AN UPDATE IS REQUIRED TO CONTINUE USING THIS REGULATION: WHY THE HIPAA PRIVACY RULE SHOULD BE MODIFIED TO PROTECT A BROADER RANGE OF HEALTH DATA

LAUREN CAVERLY PRATT[1]

[1] Lauren Caverly Pratt is a 3L at Belmont University College of Law at the time of publishing, and hopefully a graduate of the same by May 2022. She submitted this note as a 2L before being elected to serve as Editor-In-Chief of the Health Law Journal during her final year of law school. Lauren would like to thank her advisor, Dean Debbie Farringer, for all of her candid advice, guidance, and grace during the note-writing process. She would also like to thank her husband, Ryan Pratt, for inspiring her to go to law school and being her constant source of support, especially during the most stressful times. Finally, Lauren believes she also needs to thank their dogs, Caesar and Annie, for keeping her company and bringing her joy during the COVID-19 pandemic. She would not have finished this note without all of you.

I. INTRODUCTION

Bailey wakes up to her alarm at 7:00 a.m. She checks her smartwatch and learns she fell asleep at 11:37 p.m., completed four REM cycles, and woke up briefly at 3:24 a.m. She gets out of bed and goes to the bathroom, then to the kitchen to start a pot of coffee. Her smartwatch tracks the number of steps she takes on this short journey through her apartment. Bailey is a diabetic and before she prepares breakfast, she tests her blood sugar with a blood sugar meter. The meter is connected via Bluetooth® to a mobile app on her phone, where her blood sugar readings are visualized in neat graphics. After breakfast, Bailey opens a fitness app on her tablet and joins a virtual workout class from her apartment. Her smart watch tracks her heart rate, the number of calories she burns, and her blood oxygen levels during her workout, then summarizes trends in her weekly fitness and activity levels. Bailey gets ready for the day and sits down at her desk to start working. Once per hour, her smartwatch buzzes to remind her to stand and stretch for a few minutes. Before lunch, she checks her blood sugar level again and opens a different mobile app to track her menstrual cycle. By 12:00 PM, only five hours after waking up, Bailey's various pieces of technology have collected hundreds of data points related to her health.

Bailey probably wants to share information related to her diabetes with her doctor. She may want to share her workout stats with friends. But what control does she have over the health data collected on her personal devices that she wishes to keep private? In most of the United States, the answer is very little. While the Health Insurance Portability and Accountability Act (HIPAA)[1] protects sensitive patient health data through the Privacy Rule[2], its protection extends to more traditional relationships between patients and healthcare providers. The rise in popularity of personal health, combined with the tech boom of the 2010s has led to the creation of myriad technologies that allow individuals to record their own health data through web applications, mobile applications, and a variety of physical devices that can connect to mobile phones or other Internet-enabled devices.[3] However, federal regulation in the United States has not caught up to protect health data in this new arena outside the traditional healthcare model.

While there is no constitutional right to privacy of information, general public sentiment leans in favor of keeping

---

[1] 45 C.F.R. § 160 (2021), 45 C.F.R. § 162 (2021), 45 C.F.R. § 164 (2021).
[2] 45 C.F.R. § 164.502 (2021).
[3] *What is Digital Health?*, U.S. FOOD & DRUG ADMINISTRATION (last updated Sept. 22, 2020), https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health.

personal health data private.[4] More precisely, individuals would like information known only to the individual and other parties to whom he or she chooses to disclose the information. This is because public knowledge of sensitive personal data may harm the individual economically, socially, or in other intangible ways.[5] The benefits of public knowledge of such individually identifiable health data do not outweigh these potential harms. Privacy should be the default.

To achieve this, HIPAA must be expanded to protect private health data beyond the confines of traditional patient-provider relationships and in the broader digital healthcare industry. This note will provide relevant background information on the current state of the HIPAA Privacy Rule and California's Confidentiality of Medical Information Act (CMIA)[6]. The primary issue this Note will discuss is that advancements in technology have fundamentally changed the healthcare landscape to the point where existing federal regulations neither address nor protect private health data when it is created or transmitted between non-traditional providers of healthcare. For example, companies that create technological products that allow consumers to track their personal health data are not covered by the HIPAA Privacy Rule. Thus, the collection, processing, and storage of such data is not subject to federal health regulations. This note will argue that more classes of entities, specifically businesses that track and store individuals' health data, should be subject to HIPAA privacy regulations. A state-by-state solution would be less effective than a federal regulation because it would likely cause confusion for businesses and consumers regarding when data is protected and when it is not. Furthermore, it is likely that such an approach would prove wasteful if Congress were to enact general data privacy regulations in the near future. Finally, this note will conclude that the most comprehensive and simple approach to addressing the issue of health data privacy is to modify the HIPAA Privacy Rule to cover a broader range of entities in the United States.

