Wearing Down HIPAA: How Wearable Technologies Erode Privacy Protections

John T. Katuska

I. INTRODUCTION

With the increasing popularity of wearable health technology,[1] more and more

1. For the purposes of this Note, wearable health technology includes all wearable devices that can or do collect and track health, fitness, or wellness information of the wearer. Many of the assertions made in this Note

personal health data is being collected. Because this data is collected for personal use and often by technology companies that do not deal in healthcare, the privacy protections provided by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2] may not always be available to individuals using these technologies. This Note argues for an expansion of HIPAA to further guard individuals' protected health information (PHI) by broadening the scope of what is considered a covered entity. The Note will discuss the current HIPAA definitions of covered entities and PHI, analyze whether and how those definitions apply to technology companies that produce wearable health technology, and address whether such technology companies are required to abide by HIPAA's Privacy Rule and Security Rule to protect individuals' health information.

Part II of this Note will explore what kinds of businesses are subject to HIPAA regulations, what type of health information is protected by HIPAA's Privacy Rule and Security Rule, and what technological developments have emerged that confuse HIPAA's application. Part III will analyze the problems that arise when determining whether health technology companies are subject to HIPAA's regulations. Part III will also discuss the issues that may arise if these companies are not covered by HIPAA. Part IV recommends changing HIPAA's definition of covered entities to better protect PHI and regulate the current health technology market.

II. BACKGROUND

Passed in 1996, HIPAA is federal law aimed at addressing a "variety of issues related to health care" and health information.[3] This Note will focus on Title II of HIPAA, which establishes national standards for health care transactions as well as rules regarding the privacy and security of individualized health information when possessed by certain entities.[4]

HIPAA's protections do not apply to all companies that collect or otherwise obtain an individual's health information, nor do they apply to all forms of health information.[5] Those companies or individuals to whom HIPAA regulations do apply are referred to as "covered entities [or] business associates,"[6] while only PHI is protected by HIPAA's Privacy Rule and Security Rule.[7] Therefore, to understand how and why modern technology companies and wearable health technology can slip through the cracks of HIPAA protection, it is important to first understand what makes an entity a covered entity or business associate, what type of health information can be deemed PHI, what protections are afforded to PHI under HIPAA's Privacy Rule and Security Rule, and what wearable health technology and the technology companies that produce those wearables look like today.

---

also apply to smartphones and other technologies, however, such devices are not directly contemplated.

2. Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996) (codified at 29 U.S.C. § 1181, scattered sections of 42 U.S.C., and scattered sections of 45 C.F.R.).

3. *Health Insurance Portability & Accountability Act*, N.H. DEP'T HEALTH & HUM. SERVS., https://www.dhhs.nh.gov/oos/hipaa/index.htm (last visited Sept. 13, 2018).

4. *Id.*

5. 45 C.F.R. § 160.103 (2014).

6. *Covered Entities and Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

7. 45 C.F.R. § 160.103 (2014).

A. Covered Entities and Business Associates

For HIPAA regulations to apply, the entity controlling the information must be a covered entity or business associate.[8] There are three broad categories of organizations or individuals that HIPAA defines as covered entities: (1) health plans, (2) health care clearinghouses, and (3) health care providers who transmit any health information in electronic form in connection with a transaction covered by this chapter.[9]

Health plans are, "[w]ith certain exceptions, an individual or group plan that provides or pays the cost of medical care . . . ."[10] Health plans include health insurance companies like Aetna or Kaiser Permanente, health maintenance organizations (HMOs), employer-provided health plans, and government-provided health care programs such as Medicare, Medicaid, and TRICARE.[11] Health care clearinghouses are "entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa."[12] These entities can include "billing service[s], repricing compan[ies], community health management information system[s] or community health information system[s], and 'valueadded' networks and switches that either process or facilitate the processing of health information" into a standard format.[13] Health care providers are those groups or individuals who directly provide care to individuals—"doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies . . . but only if they transmit any information in an electronic form in connection with a transaction for which HHS[, the Department of Health and Human Services,] has adopted a standard."[14]

HIPAA regulations also apply to business associates of covered entities.[15] A business associate is any person who

> (i) On behalf of [a] covered entity or of an organized health care arrangement . . . creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities . . . billing, benefit management, practice management, and repricing; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation . . . management, administrative, accreditation, or financial services to or for such covered entity . . . where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.[16]

---

8. Timothy Newman & Jennifer Kreick, *The Impact of HIPAA (and Other Federal Law) on Wearable Technology*, 18 SMU SCI. & TECH. L. REV. 429, 433 (2015).

9. 45 C.F.R. § 160.103 (2014).

10. *To Whom Does the Privacy Rule Apply and Whom Will it Affect?*, NAT'L INSTS. OF HEALTH, https://privacyruleandresearch.nih.gov/pr_06.asp (last updated Feb. 2, 2007).

11. *Covered Entities and Business Associates*, *supra* note 6.

12. *Id.*

13. *To Whom Does the Privacy Rule Apply and Whom Will it Affect?*, *supra* note 10.

14. *Covered Entities and Business Associates*, *supra* note 6.

15. 45 C.F.R. § 160.103 (2014).

