study Use of Fitness Wearables, Data*, HEALTH DATA MGMT. (Mar. 1, 2019), https://www.healthdatamanagement.com/news/health-plans-take-steps-to-study-use-of-fitness-wearables-data [https://perma.cc/U94W-WU47]; N.L., *supra* note 106; Johanna Mischke, *Why Insurance Firms Increasingly Embracing Wearable Devices and Fitness Trackers*, WEARABLE TECHNOLOGIES (Nov. 12, 2018), https://www.wearable-technologies.com/2018/11/why-insurance-firms-increasingly-embracing-wearable-devices-and-fitness-trackers/ [https://perma.cc/ZL2Y-6XGV].

signed a "Business Associate Agreement" with the insurer.[111] Simply put, in the absence of a Business Associate Agreement, the data is subject to HIPAA when the insurer has it, but not while the wearable technology collects it.

Companies can easily exploit the "who provides it" gap, as Apple did with its Apple Watches in UnitedHealthcare's Motion program. A subtle but important distinction between how the Motion program uses Fitbit devices and how it uses Apple Watch devices illustrates this point: UnitedHealthcare can *provide* the Fitbits to their insureds, but it merely *discounts* its policyholders' purchase of an Apple Watch. Because UnitedHealthcare can provide the relevant Fitbits for free, and Fitbit likely signed Business Associate Agreements with UnitedHealthcare,[112] the Motion Fitbit users' PHI is protected while in both UnitedHealthcare's and Fitbit's custody. However, Motion Apple Watch users either order their device (through the Motion program) for an initial discounted price and must meet certain exercise goals each month in order to avoid paying additional monthly fees, or use their already-purchased Apple Watches.[113] It also appears Apple has not signed any Business Associate Agreements with UnitedHealthcare.[114] Therefore, it's likely that only UnitedHealthcare must meet HIPAA's standards when handling the Motion Apple Watch users' PHI,[115] leaving Apple free from responsibility.

111. 45 C.F.R. §§ 164.502(e), .504(e) (2017).

112. As discussed *infra* in Part II.B.2, Fitbit has voluntarily become HIPAA compliant and therefore likely signed Business Associate Agreements for its dealings with UnitedHealthcare.

113. Potuck, *supra* note 108.

114. A thorough internet search revealed no evidence that Apple signed a Business Associate Agreement for its dealings with UnitedHealthcare. If Apple signed a Business Associate Agreement, this would very likely be huge public news, as it would draw Apple under HIPAA's purview.

115. Given the lack of authority on the subject, it is uncertain whether merely providing a discounted purchase price, linked to its insurance program, would make UnitedHealthcare the "provider" of the devices. However, legal experts advise that covered entities "who have partnered with wearable [technology] companies are responsible for protecting the privacy of patient data." *Cf.* MDLINX: PHYSICIAN SENSE, *supra* note 96 ("If the physician is the one who recommends the wearable to the patient, or is facilitating or interfacing with the wearable company and is accessing the health data generated by the wearable, there is a HIPAA implication . . . ." (internal quotations omitted)). Therefore, it is highly likely that UnitedHealthcare must manage the Apple Watch data in accordance with HIPAA. However, the fact that the policyholders purchase their

2. The "Limited Voluntary Compliance" HIPAA Coverage Gap

Wearable technology companies are clearly not a covered entity under the current HIPAA definition.[116] However, they can become subject to HIPAA regulations if they voluntarily upgrade their data security and privacy programs, so as to become HIPAA compliant, and work as business associates of certain covered entities.[117] Business associates are subject to the same HIPAA regulations as covered entities.[118] Wearable technology companies are voluntarily upgrading their data security measures to become HIPAA compliant, so that they may work directly with covered entities who want to use their products.[119] Despite voluntary compliance with HIPAA, HIPAA regulatory scheme will only apply to the wearable technology subject to those specific business associate agreements. This Note will refer to this gap in HIPAA coverage as the "limited voluntary compliance" gap.

The "limited voluntary compliance" gap is best illustrated by recent changes at Fitbit. In 2015, Fitbit announced its HIPAA compliance program, which upgraded their data privacy and security measures.[120] This allowed its "Fitbit Wellness" program to work more closely with HIPAA covered entities, such as health plans and self-insured employers, because it could now enter into Business Associate Agreements with those covered entities.[121] The Fitbit devices covered under these Business Associate

Apple Watch devices appears to have allowed Apple to evade entering into a Business Associate Agreement, keeping Apple outside of HIPAA's purview.

116. Covered entities include health plans, health care clearinghouses, and health care providers who transmit "any health information in electronic form in connection with a transaction covered by this subchapter." 45 C.F.R. § 160.103 (2017).