II. BACKGROUND

HIPAA is the primary federal authority regarding health data privacy in the United States. Signed into law in 1996, HIPAA was

---

[4] Kaveh Safavi & Brian Kalis, *How Can Leaders Make Recent Digital Health Gains Last?: Re-Examining the Accenture 2020 Digital Health Consumer Survey*, ACCENTURE (last modified Aug. 26, 2020), *available at* https://www.accenture.com/_acnmedia/PDF-130/Accenture-2020-Digital-Health-Consumer-Survey-US.pdf

[5] BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH (Sharyl J. Nass et al. eds., National Academies Press, 2009).

[6] Codified at CAL. CIV. CODE §§ 56-59.

initially an attempt at broad healthcare reform.[7] Some of its original purposes were to improve portability and continuity of health insurance, such that employees would not lose coverage when changing jobs, and to combat waste, fraud, and abuse in the healthcare and health insurance industries.[8] In its twenty-four-year lifespan, HIPAA has been modified and added to six times.[9] Most notably, the HIPAA Privacy Rule became effective in 2003.[10] The Privacy Rule protects individuals' personal health information from unauthorized use and disclosure.[11] However, HIPAA has not been significantly modified in recent years to address the rapid advances in technology that have meaningfully changed the way Americans access health care and manage personal health data.

a. The HIPAA Privacy Rule

Broadly, the purpose of HIPAA's Privacy Rule is to protect individuals' personal medical records and personal health information from unauthorized access or disclosure.[12] While privacy of personal data has not been recognized as a constitutionally fundamental right, Congress has acknowledged the importance of protecting individually identifiable health information with the passage of the Privacy Rule.[13] The Rule is codified at 45 C.F.R. § 164, though definitions to several key terms are carried over from 45 C.F.R. § 160.

i. Definitions

The definitions provided at 45 C.F.R. § 160.103 indicate the scope of the Privacy Rule; that is, what information is protected and to which parties the Privacy Rule applies. Several definitions are relevant to the discussion in this Note, including "health information." Health information is defined as

> any information, whether oral or recorded in any form or medium, that (1) is created or received by a

---

[7] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 45 U.S.C).
[8] *Id*.
[9] *The History of HIPAA*, ACCOUNTABLE (May 14, 2020), https://www.accountablehq.com/post/history-of-hipaa.
[10] *Id.*
[11] 45 C.F.R. § 164.502.
[12] *Id.*
[13] Standards for Privacy of Individually Identifiable Health Information; Final Rule, 67 Fed. Reg. 53181 (August 14, 2002) (Codified at 45 C.F.R. §§ 160 and 164).

> healthcare provider, health plan, public health authority, employer, life insurer, school or university, 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.[14]

The second part of this definition is quite expansive. Information must only "relate" to one of three healthcare aspects in order to be protected by the Privacy Rule. First, information may relate to an individual's physical or mental health condition, which includes information that the public traditionally associates with health care such as a vitals taken at a yearly checkup, genetic test results, or diagnosis or treatment of a disease.[15] But it also may include information such as a person's daily routine, eating habits, sleep patterns, and thoughts and feelings, as this type of information certainly relates to an individual's physical and mental health and condition. Second, information may relate to the provision of healthcare to a person.[16] This includes the conventional provision of healthcare by a doctor to a patient, such as assessing the patient, prescribing medication, performing operations. But it could also be broadly construed to include the work of professionals who are not traditionally thought of as "healthcare" workers, such as personal trainers or nutrition coaches, but whose work centers around improving individuals' health.[17] Finally, information may relate to past, present, or future payment for provision of healthcare.[18] Overall, the second part of the definition of health information covers a wide expanse of information conveyed orally or recorded in any form or medium.

However, the first part of the definition drastically limits the scope of the Privacy Rule, only offering protection if such information is "created or received" by one of the Privacy Rule's seven designated entities.[19] "Healthcare provider" is defined as

---

[14] 45 C.F.R. § 160.103.
[15] *What is Considered Protected Health Information Under HIPAA?* HIPAA JOURNAL (Apr. 2, 2018), https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.
[16] 45 C.F.R. § 160.103.
[17] For example, a personal trainer works to improve the physical health of trainees and a nutrition coach works to help clients maintain a balanced diet. Neither is traditionally considered a "healthcare" worker.
[18] 45 C.F.R. § 160.103.
[19] *Id.*

> a provider of services (as defined in 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, codified at 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.[20]

"Provider of services" is defined as a hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, or hospice program.[21] "Medical or health services" has a broad definition that outlines specific activities and medical items related to particular illnesses, diseases, and treatments.[22] The catch-all provision at the end generally refers to health insurance companies.[23]