16. *Id.*

Typical business associates might be CPA firms, attorneys, consultants, health care clearinghouses, independent medical transcriptionists, or pharmacy benefits managers whose work involves or requires access to PHI obtained from covered entities.[17] A covered entity may also be a business associate of a separate covered entity if it has any of the defining characteristics of a business associate.[18] While the definition of a business associate is broad, there are several entities that are expressly excluded from the definition of business associate, such as certain health care providers, health plan sponsors, government agencies, and covered entities in specific situations.[19]

B. Protected Health Information

As noted above, not all forms of health information are afforded protection by HIPAA regulation.[20] Those types of health information that are protected are referred to as protected health information (PHI) and are generally defined as "individually identifiable health information . . . that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium."[21] PHI excludes individually identifiable health information "(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);[22] (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years."[23]

The key to deciding whether health information is PHI is to determine whether or not it is "individually identifiable."[24] Individually identifiable health information is a "subset of health information," which:

> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates 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; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[25]

Simply put, PHI is any information that identifies or could reasonably identify an

17. U.S. DEP'T OF HEALTH & HUMAN SERVS., BUSINESS ASSOCIATES 2 (2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf.

18. 45 C.F.R. § 160.103 (2014).

19. *Id.*

20. *Id.*

21. *Id.*

22. "[R]ecords on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice." 20 U.S.C. § 1232g(a)(4)(B)(iv) (2013).

23. 45 C.F.R. § 160.103 (2014).

24. *Id.*

25. *Id.*

individual and relates to any medical condition of the individual, the provision of health care services to that individual, or the individual's payment for the rendered health care services.[26] Under this definition, laboratory bills, hospital bills, medical records, medical referral documents, and the like would likely be considered PHI if controlled by a covered entity or business associate.[27]

C. HIPAA's Privacy Rule and Security Rule

The two HIPAA rules most relevant to this Note are the Privacy Rule and the Security Rule. The Privacy Rule applies broadly to covered entities and business associates and requires them to establish certain standards and practices that assist in safeguarding PHI.[28] To comply with the Privacy Rule, covered entities and business associates must:

> (1) adopt internal procedures to protect the privacy of protected health information; (2) train employees regarding privacy procedures; (3) designate a privacy officer; (4) secure patient records that contain protected information; and (5) establish and enforce agreements with certain third parties . . . that ensure that they maintain privacy protection for information [the third party] has access to.[29]

In general, the Privacy Rule forbids covered entities or business associates from disclosing any PHI to any third party.[30] There are, however, a multitude of exceptions which allow, and sometimes require, covered entities and business associates to disclose PHI to various other entities.[31]

The Security Rule deals specifically with electronic PHI (e-PHI), and "establishes national standards to protect" that e-PHI.[32] Specifically, the Security Rule requires covered entities and business associates to ensure the confidentiality of e-PHI, identify and protect against threats to the security of e-PHI, protect against impermissible uses or disclosures of e-PHI, and ensure compliance by their employees.[33] To comply with the Security Rule, covered entities and business associates must "perform risk analysis as part of their security management process[]"[34] and maintain administrative,[35] physical,[36] and technical[37]

---

26. Newman & Kreick, *supra* note 8, at 434.

27. *Id.*

28. *Id.*

29. MARK A. HALL ET AL., HEALTH CARE LAW AND ETHICS 170 (8th ed. 2013).

30. 45 C.F.R. § 164.502(a) (2013); *see also* Cicely N. Tingle, *Developments in HIPAA and Health Information Technology*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 677, 680 (2007–08) (describing the Privacy Rule).

31. 45 C.F.R. § 164.502 (2013) (defining when and how a covered entity may or must disclose PHI); *see* HALL ET AL., *supra* note 29, at 171–72 (explaining that the Privacy Rule permits or requires disclosure of PHI in certain situations and also noting the complexity of determining when disclosure is permitted or required due to the cross-referencing of exceptions to the Privacy Rule to a variety of other sections of HIPAA). Among other permitted uses and disclosures, PHI may be disclosed to the individual to whom it relates and may be used or disclosed for treatment or payment. 45 C.F.R. § 164.502. None of the permitted uses or disclosures allow a covered entity or business associate to disclose PHI to a third party for financial gain. *Id.*

32. *The Security Rule*, U.S. DEP'T. HEALTH & HUM. SERVS. (May 12, 2017), https://www.hhs.gov/hipaa/for-professionals/security/index.html.

33. *Id.*

34. *Summary of the HIPAA Security Rule*, U.S. DEP'T. HEALTH & HUM/ SERVS. (July 26, 2013) https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

35. 45 C.F.R. § 164.308 (2013).

36. *Id.* § 164.310.

37. *Id.* § 164.312.

safeguards.[38]

D. Wearable Health Technology and Health Technology Companies

Wearable technology, in general, has seen massive growth in the past few years, with 102.4 million units shipped in 2016, up 25% from the 81.9 million units shipped in 2015.[39] While wearable technology has gained popularity, its value has been seen as "questionable at best;" however, some of the major technology companies producing wearable technology have pivoted to what they see as a more viable use of wearable technology—health and fitness tracking.[40] Some technology companies produce wearable technology that tracks information such as daily steps taken, heart rate, and sleeping patterns,[41] while others track more detailed health information such as glucose levels[42] or blood alcohol concentration.[43] Health and fitness tracking capabilities are a "major focus" for companies producing wearable technology,[44] and this may present privacy concerns for consumers where the technology companies are not considered covered entities or business associates under HIPAA or where the health information collected is not PHI.