117. *See* Fred Donovan, *How Does HIPAA Apply to Wearable Health Technology?*, HEALTH IT SECURITY (July 24, 2018), https://healthitsecurity.com/news/how-does-hipaa-apply-to-wearable-health-technology [https://perma.cc/FU9X-8ZFF] (discussing how wearable technology makers such as Fitbit are voluntarily upgrading their platforms to ensure their wearable technology is HIPAA compliant).

118. *See supra* the discussion of "business associates" in Part I.A.1.

119. Donovan, *supra* note 117.

120. *Fitbit Extends Corporate Wellness Offering with HIPAA Compliant Capabilities*, FITBIT (Sept. 16, 2015), https://investor.fitbit.com/press/press-releases/press-release-details/2015/fitbit-extends-corporate-wellness-offering-with-hipaa-compliant-capabilities/default.aspx [https://perma.cc/B89W-Q5XP].

121. *Id.*

Agreements will be regulated by HIPAA, but the millions of Fitbit devices bought directly by consumers for personal use will be outside of HIPAA's protection and regulation.

While Fitbit appears to be the only wearable technology company that is voluntarily HIPAA compliant, other companies have started to move in that direction. Apple has yet to upgrade its Apple Watch platform to be entirely HIPAA compliant or enter into Business Associate Agreements with covered entities, but it has made several newsworthy steps towards HIPAA compliance.[122] The Apple Watch uses "HealthKit," its health information software, to ensure the user's personal health information is shared securely[123] and has been recently updated to include a section that "allows users to view their medical records directly on their iPhones."[124] Apple Watches also have a third-party app called "AirStrip" that allows users to directly send their HIPAA-compliant data to physicians.[125] Voluntary HIPAA compliance, or steps towards it as in Apple's case, does not ensure that all users of wearable technology will be protected under HIPAA. However, it does suggest that wearable technology companies are aware of the nature of the personal health information they collect and may be anticipating future regulation.

122. It should be noted that Apple has explicitly stated that its iCloud software cannot be used by covered entities or business associates to store PHI. *See Is iCloud HIPAA Compliant?*, HIPAA J. (Feb. 6, 2018), https://www.hipaajournal.com/icloud-hipaa-compliant/ [https://perma.cc/EGA6-Y5ZG] (stating that Apple includes in its Terms & Conditions for iCloud that "the use of iCloud by HIPAA-covered entities or their business associates for storing or sharing ePHI is not permitted, and that doing so would be a violation of HIPAA Rules"). However, this Note will focus exclusively on the Apple Watch in its discussion of wearable technology, and not Apple's iCloud storage system.

123. Pamela Greenstone, *HIPAA Guidelines Should Evolve with Wearable Technology*, HILL (Mar. 14, 2018), https://thehill.com/opinion/healthcare/378450-hipaa-guidelines-should-evolve-with-wearable-technology [https://perma.cc/988U-XRJN].

124. *iPhone Users*, *supra* note 94. This part of the Health app is "based on Fast Healthcare Interoperability Resources (FHIR)—a standard for transferring and sharing electronic medical records" and "[d]ata transmitted to the user's iPhone is encrypted to prevent unauthorized access." *Id.*

125. *See* Jacob Brogan, *Apple's Most Exciting New Design Feature? HIPAA Compliance.*, SLATE (Sept. 10, 2015), https://slate.com/technology/2015/09/apple-s-and-airstrip-s-hipaa-compliant-features-were-the-most-exciting-part-of-its-latest-announcement.html [https://perma.cc/2NVR-LYMP]; Leigh Householder, *HIPAA Compliant Data from the Apple Watch*, SYNEOS HEALTH COMM. (Nov. 30, 2016), https://syneoshealthcommunications.com/blog/hipaa-compliant-data-from-the-apple-watch [https://perma.cc/5LSY-XT4Q].

C. OTHER LAWS AND REGULATIONS THAT COULD AFFECT WEARABLE TECHNOLOGY OR HEALTH DATA OBTAINED FROM THESE DEVICES ARE INADEQUATE

HIPAA is one of several existing federal laws and regulations that fail to regulate wearable technology or protect the data collected from wearable technology. But unlike HIPAA, which provides an appropriate regulatory structure that could provide complete protection of health information from wearable technology, other federal approaches could not properly protect consumers from the risks presented by wearable technology. This Section will address these alternative federal approaches and why they are inadequate regulatory vehicles for wearable technology and the health information it collects.[126]

1. The Electronic Communications Privacy Act of 1986

Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) with the primary purpose of limiting what information can be disclosed to the government, but also to "protect[] individuals' communications . . . from third parties without legitimate authorization to access the messages."[127] Most pertinent to this Note, Title II of the ECPA, the Stored Communications Act (SCA),[128] protects electronically stored communications and their contents.[129] However, the ECPA and the SCA are severely outdated and "did not contemplate modern communication technology."[130]

126. Given the vast range of possibilities that could be discussed, this Section will only examine those approaches identified by other scholars.