"Health plan" includes private health insurers, Medicare, and Medicaid, but explicitly excludes other types of private insurers (such as automobile or liability insurance companies) and other government programs.[24] "Employer" borrows its definition from 26 U.S.C. § 3401(d): ". . . the person for whom an individual performs or performed any service, of whatever nature, as the employee of such person."[25] "Health care clearinghouse" is defined as a public or private entity that processes health information received from another entity and either converts it into a specified data format.[26] In plain words, health care clearinghouses are simply data processing companies. A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency.[27] The other listed entities are not explicitly defined in this Privacy Rule and for this Note the dictionary meaning will be used for "life insurer"[28] and "school or university."[29]

Thus, "health information" for purposes of the Privacy Rule is any information relating to a person's physical or mental health, provision of healthcare, or payment for healthcare when it is created

---

[20] *Id.*
[21] 42 U.S.C. § 1395x(u).
[22] 42 U.S.C. § 1395x(s).
[23] 45 C.F.R. § 160.103.
[24] *Id.*
[25] 26 U.S.C. § 3401(d).
[26] *See* 45 C.F.R. § 160.103.
[27] *See* 45 C.F.R. § 164.501.
[28] See *life insurance*, MERRIAM-WEBSTER DICTIONARY, (11th ed. 2014).
[29] See *school*, MERRIAM-WEBSTER DICTIONARY, (11th ed. 2014).

or received by certain entities traditionally associated with healthcare or health insurance. It appears that Congress intended for "health information" to encompass a broad range of information, limited by the requirement it be created or received by designated entities.

"Individually identifiable health information" is health information, as defined above, which identifies the individual.[30] "Protected health information" is individually identifiable health information which is transmitted or maintained in electronic or other form or media.[31] A select few categories of individual identifiable health information are excluded from protection, including information that is in education or employment records held by covered entities. Thus, the scope of protected health information under the HIPAA Privacy Rule can be summarized as individually identifiable information related to the physical or mental health or condition, the provision of healthcare, or the payment of healthcare of a person which is created or received by one of seven designated entities.

ii. Covered Entities

While several entities are designated in the definition of health information, as discussed above, the Privacy Rule applies only to three types of entities: health plans, healthcare clearinghouses, and healthcare providers who transmit any health information in electronic form in connection with a transaction covered by the Privacy Rule.[32] The definitions from 45 C.F.R. § 160.103 carry over into this section of the rule, and these entities are described as "covered entities." The Department of Health and Human Services has provided guidance on which entities qualify as covered entities: healthcare providers include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies; health plans include health insurances companies, HMOs, company health plans, and government programs which pay for healthcare; and healthcare clearinghouses include entities that process nonstandard health information received from another entity into a standard (i.e., standard electronic format or data content), or vice versa.[33]

Therefore, the Privacy Rule does not apply to any business, person, or other entity that does not meet the definition of health

---

[30] 45 C.F.R. § 160.103.
[31] *Id.*
[32] 45 C.F.R. § 164.104.
[33] Office for Civil Rights, *Covered Entities and Business Associates*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (last updated Jun. 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

plan, healthcare clearinghouse, or healthcare provider.[34] This means that a business that does not meet HIPAA's definition of healthcare provider, even though it may present itself to the general public as a health-related company, may collect and disseminate individually identifiable health information from a person without running the risk of violating the HIPAA Privacy Rule.

iii. The Privacy Rule

The Privacy Rule addresses several aspects relating to keeping individually identifiable health information private, including permitted uses and disclosures, rights to request such information, and notice of privacy practices. The basic premise of the Privacy Rule is that a covered entity may not use, disclose, or sell protected health information except in situations explicitly permitted by the Privacy Rule.[35] When use or disclosure of protected health information is permitted, the covered entity "must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request ."[36] Furthermore, communication of such protected health information must be confidential.[37]

Covered entities are, naturally, permitted to use or disclose protected health information to the individual and in relation to treatment, payment, or healthcare operations.[38] De-identified health information, as it does not meet the definition of protected health information, may be used or disclosed by a covered entity without repercussion.[39] In nearly all other situations, the covered entity must obtain valid authorization or provide the individual with an opportunity to object to the use or disclosure of protected health information.[40] The Privacy Rule explicitly lists three situations where authorization must be obtained: psychotherapy notes, marketing, and sale of protected health information.[41] Marketing and sale of health information each present an opportunity for entities to profit off of data that is personal and integral to the well-being of a person.

---

[34] The Privacy Rule also applies to "business associates," which are persons who participate in business practices alongside or on behalf of the defined covered entities, in specific circumstances. *See id.*; *see also* 45 C.F.R. § 164.104.
[35] 45 C.F.R. § 164.502(a).
[36] 45 C.F.R. § 164.502(b).
[37] 45 C.F.R. § 164.502(h).
[38] 45 C.F.R. § 164.502(a)(1).
[39] 45 C.F.R. § 164.502(d).
[40] 45 C.F.R. § 164.502(a)(1)(iv).
[41] 45 C.F.R. § 164.508(a)(2)-(4).