For instance, Fitbit, the market leader in wearable devices,[45] as well as Apple, Garmin, and Samsung, among others, are technology companies that produce wearable fitness trackers and do not fall under any of the three categories of covered entities. Each of these companies, however, store health information collected from consumers and allows users to access that information via an app or the company's website.[46] Whether they are considered business associates, thus requiring them to abide by HIPAA's Privacy Rule and Security Rule, is a factual question which would require determining what other entities they come into contact with, the relationship between those other entities and the technology companies, and whether any of the health information collected by their wearable technology is shared with those other entities.[47] This question is addressed in further detail in Part III.A.1.b.

---

38. *Summary of the HIPAA Security Rule*, *supra* note 34. *See infra* Part II.E for a more detailed look at the requirements of the Security Rule and how covered entities and business associates comply with it in practice.

39. Marko Maslakovic, *Wearable Sales Hit All Time High in 2016, Fitbit Loses Ground*, GADGETS AND WEARABLES (Mar. 3, 2017), http://gadgetsandwearables.com/2017/03/03/idc-wearables/.

40. *Wearables Aren't Dead, They're Just Shifting Focus as the Market Grows 16.9% in the Fourth Quarter, According to IDC*, BUS. WIRE (Mar. 2, 2017), http://www.businesswire.com/news/home/20170302005298/en/Wearables-Arent-Dead-Theyre-Shifting-Focus-Market [hereinafter *Wearables Aren't Dead*].

41. *Fitbit Ionic*, FITBIT, https://www.fitbit.com/ionic (last visited Sept. 30, 2017).

42. Benjamin Mayo, *Report: Tim Cook Testing Wearable Blood Sugar Tracker on Apple's Campus, Connected to Apple Watch*, 9TO5MAC (May 18, 2017, 12:48 pm), https://9to5mac.com/2017/05/18/report-tim-cook-testing-wearable-blood-sugar-tracker-on-apples-campus-connected-to-apple-watch/.

43. *BACtrack Skyn,* BACTRACK, https://www.bactrack.com/pages/bactrack-skyn-wearable-alcohol-monitor (last visited Sept. 30, 2017).

44. *Wearables Aren't Dead*, *supra* note 40.

45. *Id.*

46. Robert J. Nelson, *Everything You Need to Know About Fitbit*, WINDOWS CENT. (June 12, 2014), https://www.windowscentral.com/everything-you-need-know-about-fitbit; *Your Heart Rate. What It Means, and Where on Apple Watch You'll Find It*, APPLE, https://support.apple.com/en-us/HT204666 (last visited Sept. 28, 2017); *Your Health in Your Hands*, SAMSUNG, http://www.samsung.com/us/samsung-health/ (last visited Sept. 30, 2017).

47. 45 C.F.R. § 160.103 (2014).

E. Application of the Privacy and Security Rules to Covered Entities and Business Associates

To comply with the Privacy Rule and Security Rule, covered entities and business associates must implement many protective procedures. The Privacy Rule regulates the circumstances under which a covered entity or business associate may disclose PHI, while the Security Rule requires covered entities and business associates to proactively implement and maintain security measures to protect the PHI itself.[48] Accordingly, compliance with the Privacy Rule is achieved largely through educating and training employees on those procedural rules. The Security Rule, on the other hand, requires covered entities to take affirmative, often costly, steps to protect PHI when it is in their possession.[49]

As noted above, to comply with the Security Rule, covered entities and business associates must maintain administrative,[50] physical,[51] and technical[52] safeguards. Each of these categories of safeguards require certain actions on the part of covered entities and business associates and suggests other safeguarding measures to be taken when "reasonable and appropriate to do so."[53]

With respect to administrative safeguards, covered entities and business associates must "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."[54] To this end, covered entities and business associates are required to "thorough[ly] assess[] . . . the potential risks and vulnerabilities to the confidentiality" of e-PHI in their possession, "[i]mplement security measures sufficient to reduce [those] risks and vulnerabilities[,]" sanction employees who fail to comply with security policies, and "[i]mplement procedures to regularly review records of information system activity."[55] They must also designate a security official responsible for implementation and oversight of these security policies and procedures.[56] In the event of a security breach or incident, covered entities and business associates must identify and respond to the incident, mitigate harmful effects, and document the incident and its outcome.[57] To prevent loss or damage to e-PHI in the event of an emergency, e-PHI must be backed up and maintained, procedures must be in place to recover any loss of data, and an emergency mode operation plan must be enacted to allow for continued protection of e-PHI during the emergency situation.[58] Lastly, covered entities and business associates must evaluate their policies and procedures to ensure continued compliance.[59]

The security safeguard requirements deal mainly with workstations and physical devices that store e-PHI. To meet these requirements, covered entities and business

48. *See id.* § 164.502(a); *The Security Rule*, *supra* note 32.