127. *Electronic Communications Privacy Act*, UNIV. OF CIN.: OFFICE OF INFO. SECURITY, https://www.uc.edu/infosec/compliance/ecpa.html [https://perma.cc/B8R8-4EBW]; *see also* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

128. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).

129. *Electronic Communications Privacy Act of 1986 (ECPA)*, JUST. INFO. SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 [https://perma.cc/6Z2J-D8CM].

130. Matthew R. Langley, Note, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1642–43 (2015).

As currently written, the ECPA and the SCA do not apply to wearable technology. The SCA limits when providers of an "electronic communication service"[131] or a "remote computing service"[132] can voluntarily disclose customer information to commercial third parties.[133] The stringency of the disclosure laws depends on whether the communications are considered "content"[134] or "noncontent,"[135] as noncontent can be disclosed to any person other than the government without restriction.[136] Though Congress designed the ECPA to regulate electronic communications as they existed in 1986, it is plausible that wearable technology could be considered providers of an electronic communication service and a remote computing service.[137] However,

131. As defined in the SCA, an electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

132. The SCA defines a remote computing service as "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2). An electronic communications system is "any wire, radio, electromagnetic, photooptical [sic] or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14).

133. *See id.* § 2702(a)(1)–(2) (stating that "a person or entity providing an electronic communication service [or a remote computing service] to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service" unless one of the listed exceptions under *id.* § 2702(b) applies).

134. *Id.* § 2510(8) ("[W]hen used with respect to any wire, oral, or electronic communication, [content] includes any information concerning the substance, purport, or meaning of that communication."). The disclosure rules for content are much stricter and do not allow for disclosure to nongovernmental third parties. *See id.* § 2702(b).

135. Noncontent is not expressly defined in the ECPA or the SCA, but includes customer records and "information about the communication that the network uses to deliver and process the content information." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1228 (2004).

136. 18 U.S.C. § 2702(c)(6).

137. For an analysis of how wearable technology could be considered to provide both an electronic communication service and a remote computing service, see Langley, *supra* note 130, at 1653–55 ("When an individual uses the Apple Watch to voluntarily communicate heart rate data to a friend, the health app is functioning as an electronic communication service; clearly this is an electronic communication, and the health app is providing the ability to send the user's heart rate data to a friend. When the wearable is merely collecting heart rate data from the user, it is functioning as a remote computing service; the

health data from wearable technology would likely not be considered "content" under current case law because it generates automatically and is therefore not an "intended" communication.[138] Therefore, wearable technology companies can disclose or sell customer health data to commercial third-parties without violating the SCA.

2. FDA Regulations

The FDA has jurisdiction to regulate medical "devices" under the Federal Food, Drug, and Cosmetic Act.[139] Medical devices are broadly defined to include "any product intended to diagnose, cure, mitigate, treat, or prevent disease, or any product intended to affect the structure or function of the body."[140] Under such broad language, wearable technology appears to be subject to the FDA's jurisdiction because it can be used to "prevent disease" by encouraging healthy habits.[141] However, the FDA focuses on a product's "intended use," as defined by the product's manufacturer.[142] FDA regulations define "intended use" as how the company marketing the devices objectively intended it to be used, including the claims made about the device.[143] This allows wearable technology companies to avoid FDA regulation by labeling and marketing their devices as ones for personal use. Additionally, 2016 FDA guidance states that the FDA will not regulate products so long as they are "intended for only general wellness use" and "low risk."[144] Wearable technology fits squarely within

health app is available to anyone with a wearable, its main function is to track heart rate data, and it stores and processes data for the user.").

138. *See In re* Zynga Privacy Litig., 750 F.3d 1098, 1106 (9th Cir. 2014) (holding that content "refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication"); *In re* iPhone App. Litig., 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (holding that geolocational information was not "content" under the SCA because it "generated automatically, rather than through the intent of the user").

139. *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)).

140. Cortez, *supra* note 83, at 1200–01 (citing 21 U.S.C. § 321(h) (2012)).

141. *Id.*

142. *See* Scott Danzis, *FDA Proposes Amending the Definition of "Intended Use,"* INSIDE MED. DEVICES (Sept. 28, 2015), https://www.insidemedicaldevices.com/2015/09/fda-proposes-amending-the-definition-of-intended-use/ [https://perma.cc/HBV3-GZP2].

143. *See* 21 C.F.R. § 801.4 (2013).