Overall, the Privacy Rule is a comprehensive regulation that allows use and disclosure of protected health information only in specific limited situations. The language and breadth of the Rule strongly suggest a preference towards keeping such information as private as possible, and only allowing disclosure when it would benefit the individual or when necessary for treatment or payment of healthcare. At the time of its promulgation, healthcare was mostly limited to traditional models of humans visiting doctor's offices to receive care, and technology was not as integrated into the daily lives of Americans as it is today.[42] This is part of the reason the entities to which the Privacy Rule applies are limited to those traditionally associated with healthcare. However, as will be discussed, technology has disrupted the healthcare industry in many ways, both positive and negative. Notably, businesses that operate primarily as technology companies and secondarily as providers of healthcare now collect significant amounts of health information. Changing times call for changes to regulations.

b. CMIA

California is the first state to significantly regulate health data, electronic or otherwise, and increase health data privacy protections for its residents with its 2013 amendments to the CMIA.[43] Most of the CMIA definitions resemble the HIPAA definitions. For example, "medical information" is defined as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment."[44] This is virtually identical in meaning to the HIPAA definition of "health information" because a broad range of information relating to a person's physical or mental health or condition is protected under the regulation if it is created or received by a designated entity.

However, more entities are covered by the CMIA than by HIPAA.[45] In addition to the traditional providers of healthcare, the

---

[42] For example, a diabetes patient in 1996 would most likely communicate with her doctor in person or over the telephone. She would not be able to track her blood sugar levels with a biosensor device that connects to a mobile application on her phone and sends updates to her doctor.

[43] Nick Stamos, *California Expands the Confidentiality of Medical Information Act to Personal Health Records and Mobile Applications*, ALSTON & BIRD PRIVACY & CYBERSECURITY BLOG (Sept. 11, 2013), https://www.alstonprivacy.com/california-expands-the-confidentiality-of-medical-information-act-to-personal-health-records-and-mobile-applications.

[44] CAL. CIV. CODE § 56.05(i) (2019)

[45] CAL. CIV. CODE § 56.06 (2019).

CMIA applies to three types of business organizations in California.[46] First, it applies to companies that maintain health data:

> Any business organized for the purpose of maintaining medical information . . . in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual . . . shall be . . . subject to the requirements of this part.[47]

For example, a technology company that builds, maintains, and licenses software to be used as a database for patient medical records is regulated by the CMIA.

Second, the CMIA applies to healthcare technology companies. Specifically, it applies to

> [a]ny business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information . . . in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual . . .[48]

For example, a business that developed a mobile application for the purpose of allowing users to input and maintain their personal health information is subject to the CMIA regulation.

Finally, the CMIA applies to any business licensed to sell cannabis for medical purposes.[49] By expanding the types of businesses to which the regulation applies, California has broadly expanded the overall scope of medical data privacy to which its residents are entitled.

I. ISSUE

When the HIPAA Privacy Rule became effective in 2003, smartphones were clunky, expensive, and not widely used by the

---

[46] *Id.*
[47] CAL. CIV. CODE § 56.06(a).
[48] CAL. CIV. CODE § 56.06(b).
[49] CAL. CIV. CODE § 56.06(c).

general American public.[50] The thought of using a mobile phone to track and maintain personal health data was nearly inconceivable. It was not until 2007 that Apple's iPhone kick-started innovation in the smartphone industry and spurred on a new wave of personal technology.[51] Over the past thirteen years, the popularity and usefulness of smartphones has steadily risen. In 2019, 81% of U.S. adults owned a smartphone[52] and that percentage has surely continued to grow since then. This is in addition to the 74% of U.S. adults who own a personal computer and the 52% who own a tablet computer.[53]

The market for digital health tools has grown exponentially with the widespread adoption of smartphones, tablets, and personal computers.[54] Many digital health tools are designed to be paired with a wearable device that can track a person's physical metrics, ranging from fitness trackers that count the wearer's steps to heartrate to insulin pumps which can be controlled from an app. A 2017 report found that there were over 318,000 health apps and 340 wearable devices on the market at the time with over 200 applications being added to app stores each day.[55] If this rate has remained steady, there were over half a million health apps on the market in 2020. This is in addition to digital tools that are available for use on personal computers or as web applications that individuals may access through a web browser.

Some people do not mind sharing their whole lives with the world; others are generally private people who wish to publicly share limited glimpses of their lives. Neither outlook on life is inherently better than the other. But the nature of information is such that once it is shared, it cannot be taken back. This is especially true in a digital world where data and information can travel far and wide once posted or shared.[56] Data posted on social media or logged in a mobile app is generally stored on remote servers. Even if a user

---

[50] Owen Andrew, *The History and Evolution of the Smartphone: 1992-2018*, TEXT REQUEST (Aug. 28, 2018), https://www.textrequest.com/blog/history-evolution-smartphone/.