49. Jason Wang, *How Do I Become HIPAA Compliant? (A Checklist)*, TRUEVAULT (Oct. 30, 2013), https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html.

50. 45 C.F.R. § 164.308 (2013).

51. *Id.* § 164.310.

52. *Id.* § 164.312.

53. Wang, *supra* note 49.

54. 45 C.F.R. § 164.308(a)(1)(i) (2013).

55. *Id.* § 164.308(a)(1)(ii)(A)–(D).

56. *Id.* § 164.308(a)(2).

57. *Id.* § 164.308(a)(6).

58. *Id.* § 164.308(a)(7).

59. 45 C.F.R. § 164.308(a)(8) (2013).

associates must implement policies and procedures regarding the proper use of workstations that have access to e-PHI, and those workstations must only be accessible to authorized users.[60] Additionally, there must be policies and procedures regarding the final disposition of hardware that stores e-PHI, as well as procedures for removing e-PHI from such hardware.[61]

Covered entities and business associates are further required to maintain technical safeguards regarding access to e-PHI. To track who accesses e-PHI, they must assign unique identifiers to each individual who has access to e-PHI and establish procedures for accessing e-PHI in emergency situations.[62] Covered entities and business associates must also establish audit controls that can "record and examine" activity on systems that have access to e-PHI.[63] Finally, authentication procedures must be in place "to verify that a person or entity seeking access . . . is the one claimed."[64]

In addition to each of these requirements, the Security Rule suggests other protections covered entities and business associates ought to put in place.[65] Together, these administrative, security, and technical safeguards regulate who or what can access an individual's e-PHI. When it is clear that a given entity qualifies as a covered entity or business associate, the Privacy Rule and Security Rule adequately protect PHI and e-PHI from improper disclosure and access. However, in the case of health technology companies that produce wearable technology it is not so clear that they are covered entities or business associates, and thus they are caught between violating federal regulations and taking unnecessary and potentially inefficient steps to comply with an inapplicable regulation.

III. ANALYSIS

A. The Privacy Rule and Security Rule in Practice

The Privacy Rule and Security Rule apply to covered entities and business associates and are the two main rules governing how those entities may use and control PHI and when and how those entities may disclose PHI.[66] As discussed above, these two rules are complex in their application and require much of those entities to which they apply.

---

60. *Id.* § 164.310(b)–(c).

61. *Id.* § 164.310(d).

62. *Id.* § 164.312(a)(2)(i)–(ii).

63. *Id.* § 164.312(b).

64. 45 C.F.R. § 164.312(d) (2013).

65. The regulations define some procedures as "addressable" and others as "required". *Compare id.* § 164.312(a)(2)(i), *with id.* § 164.312(a)(2)(iii). Required procedures are, unsurprisingly, required. *What is the Difference Between Addressable and Required Implementation Specification in the Security Rule?*, U.S. DEP'T. HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html. That is, a covered entity or business associate must implement that procedure. *Id.* Addressable procedures, on the other hand, were "developed to provide covered entities additional flexibility with respect to compliance with the security standards." *Id.* Covered entities and business associates have three options when it comes to addressable procedures: they can "(a) implement the addressable implementation specifications; (b) implement one or more alternative security measures to accomplish the same purpose; (c) not implement either an addressable implementation specification or an alternative." *Id.*

66. *See The Security Rule*, *supra* note 32 (discussing a general introduction to the HIPAA Security Rule); *To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, *supra* note 10.

1. Problems with HIPAA's Application to Health Technology Companies

While HIPAA's Privacy Rule and Security Rule do much to protect the integrity of PHI, the current regulatory scheme is ineffective at protecting health information when in the hands of health technology companies. This ineffectiveness largely stems from the fact that most health technology companies are neither covered entities nor business associates under HIPAA.

a. Most Health Technology Companies Are Not Covered Entities.

The only covered entities currently subject to the rules are health plans, health care clearinghouses, and health care providers that transmit e-PHI.[67] The five leading vendors of wearable devices—Fitbit, Xiaomi, Apple, Garmin, and Samsung—make up 60% of the market share for such devices and all offer for sale wearable devices that track health information.[68] None of these companies are health plans because they do not provide or pay the cost of medical care. Nor are they health care clearinghouses, as they do not convert non-standardized health information received from another entity into a standard form. Likewise, these companies are not health care providers because they are not directly providing health care to individuals. Because these companies are not health plans, healthcare clearinghouses, or health care providers, they are not subject to the Privacy Rule or Security Rule on account of being covered entities.

It is possible that some covered entities produce wearable health technology and thus some information collected through such technology would be protected by HIPAA, but it is more likely that wearable health technology and its producers will escape HIPAA regulation.[69] As a result, this analysis focuses only on companies that do not currently qualify as covered entities.

b. Not All Health Technology Companies That Produce Wearable Health Technology Are Business Associates

Given that most health technology companies that produce wearable health technology are not covered entities, HIPAA's Privacy Rule and Security Rule will only apply to them if they are business associates. Whether or not a company is a business associate is a "fact and circumstance specific" inquiry,[70] and it is unlikely that many health technology companies that produce wearable health technology would meet the factual requirements to qualify as a business associate.