144. FDA, GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES 2–5 (2016).

the category of low-risk general wellness products, and thus the FDA generally has not regulated these devices.[145]

Clearly, neither the ECPA nor the FDA are appropriately equipped to regulate wearable technology and the health information derived from it. Where these alternative federal approaches to wearable technology regulation fail, HIPAA has the potential to properly regulate wearable technology and protect consumers with minimal changes.

III. PROPOSED SOLUTION: EXPANDING THE DEFINITION OF HIPAA'S "COVERED ENTITIES" TO INCLUDE WEARABLE TECHNOLOGY COMPANIES WHOSE DEVICES INTERACT WITH PERSONAL HEALTH INFORMATION

Wearable technology collects, stores, and transmits large amounts of personal health information in a more invasive manner than that of health care providers.[146] It is also vulnerable to hacking, putting users' health information at significant risk.[147] HIPAA provides an existing framework for sensitive health information—a framework that already applies to wearable technology in select circumstances[148]—that could easily remedy these problems. Amending HIPAA to incorporate new technology and adapt to the current age is very possible, as evidenced by the HITECH Act.[149] This makes HIPAA the ideal regulatory

General wellness products have intended uses that "relate to sustaining or offering general improvement to functions associated with a general state of health," regardless of whether they reference diseases or conditions. *Id.* at 3–4. Low-risk products are not invasive, do not require implantation, and do not "involve an intervention or technology that may pose a risk to the safety of users and other persons if specific regulatory controls are not applied, such as risks from lasers or radiation exposure." *Id.* at 5.

145. Though not explicitly mentioned in the guidance, wearable technology such as the Fitbit or Apple Watch would qualify as low-risk general wellness products because their intended uses relate to general health improvement and they are non-invasive external devices. Wearable technology is also extremely similar to the listed examples of low-risk general wellness devices, such as those that "monitor[] and record[] daily energy expenditure and cardiovascular workout activities" or "monitor the pulse rates of users during exercise . . . ." *Id.* at 6–7.

146. *See, e.g.*, *supra* notes 1–5 and accompanying text.

147. *See supra* Part II.A.

148. *See* discussion *supra* Part II.B.

149. Modifications to the HIPAA Privacy, Security, Enforcement, and

mechanism for the health information derived from wearable technology. This Part proposes an amendment to HIPAA's definition of "covered entities," responds to the potential criticisms of this approach, and concludes by demonstrating why other proposed solutions, unrelated to HIPAA, would be inadequate.

A. THE PROPOSED AMENDMENT TO HIPAA'S DEFINITION OF "COVERED ENTITIES"

Amending the narrow definition of "covered entities" is the best approach to updating HIPAA to include wearable technology. Currently, covered entities consist of health plans, health plan clearinghouses, and health care providers "who transmit[] any health information in electronic form in connection with a transaction covered by this subchapter."[150] To adequately accommodate wearable technology, the definition given in section 160.103 and restated in section 160.102(b) should be amended by adding:

> (4) A company that manufactures wearable technology[151] that tracks, collects, stores, or transmits any health information in electronic form. Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to only those wearable technology products that collect, store, or transmit health information and not to the other products manufactured by companies under paragraph (4) of this definition.[152]

Breach Notification Rules Under the Heath Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566, 5568 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164) (describing how Congress passed the HITECH Act thirteen years after passing HIPAA to update HIPAA and "promote the widespread adoption and interoperability of health information technology"); *see also* HITECH Act of 2009, Pub. L. No. 111-5, 123 Stat. 115.

150. 45 C.F.R. §§ 160.102(b), .103 (2017).

151. Wearable technology would also have to be defined in HIPAA's statutory definitions, provided in 45 C.F.R. § 160.103. This Note proposes a definition of "an electronic device that (1) can be worn on the body, (2) connects to the Internet, and (3) tracks, collects, stores, or transmits information about its user." While this definition may appear broad, it is significantly limited by the proposed "covered entities" language in paragraph (4) that would limit HIPAA's application to only those wearable technology companies whose devices interact with health information.

152. To ensure consistency, HIPAA's definitions of "health information" and "individually identifiable health information" would also have to be amended to include "wearable technology company as defined in § 160.103." For the current definitions of "health information" and "individually identifiable health information," see *id.* § 160.103.

Under the proposed language, companies that manufacture wearable technology will be covered entities and subject to HIPAA's Privacy, Security, and Breach Notification rules. This definition includes wearable technology companies that exclusively sell these devices, like Fitbit, and those that sell a variety of products, like Apple. In a mixed-products company like Apple, HIPAA regulatory requirements would only apply to its Apple Watch—Apple would not be required to update its unrelated applications and products that do not interact with personal health information. The proposed language should not take immediate effect, but rather take effect on a set compliance date that would allow wearable technology companies to develop and implement their respective HIPAA compliance programs. This is standard practice for HIPAA regulatory updates[153] and will allow affected companies to strengthen their security and privacy measures without fear of punitive action by HHS.