[51] Charles Arthur, The history of smartphones: timeline, THE GUARDIAN (Jan. 24, 2012), https://www.theguardian.com/technology/2012/jan/24/smartphones-timeline.

[52] *Mobile Fact Sheet*, PEW RESEARCH CENTER (Jun. 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile.

[53] *Id.*

[54] Murray Aitken, et al., *The Growing Value of Digital Health*, IQVIA INSTITUTE (Nov. 2017), accessible at https://www.iqvia.com/-/media/iqvia/pdfs/institute-reports/the-growing-value-of-digital-health.pdf?_=1606164349006.

[55] *Id.*

[56] Lazaro Gamino, *How data travels across the internet*, THE WASHINGTON POST (May 31, 2015), https://www.washingtonpost.com/graphics/national/security-of-the-internet/bgp.

"deletes" the data, it is often stored in an unreadable, yet accessible, format on the host's servers for a set period of time.[57] Furthermore, a public post may be screenshotted[58] by anyone who views the post, which takes any control of the information away from the original poster. Because of this, individuals should have the right to choose whether or not certain personal data will be shared publicly, especially if that data is potentially embarrassing. Given the "no take backs" nature of information, public policy should skew in favor of protecting personal sensitive data. Policy should automatically allow those who wish to keep it this information private to do so, while also allowing those who wish to share it to do so as well.

This intrinsic harm may be difficult to quantify[59], but the risk of potential economic harm exists as well. While it is a violation of the Family and Medical Leave Act and the Americans with Disabilities Act to discriminate in employment matters on the basis of a medical condition[60], the reality is that employers may consider the overall health of employees when making hiring, promotion, or firing decisions. Should an employer gain unfettered access to a prospective employee's personal health records, the employer may use this information against him or her in making employment decisions. For example, if two candidates for an open position are equally qualified for the role, the employer may look to other factors that may indicate one is a better long-term investment. The employer may consider overall health as an indicator of which candidate would need to take less time off from work, which may use less health insurance benefits, and which candidates physical and mental health would allow him or her to advance or continue in the role for a longer period of time. Thus, if employers were able to access prospective employees' personal health data, employees may risk losing out on jobs, and consequently employer-sponsored health insurance.[61]

There are also social and psychological risks associated with public knowledge of an individual's medical or other health information.[62] Mental health issues and disorders in particular carry

---

[57] Jada Green, *Here's What Really Happens When You 'Delete' Something on the Internet*, MEN'S HEALTH (Oct. 20, 2015), https://www.menshealth.com/technology-gear/a19547921/deleted-social-media-posts/.

[58] A screenshot, or screen grab, is when a digital image is captured of the entire screen, or part of the screen, of a smartphone, tablet, or computer.

[59] Richard S. Saver, *Medical Research and Intangible Harm*. 74 U. CIN. L. REV. 941, 945 (2006).

[60] *See* 29 U.S.C. § 2615; *see also* 42 U.S.C. § 12112.

[61] Nass, *supra* note 5 (citing LAWRENCE O. GOSTIN & LINDSAY F. WILEY, *PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT*, (3rd ed. 2016)).

[62] Norman Sartorius, *Stigmatized Illnesses and Health Care*, 48(3) CROAT MED J. 396 (2007).

significant stigma in American society.[63] Often, persons with mental health disorders such as anxiety and depression are reluctant to seek help. Furthermore, those who do seek help often fail to follow through with full treatment due to the stigma around mental illness.[64] Physical diseases also commonly carry stigma of different kinds. Persons diagnosed with contagious diseases such as HIV and other sexually transmitted diseases may be ostracized in social settings.[65] Individuals would be more likely to seek treatment and other help for physical and mental health conditions knowing that doing so would not expose them to societal stigma or exclusion.

Could a simple answer to alleviate the privacy risks associated with individually identifiable health data be to anonymize or otherwise de-identify the data in storage? The European Union's General Data Privacy Regulation (GDPR) contemplates de-identification as a method for maintaining data privacy.[66] Businesses which track and maintain individually identifiable health data can anonymize the data such that the individual is no longer identifiable.[67] However, the bar to do this is extremely high,[68] given that roughly 87% of Americans can be identified with three data points: zip code, date of birth, and gender.[69] Pseudonymization, an alternative to anonymization, is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information that is kept separate.[70] However, depending on the specific method used to anonymize data, it could be relatively easy to re-identify such data.