---

67. *See Covered Entities and Business Associates*, *supra* note 6.

68. *See Wearables Aren't Dead*, *supra* note 40. For example, Fitbit produces many products that collect health and fitness information. This information is collected using a 3-axis accelerometer which measures frequency, duration, intensity, and patterns of movement. The information collected by the accelerometer is used to determine steps taken, distance traveled, calories burned, and sleep quality. *How Does My Fitbit Device Calculate My Daily Activity?*, FITBIT, https://help.fitbit.com/articles/en_US/Help_article/1143 (last updated July 6, 2018).

69. *See* Donna Marbury, *Top 10 Healthcare Wearables to Watch*, MOD. HEALTHCARE EXECUTIVE (Mar. 10, 2017), http://www.managedhealthcareexecutive.com/health-management/top-10-healthcare-wearables-watch (discussing ten wearable health technology products from non-covered entities).

70. U.S. DEP'T. HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS, HEALTH APP USE SCENARIOS & HIPAA 1 (2016), https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf [hereinafter HEALTH APP USE SCENARIOS & HIPAA].

The Office for Civil Rights (OCR), the unit within the Department of Health and Human Services responsible for enforcing HIPAA compliance, has attempted to give some guidance to developers of health apps to assist in the determination of whether a given company is a business associate.[71] The scenarios laid out by OCR indicate that the key question is whether or not the company is providing any goods or services to or on behalf of a covered entity.[72] If the company is primarily providing a good or service to or on behalf of a covered entity, then the company will most likely be a business associate and subject to HIPAA.[73] However, if the company primarily provides the same goods or services to or on behalf of an individual, the company is likely not a business associate even if the company does interact with covered entities.[74] Because many wearable health technologies are produced with the intention of sale directly to consumers, rather than through or by covered entities, the guidance provided by OCR indicates that the majority of these companies will not be subject to the Privacy Rule and Security Rule.

For example, if a physician who is a health care provider directs a patient to purchase a wearable fitness tracker, and the physician contracts with the producer of that wearable fitness tracker to receive the information collected by the tracker, then the producer is a business associate according to HIPAA because it "creates, receives, maintains or transmits protected health information (PHI) on behalf of a covered entity."[75] However, if a physician who is a health care provider informs a patient that they need to take a minimum of 10,000 steps a day to lose weight and the physician recommends a Fitbit device to keep track of steps, even if the patient purchases a Fitbit and sends the collected step information to the physician, Fitbit, under these facts, would not be a business associate because it is not "creat[ing], receiv[ing], maintain[ing] or transmit[ing] personal health information (PHI) on behalf of a covered entity or another business associate."[76] Rather, it is creating, receiving, maintaining or transmitting health information on behalf of the patient.[77]

While this may seem straightforward, consider that a given company may simultaneously be both a business associate and not a business associate. That is, in the example above, a company that produces wearable health technology may contract directly with a covered entity and receive PHI on the covered entity's behalf, and also offer its services directly to consumers. With respect to the information collected on behalf of covered entities, the company would be a business associate and would thus be required to protect the PHI in accordance with the Privacy Rule and Security Rule. However, with respect to the information collected on behalf of its customers, the company would not be required to protect the health information and could disseminate the information as the company pleased.

B. Uncertainty Limits HIPAA's Effectiveness and Negatively Impacts Health Technology

71. *Id.*

72. *See id.* (listing a series of questions for determining if an entity is providing services for a covered entity); Newman & Kreick, *supra* note 8, at 447.

73. HEALTH APP USE SCENARIOS & HIPAA, *supra* note 70, at 4.

74. *See id.* (explaining that an app developer is not a business associate even if a consumer downloads the developer's health app and requests that the app developer and the consumer's health care provider enter into a contract such that e-PHI may be exchanged securely between the app and the health care provider).

75. *Id.* at 1.

76. *Id.*

77. *Id.*

Companies and Consumers

Because health technology companies that produce wearable health technology are likely not subject to HIPAA's Privacy Rule and Security Rule, any health information collected by those companies is not protected by the same rigorous procedures and policies. This directly undermines the Department of Health and Human Services' goal of "protect[ing] individuals' medical records and other personal health information."[78]

The lack of protections can also negatively impact the individuals who use wearable health technologies. In absence of the Privacy Rule, individuals' health information "could, without the [individual]'s permission, be passed on to a lender who could then deny the patient's application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions."[79] Individuals could thus suffer both personal and professional harm as a result of HIPAA's inapplicability to health technology companies.

Finally, uncertainty in determining whether a health technology company is subject to the Privacy Rule and Security Rule may negatively affect individual health technology companies as well as the health technology market as a whole. Individual companies will face the difficult decision of expending potentially substantial capital to become HIPAA compliant[80] when they in fact do not need to, or not implementing HIPAA-compliant policies and procedures and risking facing fines up to $50,000 per violation.[81]

1. HIPAA's Effectiveness Is Undermined if Health Technology Companies Are Not Subject to the Privacy Rule and Security Rule.