This Note is not the first to propose a "covered entities" approach to the wearable technology conundrum,[154] but it is the first to provide a comprehensive and workable one. Another scholar suggests amending the definition of "covered entities" to include "companies that produce devices, a primary purpose of which is achieved through collecting health information from individuals."[155] This introduces an admittedly "unwieldy" primary purpose test that would require judicial intervention to interpret the definition.[156] Not only would this be burdensome on HIPAA enforcement, it would be costly on both the government and wearable technology companies. It also would create a massive loophole ripe for exploitation: companies like Apple could merely

153. When the HHS final rule implementing stricter standards under the HITECH Act was passed, its compliance date was nearly six months after its effective date. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Heath Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. at 5566 (stating that the effective date of the final rule was March 26, 2013 and the compliance date for the applicable requirements was September 23, 2013). Given that this proposed regulation would draw an entirely new industry into HIPAA's regulatory purview, the compliance date would likely have to be further out than six months.

154. *See, e.g.*, Arnow, *supra* note 73.

155. John T. Katuska, Note, *Wearing Down HIPAA: How Wearable Technologies Erode Privacy Protections*, 44 J. CORP. L. 385, 399 (2018).

156. *Id.*

argue their devices' primary purpose is not collecting health information, or re-market their devices as such. Finally, it does not define the term "devices" and thus could require the *entire* company to become HIPAA compliant, including with respect to its devices that lack the trademark features (i.e. Internet-connectedness) and higher privacy and security needs of true wearable technology.[157] This would significantly raise compliance costs for wearable technology companies, making them much more likely to object a possible definitional amendment of HIPAA's "covered entities."

Amending the definition to "covered entities" is not the only possible HIPAA-based solution; some scholars have suggested amending the definition of "business associates" to include wearable technology companies whose products are used in conjunction with medical treatment or health insurance.[158] This, however, would be unnecessarily complex. For example, following the "business associates" amendment approach would require covered entities like doctors to sign Business Associate Agreements with wearable technology companies each time they "prescribed" a wearable device to assist in medical treatment.[159] This approach would also essentially replicate the HIPAA coverage gaps discussed in Part II.B.

Conversely, this Note's "covered entities" amendment approach would regulate *all* wearable technology that interacts with personal health information, eliminating the "who provides it" and "limited voluntary compliance" HIPAA coverage gaps.[160] It would provide uniform regulation for all wearable technology users and protect their invaluable health information. Wearable

157. *Id.*

158. *See, e.g.*, Arnow, *supra* note 73, at 632–33.

159. Covered entities are required to enter into "Business Associate Agreements," or "business associate contracts," with their business associates that handle PHI. *See* 45 C.F.R. 164.504(e) (2017). These agreements must meet several requirements, such as defining the permitted uses and disclosures of PHI by the business associate. *See Business Associate Contracts*, U.S. DEP'T OF HEALTH & HUM. SERVICES (Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html [https://perma.cc/QAE5-G4ZT].

160. For explanations of the "who provides it" and the "limited voluntary compliance" HIPAA coverage gaps, see *supra* Part II.B.

technology companies would be required to meet HIPAA data security standards,[161] forcing them to remedy their devices' significant vulnerabilities to hacking.[162] Wearable technology users would also gain several more important protections: notification in the case of data breach,[163] meaningful protection against unauthorized sales of their health information and use of their health information for marketing purposes,[164] and a right to an accounting of the disclosures of their PHI.[165]

B. POTENTIAL CRITICISMS OF THIS APPROACH

The HIPAA "covered entities" approach represents the best and most realistic option for regulating the health information derived from wearable technology. However, it is not without its flaws. The potential criticisms of this approach would likely fall into two general categories: concerns that it would do too little for consumers and concerns that it would do too much to the wearable technology industry. This Section will respond to each of these categories in turn.

The HIPAA "covered entities" approach could be criticized as inadequate for consumers for two reasons. First, it fails to protect users' non-health information. Under this approach, a breach involving geolocational data would not be affected by HIPAA, and users would have little to no remedies.[166] Though

161. *See supra* Part I.A.2.b.

162. For a discussion of wearable technology's security vulnerabilities, see *supra* Part II.A.

163. *See supra* Part I.A.2.d.