As the use and development of technology in the healthcare industry has proliferated, so too has the amount of personal, individually identifiable health data being collected, transmitted, and stored. Unfortunately, because most of the companies who build and maintain digital health tools (and the data systems underlying them) do not qualify as a covered entity under HIPAA, there is little regulation regarding how this information may be used and disclosed. Health data is among the most sensitive categories of data, and individuals should have the right to keep such information private. Some may choose to allow limited or unlimited access to

---

[63] Patrick Corrigan, *How Stigma Interferes with Mental Health Care*, 59(7) AM. PSYCHOL. 614 (2004).
[64] *Id.*
[65] 48(3) Croat Med J. 396.
[66] GDPR Article 11.
[67] Matt Wes, *Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization*, IAPP (Apr. 25, 2017), https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization.
[68] *Id.*
[69] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, CARNEGIE MELLON UNIVERSITY, 2000 at 2.
[70] 2016 O.J. (L 119) 33.

their health data, but permitting others' access to personal health data should be a conscious choice.

The definition of "health information" as provided in 45 C.F.R. § 160.103 and the list of entities covered by the Privacy Rule should both be amended to include businesses that are not part of the traditional healthcare model, such as healthcare companies who solely operate digitally.

II. ARGUMENT

A. The HIPAA Privacy Rule Should Be Modified to Expand the Types of Entities to Which It Applies.

The most effective solution to fully protect individually identifiable health data is to modernize and expand the HIPAA Privacy Rule. The healthcare industry has changed significantly in the years since the Privacy Rule was promulgated such that the Rule no longer offers adequate protection of private health information. While the provisions of the rule are comprehensive enough to offer adequate protection, the entities to which the Privacy Rule apply and the definition of "health information" are outdated. The definition of health information should be expanded to include information that is created or received by the types of digital health businesses which process and store large amounts of consumer personal health data. Similarly, the Privacy Rule should be amended to apply to these types of businesses. The language in California's CMIA would be a logical point of reference for how to do this.

i. Effects of Increased Investment in Digital Health Companies

Digital healthcare is a rapidly growing industry, especially due to the COVID-19 pandemic. In the first three quarters of 2020, digital health companies in the United States raised $9.4 billion in venture funding.[71] This puts the industry on track to have its largest funding year ever[72] and demonstrates how more money than ever before is being invested in digital health products and services in the United States. Naturally, this influx of capital gives the digital health

[71] Elaine Wang & Sean Day, *Q3 2020: A new annual record for digital health (already)*, ROCK HEALTH (Oct. 2020), https://rockhealth.com/reports/q3-2020-digital-health-funding-already-sets-a-new-annual-record/.

[72] For comparison, these types of companies raised $5.8 billion and $7.8 billion in the 2017 and 2019 calendar years, respectively. *See* Nina Chu, et al., *2020 Midyear Digital Health Market Update: Unprecedented funding in an unprecedented time*, ROCK HEALTH (Jul. 2020), https://rockhealth.com/reports/2020-midyear-digital-health-market-update-unprecedented-funding-in-an-unprecedented-time.

industry the resources to produce more products and offer more services in the coming years. Some examples of new digital health products include a wearable cardiac defibrillator which can be monitored by a smartphone app and a software platform for health systems to manage patient payments.[73] Some examples of new services include a full-service digital pharmacy complete with prescription delivery and on-demand urgent care services.[74]

Consumer adoption of digital health products and services also surged in 2020 due to the COVID-19 pandemic.[75] For example, one healthcare provider reported a 50% increase in telehealth visits in one week and another provider reported a 2000% in increase in telehealth visits over a two month period.[76] One key impediment to wider consumer adoption of these products and services that a majority of consumers do not view digital products and services as effective when compared their tangible, in-person counterparts.[77] This issue has potential to be solved quickly: with increased investment in the digital health industry, companies will have the financial resources to improve the user experiences. Such capital is necessary to hire user experience (UX) researchers and designers, fund product teams with product managers and technical talent, and conduct behavioral analytics to further iterate on and improve existing products and services.[78] With key improvements to the user experience, digital health companies will be able to offer consumers more effective experiences. With this barrier to wider adoption removed, overall consumer adoption of digital health tools is likely to increase.

The surge in investment, combined with increased consumer adoption, means that the amount and types of personal health data being collected by digital health companies will grow exponentially in years to come. Consequently, the risks associated with leaving such data inadequately protected will also increase. The most comprehensive step to take to alleviate the risks is to enact federal regulations which require companies to adequately protect data.

ii. Benefits of Increased Regulation of Health Data Privacy

---

[73] *Id.*
[74] *Id.*
[75] Safavi, *supra* note 4.
[76] *Id.*
[77] *Id.*
[78] Ivan Annikov, *How to Conduct Effective UX Research – A Guide*, TOPTAL (last visited Jan. 2, 2021), https://www.toptal.com/designers/user-research/budget-ux-user-research.