By regulating how covered entities and business associates are permitted to handle e-PHI, Congress has, in effect, announced that individually identifiable health information is particularly important to the individual and ought to be kept confidential except in specific circumstances. While those defined circumstances may have been an appropriate regulation of the healthcare market in the past, the development and proliferation of wearable health technology has limited HIPAA's effectiveness in achieving the goal of "protect[ing] the confidentiality, integrity, and availability of electronic protected health information."[82]

Health technology companies that produce wearable health technologies collect health information that, if collected by a covered entity or business associate, would be e-PHI. Neither the fact that the information is collected at the request of the individual nor that the information is collected by a health technology company should diminish an

78. *What Does the HIPAA Privacy Rule Do?*, U.S. DEP'T. HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html.

79. *Why Is the HIPAA Privacy Rule Needed?*, U.S. DEP'T. HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.html.

80. *See* Doug Pollack, *Security Compliance by HIPAA Business Associates May Be Unexpectedly Costly*, IDEXPERTS (Sept. 11, 2013), https://www2.idexpertscorp.com/knowledge-center//single/security-compliance-by-hipaa-business-associates-may-be-unexpectedly-costly (noting that costs for a security risk analysis and PHI inventory could cost between $50,000 to $100,000).

81. Morgan Brown, *What Is the Penalty for a HIPAA Violation?*, TRUEVAULT (Jan. 9, 2014), https://www.truevault.com/blog/what-is-the-penalty-for-a-hipaa-violation.html.

82. *Why Is the HIPAA Security Rule Needed and What Is the Purpose of the Security Standards?*, DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/2000/why-is-hipaa-needed-and-what-is-the-purpose-of-security-standards/index.html [hereinafter *Why Is the HIPAA Security Rule Needed?*].

individual's interest in the confidentiality and integrity of the information. Given that the health information collected by many wearable health devices would be considered e-PHI if collected by a covered entity or business associate, permitting health technology companies to be free from the Privacy Rule and Security Rule allows for individuals' personal health information to be used in precisely the ways HIPAA is supposed to protect against.

Insofar as its goal is to protect individuals from disclosure of personal health information without their consent, HIPAA's effectiveness in achieving that goal diminishes as wearable health technology grows in popularity. The more non-covered entity, non-business associate companies collect personal health information, the more likely it is that personal health information will be disclosed in ways that will be harmful to an individual. If the goal of the Security Rule is indeed "to protect the confidentiality, integrity, and availability of electronic protected health information"[83] and the goal of the Privacy Rule is "to protect individuals' medical records and other personal health information,"[84] HIPAA will continue to fall short if it is not adapted to fit the current market of health technology companies.

2. Individuals' Health Information Could Be at Risk of Unwanted Disclosure

Without being subject to Privacy and Security Rules, health technology companies can disclose collected health information to whomever, whenever they wish.[85] Individuals have an important interest in maintaining the confidentiality of their personal health information, as such information is sensitive and susceptible to be used "for reasons that ha[ve] nothing to do with a[n individual]'s medical treatment or health care reimbursement."[86]

Misuse of an individual's health information can have devastating consequences to the individual's personal and professional lives. The Department of Health and Human Services provides two examples of such misuse and the ramifications that can follow, "[f]or example, . . . without the Privacy Rule patient information held by [an entity] could, without the patient's permission, be passed on to a lender who could then deny the patient's application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions."[87]

Misuses of personal health information due to the inapplicability of the Privacy Rule are perhaps less nefarious than those that can arise when the company possessing personal health information is not subject to the Security Rule. The Security Rule exists "to ensure that every covered entity has implemented safeguards to protect the confidentiality, integrity, and availability of electronic protected health information."[88] Without the administrative, physical, and technical safeguards to e-PHI afforded by the Security Rule, health technology companies are not held to the same rigorous standards of data protection. Without these safeguards, data collected and held by health technology companies are more susceptible to theft or destruction. Depending on the type of health information being

83. *Id.*
84. *What Does the HIPAA Privacy Rule Do?*, *supra* note 78.
85. Notwithstanding state laws regulating the protection of health information.
86. *Why Is the HIPAA Privacy Rule Needed?*, *supra* note 79.
87. *Id.*
88. *Why Is the HIPAA Security Rule Needed?*, *supra* note 82.

collected, one could easily imagine an e-PHI security breach leading to identity theft and other fraudulent activity.

While these concerns regarding the use and misuse of health information exist now, the likelihood of such misuse will only increase as wearable health technology grows in popularity. Sales of wearable devices in general are projected to increase by more than 90% from 2017 to 2021.[89] Since a majority of those devices are capable of collecting and tracking health information, the risks associated with that data being held by entities not subject to the Privacy Rule and Security Rule will not disappear without altering the definition of a covered entity.