164. *See supra* Part I.A.2.a. HIPAA's protection against unauthorized disclosure or use is especially meaningful in the wearable technology context. Authorizations for the user or disclosure of PHI generally cannot be combined with any other document to create a "compound authorization"—effectively barring wearable technology companies from inserting broad authorization agreements into their terms of service or other fine-print agreements. 45 C.F.R. § 164.508(b)(3) (2017). Additionally, the authorization must specify the purpose of the use or disclosure, who will have access to the information, and a definite expiration date for the authorization. *Id.* § 164.508(c)(1). All authorizations must be signed and dated by the individual and must use plain language, amongst many other stringent requirements. *Id.* § 164.508(c)(2).

165. *See supra* Part I.A.2.a.

166. Most states do not have a constitutional right to privacy that applies to non-governmental entities. *See infra* notes 188–89 and accompanying text.

this is a serious issue, the exposure of health information presents the greatest risk to wearable technology users.[167] Lawmakers should regulate this information in a more urgent manner than non-health information, even if that means temporarily foregoing the regulation of non-health information.[168] Second, this approach is limited to HIPAA's remedies, which notably lacks a federal private enforcement right. While federal remedies would be limited to filing a complaint with the HHS Secretary, consumers in a limited number of states could attempt to sue wearable technology companies through private enforcement at the state level.[169] This would likely be limited to states who already have privacy torts that could encompass HIPAA violations, like torts for improper disclosures of medical information.[170] This is an incomplete and imperfect solution, but this issue cannot be remedied without a complete overhaul to HIPAA's enforcement scheme, which is outside the scope of this Note.

The HIPAA "covered entities" approach could also be viewed as a potential overregulation of wearable technology companies. This approach would bring an entirely new industry under HIPAA's purview and subject them to new, rigorous privacy and security standards. The imposition of a new regulatory scheme could theoretically stifle industry innovation; however, this is extremely unlikely. Companies like Fitbit have demonstrated that HIPAA compliance is not only possible, it is profitable.[171] Other

167. *See supra* Part II.A.

168. This approach also does not preclude other laws or regulations from regulating and protecting users' non-health information collected by wearable technology. Electronic information privacy is a widespread issue that affects more than just wearable technology and would likely need to be regulated under a new federal law or agency. However, this issue is beyond the scope of this Note.

169. *See supra* notes 53–54 and accompanying text.

170. For the discussion of state private remedies for HIPAA violations, see *supra* Part I.A.2.c. Some states are going beyond HIPAA and proposing legislation that would treat personal health data like property. *See* Stephanie Condon, *Oregon Lawmakers Roll Out Bill to Let Patients Get Paid for Health Data*, ZDNET (Jan. 29, 2019, 7:42 PM), https://www.zdnet.com/article/oregon-lawmakers-roll-out-bill-to-let-patients-get-paid-for-health-data/ [https://perma.cc/6EP5-MLUS] (discussing the Health Information Property Act, which would, in part, "allow consumers to elect to receive payment in exchange for authorizing the de-identification of their PHI for purpose of sale").

171. For the discussion of Fitbit's voluntary HIPAA compliance, see *supra* Part II.B.2.

large wearable technology companies are very likely capable of HIPAA compliance.[172] Even smaller wearable technology companies would not be over-burdened by this approach because the HIPAA Security Rule allows smaller companies to implement security measures appropriate for their size and budget.[173] Additionally, HIPAA compliance offers lucrative business opportunities to wearable technology companies because it allows them to partner with traditional health care providers such as insurance companies.[174] This approach could actually foster innovation in the wearable technology industry as wearable technology companies can work more closely with health care providers to create new types of devices.

C. OTHER PROPOSED STATUTORY AND REGULATORY APPROACHES TO REGULATING HEALTH INFORMATION COLLECTED BY WEARABLE TECHNOLOGY WOULD BE INADEQUATE

Amending HIPAA is not the only proposed solution to the problem discussed in this Note. Other scholars have proposed amending the ECPA, adapting FDA regulations, and creating new federal agencies to better address wearable technology. State approaches, such as constitutional amendments and legislative changes, have also been discussed. But unlike the proposed amendment to HIPAA's "covered entities," other federal and state approaches could not properly protect consumers from

172. The estimated costs of HIPAA compliance vary based on organization size, and there is very little publicly available information on actual compliance costs. In its first twenty-eight months of HIPAA compliance, the Mayo Clinic's HIPAA start-up costs were slightly over $4.6 million. *See* Arthur R. Williams et al., *HIPAA Costs and Patient Perceptions of Privacy Safeguards at Mayo Clinic*, 34 JOINT COMMISSION ON QUALITY & PATIENT SAFETY 27, 30 tbl.2 (2008). Its annual HIPAA operating costs, for 2001–2003, were $1.27 million. *Id.* at 31. Mayo Clinic is an extremely large health care provider with annual revenues of nearly $12 billion, so it is likely that its HIPAA compliance costs are on the higher end. *See Mayo Clinic Facts*, MAYO CLINIC, https://www.mayoclinic.org/about-mayo-clinic/facts-statistics [https://perma.cc/K8E9-ZKA2]. Assuming similar compliance costs for large wearable technology companies, it is also likely that they can afford both the start-up and annual operating costs of HIPAA compliance.