New technologies have spurred on innovation in the healthcare industry, but federal data privacy regulations have not matched pace. In fact, there has been no significant modification to the HIPAA Privacy Rule since 2013.[79,80] As described above, the Privacy Rule still focuses on and applies to businesses which have adopted traditional provider-patient models of healthcare. The scope of information which could be protected by the Privacy Rule is broad: information must only relate to an individual's health or provision or payment of healthcare. Many lawyers would say that the "relate to" standard is often open to interpretation in court and could be construed broadly to encompass any data tangentially relating to an individual's health. However, the Privacy Rule is limited by two requirements: (1) information must be transmitted between designated entities, and (2) the Privacy Rule only applies to these such designated entities.

Thus, many of the digital health companies that have formed since the Privacy Rule was enacted fall outside its scope. This includes the hundreds of thousands of companies whose primary product is a mobile application which collects or monitors an individual's health data, as well as the companies that have recently secured hundreds of millions of dollars in funding to improve or mass produce their products and services. Because there is no regulation addressing the privacy of individuals' health data, digital health companies are generally free to create their own policies for protection of such data. Some companies elect to place privacy at the top of their list of priorities.[81] Other companies choose speed over security, prioritizing quick growth, user adoption, and profit over data privacy and digital security.

Given the lack of data privacy regulation, it is understandable that concerns about data privacy or security is the number one barrier to adoption of digital health tools in the United

---

[79] The HIPAA Omnibus Rule became effective in 2013 and was the most recent modification to HIPAA; *supra* note 9.

[80] New changes to the Rule were proposed in December 2020, but they do not meaningfully expand the scope of entities to which the Rule applies. Anna Kraus, et al., *HHS Announces Proposed Changes to HIPAA's Privacy Rule*, COVINGTON DIGITAL HEALTH (Dec. 21, 2020), https://www.covingtondigitalhealth.com/2020/12/hhs-announces-proposed-changes-to-hipaas-privacy-rule/.

[81] For example, Apple considers data privacy a fundamental right and lists it as one of the company's core values. Apple makes smartwatches which include fitness trackers and automatically includes a health app on its iPhones. Apple operating systems and mobile apps are designed to protect users' rights to control which data remains private and which data is allowed to be shared with Apple and with third parties. *Privacy*, APPLE (2020), https://www.apple.com/privacy/.

States.[82] A majority of individuals do not trust digital health companies to adequately protect their private health information or refrain from selling their data to third-party marketing companies.[83] Trust in traditional healthcare providers to keep private health information secure has also declined in recent years.[84] Most, if not all, digital health companies require consumers to agree to their privacy policies before engaging with their digital products or services. But these privacy policies are generally long and littered with legal language. The important information regarding how the company makes use of user data is used is often buried in pages of fine print.

It is a heavy, if not impossible, burden on the consumer to research exactly which data is collected, how and where it is stored, to whom the data may be disclosed, and what cybersecurity protections the company has in place to prevent breaches. For many, the effort involved in ascertaining the details regarding how each digital health company collects, analyzes, stores, and possibly sells data outweighs the potential benefits of engaging with new companies. And even when a company spells out its privacy policy succinctly in plain, simple terms, some consumers are leery that it may fail to abide by its own policy or that its cybersecurity is insufficient to prevent data breaches by third-party hackers.[85]

Modifying the Privacy Rule to cover digital health companies, in addition to traditional healthcare providers, would bolster consumer trust in digital healthcare. Because the Privacy Rule is set up to encompass a broad range of information, a provision should be added that reduces the limitations on the Privacy Rule. Digital health companies should be included as covered entities and the definition of "health information" should be modified to include information created or received by digital health companies. Given its nature as a state regulation of health data privacy, the CMIA is a logical point of reference for how lawmakers could implement these changes. Following California's example, a provision could be added that would deem digital health businesses as "healthcare providers" solely for purposes of the Privacy Rule. This would reduce the limitations of the Privacy Rule in the necessary ways without adding superfluous regulation. Digital healthcare businesses would be covered entities under HIPAA for Privacy Rule purposes and health information that is created or received by digital health businesses would be protected.

---

[82] Safavi, *supra* note 4.
[83] *Id.*
[84] *Id.*
[85] *Id.*

Adapting the Privacy Rule to modern times this way would require any company that collects, processes, or otherwise handles personal health data to take steps to protect it. Increasing consumer trust in the data privacy of digital health would allow many more individuals across the country, not only in California, to reap the myriad benefits of digital healthcare at all stages of the patient journey. At the wellness and prevention stage, more consumers will feel comfortable using digital health tools, such as mobile apps, to track and manage their diet, exercise, stress levels, sleeping habits, and other aspects of daily life. If they choose, there may be opportunities for patient-consumers to connect and share these types of data with primary care physicians, specialty doctors, and other healthcare providers. This would allow healthcare providers to obtain a fuller picture of their patients' health than a normal patient information form could provide.