3. Regulatory Uncertainty Could Lead Health Technology Companies Astray

As it is not always entirely clear whether a given health technology company is required to comply with the Privacy Rule and Security Rule, those companies are put in the difficult position of having to choose whether to potentially unnecessarily implement the procedures to comply or not implement the required procedures and risk facing significant fines for any violations. The Department of Health and Human Services estimates that the costs of HIPAA compliance per organization would be only roughly $1040,[90] however this estimation has been viewed as "likely inaccurate."[91] In contrast with the confusion over compliance costs, fines for HIPAA violations are clear. Depending on the violative intent of the entity, fines for civil violations range from $100 per violation to $50,000 per violation, with an annual maximum fine of $1.5 million.[92] There is also the possibility of criminal penalties for HIPAA violations, the severity of which again depend on the level of intent.[93] The criminal penalties range from small fines all the way up to ten years imprisonment.[94]

While the decision to comply with HIPAA data privacy and security rules may seem obvious in the face of the potentially large penalties for violations, the costs of compliance can be a substantial burden to entities entering the market.[95] Additionally, regulatory

89. *See* Hollie Bridgland, *Forecast Reveals Steady Growth in Smartwatch Market*, CCS INSIGHT (Mar. 16, 2017), http://www.ccsinsight.com/press/company-news/2968-ccs-insight-forecast-reveals-steady-growth-in-smartwatch-market (estimating a roughly 93% increase in wearable device sales from 2017-2021); ADITYA KAUL & CLINT WHEELOCK, TRACTICA EXECUTIVE SUMMARY: WEARABLE DEVICE MARKET FORECASTS (2016), https://www.tractica.com/wp-content/uploads/2016/03/MD-WDMF-1Q16-Executive-Summary.pdf (predicting sales of 560 million wearable devices in 2021, up from approximately 140 million in 2017).

90. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5567 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164).

91. Jen Stone, *How Much Does HIPAA Compliance Cost?*, SECURITY METRICS (Apr. 6, 2015), http://blog.securitymetrics.com/2015/04/how-much-does-hipaa-cost.html (estimating the cost of HIPAA compliance as $4000 to $10,000 for small covered entities and greater than $50,000 for medium and large covered entities); *see also* Peter Hesse, *The Costs of HIPAA Compliance*, SECURITY MUSINGS (Jan. 30, 2013), http://securitymusings.com/article/3878/the-costs-of-hipaa-compliance (explaining how current estimates are inaccurate); Pollack, *supra* note 80 (estimating the cost of HIPAA compliance as $50,000 to $100,000).

92. *See HIPAA Violations and Enforcement*, AM. MED. ASS'N, https://www.ama-assn.org/practice-management/hipaa-violations-enforcement#Criminal%20Penalties (last visited Dec. 14, 2017) (detailing the criminal offenses of HIPAA violations).

93. *Id.*

94. *Id.*

95. *See* STEVEN GARBER ET AL., RAND CORP., REDIRECTING INNOVATION IN U.S. HEALTH CARE:

uncertainty can "reduce [research and development] efforts and the level of investment."[96] Given the potential benefits of wearable health technology, the regulatory scheme should be as clear and effective as possible so as to encourage investment and development of new products.

IV. RECOMMENDATION

As discussed in Part III, the current regulatory scheme is undermined by the uncertainty of whether health technology companies must abide by the Privacy Rule and Security Rule.[97] One way to address this uncertainty would be to add a fourth category of organizations to the definition of covered entities. To avoid unnecessarily subjecting companies to the rigorous data protection standards of HIPAA while still affording protection to consumers' health information, the definition of what constitutes a covered entity ought to include companies that produce devices, a primary purpose of which is achieved through collecting health information from individuals. Put differently, if a primary purpose of a given device is achieved by collecting health information, the company that produces that device ought to be a covered entity. While this additional definition is perhaps linguistically unwieldy, companies and courts are well versed in applying primary purpose tests,[98] and thus would be capable of determining whether one of the primary purposes of a device is to collect health information from individuals.

Expanding the definition in such a way would solve many of the problems currently facing consumers and companies that produce wearable health devices, while plugging some of the current holes in HIPAA protection. The goals of HIPAA would be better achieved by this expanded definition because more health information would be protected from unwanted disclosure by the Privacy Rule and Security Rule. For consumers, their health information would be better protected, and they could purchase wearable health technology with confidence that their privacy would not be breached. Lastly, companies that produce wearable health technology would have better guidance as to whether they need to abide by the Privacy Rule and Security Rule.

A. The Goals of HIPAA Would Be More Effectively Achieved by Expanding the Definition of Covered Entities

PHI is particularly important to individuals, and Congress enacted HIPAA to keep this information confidential.[99] Expanding the definition of covered entities to include

---

OPTIONS TO DECREASE SPENDING AND INCREASE VALUE 41 (2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR308/RAND_RR308.pdf (noting that regulatory uncertainty often impacts smaller companies more than larger ones).

96. *Id.*

97. *See supra* Part III.B (discussing how uncertainty negatively impacts the regulatory scheme as a whole, consumers, and health technology companies).

98 . *See, e.g.*, State v. Dan J. Evans Campaign Committee, 546 P.2d 75 (Wash. 1976) (using a primary purpose test to determine whether a person or organization is a political committee for the purposes of state election law); UNIF. UNCLAIMED PROP. ACT § 25 (UNIF. LAW COMM'N 1995); Reinout Kok, *The Principal Purpose Test in Tax Treaties Under BEPS 6*, ERNST & YOUNG (2016), https://www.ey.com/Publication/vwLUAssets/EY-the-principal-purpose-test-in-tax-treaties-under-BEPS-6/$File/EY-the-principal-purpose-test-in-tax-treaties-under-BEPS-6.pdf; Rusudan Shervashidze & Stanley C. Ruchelman, *A Comparative View of the Principal Purpose Test – U.S. Tax Court v. B.E.P.S.*, RUCHELMAN P.L.L.C. (2018), http://www.ruchelaw.com/publications/a-comparative-view-of-the-principal-purpose-test-us-tax-court-v-beps.