173. *See supra* notes 46–47 and accompanying text.

174. For the discussion of Fitbit's voluntary HIPAA compliance, see *supra* Part II.B.2.

the risks to health information presented by wearable technology. This Section will address each of these proposals and their inadequacies in turn.

1. The Electronic Communications Privacy Act of 1986

Some scholars suggest amending the SCA to include personal health data, which would require updating the current definition of "content" and adding a definition for personal health data.[175] This proposal, however, is utterly inadequate for several reasons. First, the ECPA and SCA primarily limit disclosures of electronic communications to the government but say very little about disclosures to commercial third parties. Currently, wearable technology users face a greater risk of improper third-party disclosures to commercial parties than to governmental entities.[176] Second, regulating wearable technology through the ECPA and SCA would only protect users against improper disclosures of their health information. It would not provide users with the right to know who has received their health information, require wearable technology companies to meet security requirements for storing said information, or require companies to notify users of breaches that may affect them.[177] Because health information is markedly more sensitive than the electronic communications protected by the ECPA and SCA, it should be regulated under a more comprehensive regulatory scheme designed to protect such sensitive information.

2. FDA Regulations

Hypothetically, the FDA could regulate wearable technology by amending its definition of "medical devices" to include wearable technology that collects health information or issuing guidance that requires these devices to receive FDA approval. This seems unlikely, though, given the FDA is already administratively overburdened[178] and may not be capable of regulating an

175. *See* Langley, *supra* note 130, at 1658–59.

176. *See supra* note 88 and accompanying text.

177. For additional examples of protections that would be provided under HIPAA, see *supra* Parts I.A.2.a–b, d.

178. *See, e.g.*, David C. Vladeck, *The FDA and Deference Lost: A Self-Inflicted Wound or the Product of a Wounded Agency? A Response to Professor O'Reilly*, 93 Cornell L. Rev. 981, 983 (2008) ("By 2001, if not before, the Agency did not have the necessary resources to fulfill its mission; it is the FDA's resource deficit, as much as regulatory capture, that is to blame for the string of regulatory

entirely new category of products. Even if the FDA was able to regulate wearable technology effectively, this regulation would only address the safety and effectiveness of wearable technology as medical devices.[179] It would not address the privacy and security of users' sensitive health information, making it an incomplete and inadequate regulatory approach to wearable technology that collects health information.

3. Creation of a New Federal Agency

Clearly, no federal law or regulation currently provides the level of regulation needed to protect consumers from the risks of wearable technology. Instead of updating existing laws or regulations, some have suggested creating a new federal agency to regulate internet privacy and data security.[180] While this would "align the current patchwork regulatory structure,"[181] it appears unlikely that an increasingly inefficient Congress[182] would create a new agency *and* that agency would successfully avoid the same issues plaguing existing agencies that attempt to regulate wearable technology.[183] Additionally, an agency whose purpose is to regulate internet privacy and data security may not be equipped to specifically regulate wearable technology for the

failures that began then and have accelerated since. The FDA is chronically underfunded, overworked, incapable of effectively tackling the massive job Congress assigned it, and bereft of the leadership needed to defend itself in the court of public opinion.").

179. *Is Your Product Regulated?*, FDA, https://www.fda.gov/medical-devices/overview-device-regulation/your-product-regulated/ [https://perma.cc/2MSC-Q3BR] ("The U.S. Food and Drug Administration (FDA) regulates medical devices to assure their safety and effectiveness."). For a list of the FDA's basic regulatory requirements for medical devices, see 21 C.F.R. §§ 801, 803, 807, 812, 814, 820 (2017). *See also Overview of Device Regulation*, FDA, https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation/ [https://perma.cc/EP8N-4RV4].

180. *See* Arnow, *supra* note 73, at 630–31.

181. *Id.* at 630.

182. *See, e.g.*, Drew DeSilver, *Despite GOP Control of Congress and White House, Lawmaking Lagged in 2017*, FINANCIAL (Jan. 11, 2018), https://www.finchannel.com/world/america/70777-despite-gop-control-of-congress-and-white-house-lawmaking-lagged-in-2017 [https://perma.cc/7EMF-ZJRM] (describing how the 115th Congress was the fourth least productive in the past thirty years).