Digital health tools can offer convenience regarding to routine activities such as accessing medical records, managing appointments, and refilling prescriptions. Any patient can make use of these types of tools. Patients with diseases that require consistent monitoring could decrease the number of weekly, monthly, or annual visits to their doctor by making use of bio sensors that connect to a mobile phone or computer, and send data to the doctor. For example, Bailey, the diabetic woman from the introductory example, could use a digital health tools to monitor her blood sugar levels. She could log this information in a mobile application that tracks her blood sugar levels and automatically shares this data with designated persons, such as her doctor, a family member, and friends who live nearby. If there was ever an emergency in which Bailey was in immediate danger due to low blood sugar levels, nearby persons would be able to attend to Bailey quickly.

For these reasons, the Privacy Rule should apply to all business which operate in the digital healthcare space.

B. Why State-Specific and Other Legislative Solutions Would Be Less Effective and More Laborious

Amending the Privacy Rule to include the proposed changes is certainly not the only possible solution. It is, however, the most comprehensive yet simple way to accomplish the goal of adding privacy protection to individually identifiable health information without imposing any undue burden on digital health businesses. The Privacy Rule already exists, contains desirable language, and has been interpreted by courts. Instead of drafting brand new legislation from scratch, lawmakers could simply expand the scope of the Privacy Rule to include more businesses that are non-traditional providers of healthcare.

i. Confusion, Difficulty in Implementation, and Potential to Become Obsolete

California was the first state to implement a state-specific solution to regulate health data privacy with an amendment to the CMIA in 2013.[86] Considering no other states have implemented similar solutions in the past seven years, it is unlikely health data privacy regulations will begin appearing in all states. This leaves the majority of individuals in the United States without adequate legal protection of their private health data information. However, if each state were to decide to enact its own health data privacy regulation, the business of digital healthcare could soon become more confusing than it is worth.

For example, assume a digital health company was interested in conducting business in several states, each with its own set of health data privacy regulations. The company would need to analyze each set of regulations and determine if it is able to comply. To be able to conduct business in all states, the company would have to comply with the strictest set of regulations. Thus, the regulations of all other states would essentially be rendered null, unless or until they were modified to be stricter. Many digital health companies conduct business across all fifty states and internationally. If each state had its own regulations, digital health companies would have to constantly keep tabs on fifty sets of regulation (fifty-two, if you include Puerto Rice and the District of Columbia) to ensure they are in compliance with all regulations at any given point.

There is also potential for mass confusion among companies and consumers. The internet is not itself a physical location; technically, only the servers that host applications and websites have physical locations. These servers can be placed in locations far from a business's physical office, if it has one, often in another state. If some states chose to enact data privacy regulations and others did not, digital health companies would have to determine whether a given state's regulations apply if the company does not transact business there, but its application happens to be hosted on a server in that state. Consumers similarly could be confused about whether or not their data would be subject to privacy regulations depending on where they are in the country.

Furthermore, it is possible Congress will enact general data privacy regulations in the near future. Given how much technology has become part of Americans' everyday lives, this would come as no surprise. If each state were to enact its own health data privacy regulation, it could potentially become preempted by federal regulation that applies to all types of data, not only health data.

---

[86] Stamos, *supra* note 43.

V. CONCLUSION

HIPAA is long overdue for an update. Just like software must be updated consistently to the safest and most useful versions, health regulations must also be updated to adapt to changing times to provide the most protection and usefulness. This note has discussed the state of the HIPAA Privacy Rule today as well as a potential model example for what the Privacy Rule could look like. The primary issue is that the rise of smartphones, tablets, and personal computers has paved the way for new technologies that have changed the healthcare landscape. Patients can connect with doctors and get prescriptions through mobile applications without ever speaking to them in person. Persons with mental health issues can speak with therapists and receive treatment via videoconference. Individuals can track and monitor hundreds of data points related to their individual health, such as calories burned, steps taken, and hours slept.

Digital health technologies show no signs of slowing down production; if anything, the demand for such technologies has greatly risen due to the COVID-19 pandemic. More individually identifiable health data, which should be kept private, goes unprotected each day simply because there is no requirement to protect it. Concerns about health data privacy stand as a key barrier to wider adoption of digital health technologies, which have the potential to offer better solutions to patient care than traditional models of healthcare. By modifying the HIPAA Privacy Rule to offer a broader range of protection to individually identifiable healthcare data, consumer trust in (and consequently, adoption of) digital healthcare would increase. Other solutions would be less effective and would essentially create a competition or race towards the most privacy protections. Amending the existing Privacy Rule is the best solution to address the issues of the day.