99. *See supra* Part III.B.1 (noting the goal of "protect[ing] the confidentiality, integrity, and availability of

those companies that produce devices, a primary purpose of which is achieved through collecting individualized health information will assist in achieving this goal and will significantly increase the security of this type of information.

Because much of the health information collected by companies manufacturing wearable health technology would be considered e-PHI if collected by a health plan, health care clearinghouse, or health care provider, the goal of protecting this type information from undesired disclosure would be better achieved if those companies are required to abide by the Privacy Rule and Security Rule. These two rules were put in place to ensure that entities that obtain PHI treat it with due care. Unless the definition of covered entities is expanded to fit the current market of health technology companies there will be massive amounts of individualized health information that companies are free to disclose as they please. Thus, to better achieve the goals of "protect[ing] the confidentiality, integrity, and availability of electronic protected health information"[100] and "protect[ing] individuals' medical records and other personal health information,"[101] the definition of covered entities ought to be expanded.

B. Individuals' Health Information Would Be Better Protected by Expanding the Definition of Covered Entities and Consumers Could Purchase Wearable Health Technology Without Fear of Unwanted Disclosures

Individuals have an important interest in maintaining the security and confidentiality of their individualized health information.[102] By requiring companies that produce devices which achieve a primary purpose by collecting individualized health information to comply with the Privacy Rule and Security Rule, collected information would be far better protected from unwanted disclosure. As the popularity of wearable health technology rises, so too does the amount of individualized health information (i.e. information which would be PHI if collected by a covered entity or business associate) collected by companies not currently subject to the Privacy Rule and Security Rule. Accordingly, if HIPAA were expanded to include such companies as covered entities, more individualized health information would be protected by the Privacy Rule and Security Rule and individuals could be more confident that their health information would not be used improperly.[103]

Additionally, consumers interested in purchasing wearable health technology could do so without fear of unwanted disclosures. Wearable health technology currently has many benefits,[104] and consumers may be more interested in taking advantage of such benefits if they are confident any health information collected would be protected from disclosure. Presumably, as the uses of wearable health technology expand and wearable health devices collect more sensitive and useful health information such as blood sugar levels, blood alcohol concentration, or muscle activity, they will become more ingrained in everyday life—in much the same way as smartphones have. Affording better protection to the information collected by these types of devices will increase consumers' confidence

---

electronic protected health information").

100. *See Why Is the HIPAA Security Rule Needed?*, *supra* note 82.

101. *See What Does the HIPAA Privacy Rule Do?*, *supra* note 78.

102. *See supra* Part II.C (discussing why an individual would want the protection offered by the Privacy Rule and Security Rule).

103. *See Why Is the HIPAA Privacy Rule Needed?*, *supra* note 79.

104. *See supra* Part II.D (noting some of the uses of wearable health technology).

in the devices themselves as well as the companies that produce them.

C. Companies Would Have Better Guidance as to Whether to Comply with the Privacy Rule and Security Rule

Expanding the definition of covered entities to include companies that produce devices, a primary purpose of which is achieved through collecting individualized health information, will better inform health technology companies on whether they must implement security procedures in compliance with the requirements of the Privacy Rule and Security Rule. This will greatly benefit companies generally, as they will be less likely to face a situation where they must decide whether to forego implementing HIPAA-compliant security procedures and risk facing potentially enormous fines[105] or possibly unnecessarily incur significant costs to comply with HIPAA's regulations.

As a side effect, requiring these companies to comply with the Privacy Rule and Security Rule when it comes to protecting PHI could improve their data security and management more broadly. A company that implemented the required privacy and security policies and procedures might also implement those same policies and procedures in maintaining the safety and integrity of other data in their possession. If these policies and procedures were implemented company-wide, then all data in the possession of the company would be protected to the same extent as the sensitive health information HIPAA aims to guard.

V. CONCLUSION

Wearable health technology is already a large industry and the demand for such technology shows no signs of decreasing. As these technologies become more common, the need for better protection of the health information collected grows. Rather than crafting new legislation to protect health information collected by non-covered entity, non-business associate health technology companies, HIPAA should simply be expanded to include as covered entities companies that produce devices, a primary purpose of which is achieved through collecting health information from individuals.

Expanding the definition of covered entities in such a way will benefit wearable health technology producers and consumers while better achieving the legislative goals of HIPAA. Companies that produce wearable health technology will have better guidance as to what privacy and security procedures they must implement to protect such information. Consumers will be protected from undesired disclosure of sensitive health information, as they already are when such information is collected or used by their insurance company, doctor, healthcare clearinghouse, or any company that obtains that information on behalf of their insurance company, doctor, or healthcare clearinghouse. Lastly, HIPAA's goal of protecting sensitive health information from unwanted use and disclosure will be better achieved if more health information is protected by the Privacy Rule and Security Rule.

105. *See* Brown, *supra* note 81 ("The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that can result in jail time.").