183. *See, e.g.*, Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175 (2014) (discussing how the FDA has long struggled to regulate continuously changing and disruptive technology).

risks it presents to users' health information.[184] In order to properly protect health information collected by wearable technology, this agency would essentially have to replicate HIPAA's regulatory structure.[185] But HIPAA already applies to wearable technology in certain circumstances,[186] so any replication of health information regulation would be redundant and cause jurisdictional conflicts between HHS and the new agency. For these reasons, creating a new federal agency is not the best solution to regulating wearable technology and the data it collects.

4. State-Based Approaches

Scholars have also proposed state-based solutions to regulating health information from wearable technology.[187] The first type of state-based solution is amending state constitutions to include a right to privacy. Few states include a right to privacy in their constitutions[188] and they vary on whether that protection applies against nongovernmental entities.[189] Those proposing state constitutional amendments advocate for a constitutional right to privacy that protects against intrusion by private parties, which would allow individuals to bring suit for violations to their constitutional right to privacy if their private health information was exposed.[190] The second type of state-based solution is amending state health information legislation to protect

184. For a discussion of the sensitive nature of health information and the risks posed to consumers by medical identity theft, see *supra* Part II.A.

185. For a discussion of HIPAA's key regulatory provisions, see *supra* Part I.A.2.

186. For an explanation of when HIPAA applies to wearable technology, see *supra* Part II.B.

187. *See* Steven Spann, Note, *Wearable Fitness Devices: Personal Health Data Privacy in Washington State*, 39 SEATTLE U. L. REV. 1411, 1426–32 (2016) (proposing changes to the Washington state constitution or state legislation).

188. *See* ALASKA CONST. art. I, § 22 (amended 1972); ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, §§ 12 (amended 1982), 23 (amended 1998); HAW. CONST. art. I, §§ 6, 7 (amended 1978); ILL. CONST. art. I, §§ 6, 12; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7.

189. *Compare* State v. Hinton, 319 P.3d 9, 12 (Wash. 2014) (stating that the Washington state constitution's right to privacy "protects citizens from governmental intrusion into their private affairs without the authority of law"), *with* Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 644 (Cal. 1994) ("[T]he Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities.").

190. Spann, *supra* note 187, at 1428–30.

data derived from wearable technology.[191] These state laws provide similar protection to HIPAA, but also face similar applicability issues when it comes to wearable technology. Some state legislation would need significant overhaul before it could plausibly apply to wearable technology,[192] but other states have legislation that could apply to wearable technology as is.[193]

Amendments to state constitutions and to state legislation are both inadequate solutions to the problems posed by wearable technology. For instance, creating a right to privacy in state constitutions only allows individuals to sue once that right has been violated. It does nothing to protect that private information—other than to incidentally incentivize companies to better protect users' data out of fear of being sued. Both state-based solutions would fail for another reason: massive inconsistency across the states. If states were to independently amend their constitutions and health information laws, the standards for wearable technology health data protection would greatly vary. This would harm wearable technology companies and their consumers. Wearable technology companies would have to create products that meet all of the varying requirements across the states.[194] Their customers would have different rights depending on where they live, unfairly allowing those with more comprehensive legislative schemes to have more remedies for harm created by the same breach.

191. *Id.* at 1429–33.

192. *Id.* at 1429–30 (discussing the four definitional amendments to Washington's Health Information Act that would need to be made to accommodate regulation of health information derived from wearable technology).

193. California's Confidentiality of Medical Information Act applies more broadly than HIPAA, including to entities other than health care providers who maintain medical information. CAL. CIV. CODE § 56.06(a) (West 2012). Texas's Medical Records Privacy Act applies to "any person who . . . engages in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information." Medical Records Privacy Act, TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2) (West 2015).

194. It is possible, however, that inconsistent state laws would result in wearable technology companies adopting the standards required by the most stringent state(s). This would benefit consumers in terms of the data security and privacy measures enacted by the wearable company but would likely not affect variations in available remedies or data breach notification requirements.

CONCLUSION

Health information and medical records are now generated by a growing number of non-medical entities, including wearable technology. And wearable technology has unprecedented levels of access to its users' health information—information, that if collected by doctor or insurance company, would be subject to extensive security and privacy regulations. Its lax security standards and constant collection of health information means that hackers have easy access to vastly more information than if they were to target a traditional health care entity.

This Note advocates for equal regulation and protection of personal health information, regardless of how that information is initially collected. It proposes an expanded definition of "covered entities" to draw wearable technology companies into HIPAA's regulatory purview, which provides uniform regulation of health information and closes the existing HIPAA coverage gaps for wearable technology. This proposal is not only a viable option, it is the best option for doing so. Medical privacy is one of the foundational pillars of the American health care system, but this pillar is cracked. HIPAA must be updated to reflect the modern reality of the health care system before it crumbles.