MENTAL HEALTH MOBILE APPS AND THE NEED TO UPDATE FEDERAL REGULATIONS TO PROTECT USERS

Kewa Jiang[*]

ABSTRACT

With greater societal emphasis on the need for better mental health services coupled with COVID-19 limits, mental health mobile applications have significantly risen in variety, availability, and accessibility. As more consumers use mental health mobile applications, more data is generated and collected by mobile application companies. However, consumers may have the false assumption that the data collected is protected under HIPAA or have an expectation of privacy protection higher than current regulations afford. This Note examines HIPAA, Health Breach Notification Rule, and section 5 of the Federal Trade Commission Act, as well as how these regulations fall short of protecting the data and privacy of consumers who use mental health mobile apps. This Note then advocates for a preventative approach by Congress towards potential data breaches and protection of data from mental health mobile apps. Looking prospectively, the Note suggests how the gaps in consumer protection can be federally remedied.

TABLE OF CONTENTS

* B.A. in Psychology from UC Berkeley (‘15) and a J.D. from the University of Southern California (‘21). I was a Saks Student Scholar with the Saks Institute for Mental Health Law, Policy, and Ethics at the University of Southern California Gould School of Law. My deepest gratitude to my parents and friends who cheered me along the way.

INTRODUCTION

In 2019, 51.5 million adults aged eighteen or older were diagnosed with "any mental illness" in the United States.[1] The unprecedented disruption of the COVID-19 pandemic beginning in 2020 then further exacerbated the conditions of those diagnosed with mental illness and the general mental welfare of all. In particular, the pandemic and the need for social distancing caused major disruptions in how mental health services are provided.[2] Consequently,

1. SUBSTANT ABUSE & MENTAL HEALTH ADMIN., KEY SUBSTANCE AND MENTAL HEALTH INDICATORS IN THE UNITED STATES: RESULTS FROM THE 2019 NATIONAL SURVEY ON DRUG USE AND HEALTH 5 (2020), https://www.opioidlibrary.org/wp-content/uploads/2020/10/SAMHSA-2020-Key-SU-and-Mental-Health-Indicators-report.pdf. "Any mental illness" is defined by the National Institute of Mental Health (NIMH) as mental, behavioral, or emotional disorder that can vary in impact and severity of impairment in individuals. *Mental Illness*, NAT'L INST. OF MENTAL HEALTH, https://www.nimh.nih.gov/health/statistics/mental-illness.shtml (last updated Jan. 2022).

2. *COVID-19 Disrupting Mental Health Services in Most Countries, WHO Survey*, WORLD HEALTH ORG. (Oct. 5, 2020), https://www.who.int/news/item/05-10-2020-covid-19-disrupting-mental-health-services-in-most-countries-who-survey.

individuals and even mental health facilities turned to mental health mobile applications as a means of remotely receiving and providing care.[3]

During the past two years, downloads of mental health mobile apps from Apple's App Store and Google Play Store skyrocketed along with the types of mental health applications available.[4] The American Psychological Association estimates there are around 20,000 mental health applications available on the App Store alone.[5] The types of applications range from ones that address specific disorders, such as depression or anxiety,[6] to ones that provide specific types of therapy, such as cognitive behavioral therapy (CBT).[7] There are also applications that provide more holistic mental wellness guidance, such as guided meditation[8] or daily mood trackers. Mental health applications also provide users with a sense of anonymity, which can be beneficial for many users who fear the stigma associated with mental illness. In fact, more than half of individuals with mental illness do not seek treatment or help for their conditions due to stigma.[9]

When interacting with a mental health app, users provide a wealth of sensitive information. For instance, mental health apps commonly ask users to input their name, email address, gender, age, or date of birth. The apps will also ask for financial information if there are in-app purchases. Along with identifying information and depending on the type of app, users must also provide information about their psychological well-being to receive the promised benefit from the app. This may take the form of short surveys that ask the users about their mood and daily activities, or journal prompts that require the users to provide intimate details of their lives and emotional states. Some users might assume, since they provided health information to the app, that the Health Insurance Portability and Accountability Act (HIPAA)[10] might apply to their information or that the app would disclose to users if they were sharing information with third party companies.[11] However, several

3. Tanya Basu, *The Coronavirus Pandemic Is a Game Changer for Mental Health Care*, MIT TECH. REV. (Mar. 20, 2020), https://www.technologyreview.com/2020/03/20/905184/coronavirus-online-therapy-mental-health-app-teletherapy.

4. Kira Herzog, *Mental Health Apps Draw Wave of New Users as Experts Call for More Oversight*, CNBC (May 24, 2020, 11:15 AM), https://www.cnbc.com/2020/05/24/mental-health-apps-draw-wave-of-users-as-experts-call-for-oversight.html.

5. *Id.*

6. FEELMO, https://www.feelmo.com (last visited Apr. 28, 2022).

7. BLOOM, https://www.enjoybloom.com (last visited Apr. 28, 2022).

8. HEADSPACE, https://www.headspace.com (last visited Apr. 22, 2022).

9. *Stigma, Prejudice and Discrimination Against People with Mental Illness*, AM. PSYCHIATRIC ASS'N, https://www.psychiatry.org/patients-families/stigma-and-discrimination (last visited Apr. 17, 2022).

10. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

11. Herzog, *supra* note 4; U.S. DEP'T OF HEALTH & HUM. SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT

studies have shown mental health apps frequently share data with third parties without disclosing to users of the fact.[12]

As the use of mental health apps continue to rise, many mental health providers, privacy specialists, and legal scholars are raising the alarm about the "regulatory grey area" these apps inhabit.[13] The concern is the ambiguity in regulations may create confusion amongst regulators, users, and app developers about the required level of protection for user data. The confusion may in turn result in lower protection for user data, leaving it vulnerable to security breaches or inappropriate access by third party companies mining the data. In terms of security breach, the mere disclosure that an individual is using a particular mental health app could be personally and socially damaging since it may "out" the individual's mental illness diagnosis. Given the social stigma that still exists around mental illness, some users may not want their coworkers, family, or friends to know, for example, that they use the app Simple Bipolar to manage their disorder. Additionally, third party companies may be able to target a person with ads for specific products knowing when the person may be more susceptible to buy them based on mood tracking data.[14]

Therefore, in examining just the federal regulations, there are many ways federal agencies can adapt to the evolving methods in which mental health services are provided. While there are also substantial state laws that may apply, these will not be included in this Note's discussion. Currently, under the Department of Health and Human Services (HHS), HIPAA only applies to covered entities,[15] business associates, and some hybrid entities.[16] This leaves out most mental health apps because they are usually not created by a covered entity or by business associates on behalf of a covered entity. Likewise, the Federal Trade Commission (FTC) may bring enforcement actions under Section 5 of the FTC Act against "unfair or deceptive acts"[17] or under the Health Breach Notification Rule.[18] However, the FTC enforcement actions typically occur after a data breach has already happened, since only then do the app developers violate their promise to consumers to maintain the

---

REGULATED BY HIPAA 4 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

12. Herzog, *supra* note 4.

13. *Id.*

14. Kaitlyn Tiffany, *Online Ads Can Be Targeted Based on Your Emotions*, VOX (May 21, 2019, 1:20 PM) https://www.vox.com/the-goods/2019/5/21/18634323/new-york-times-emotion-based-ad-targeting-sadness.

15. "Covered entities" is defined by HIPAA as (1) a health plan; (2) a health care clearinghouse; or (3) "a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." 45 C.F.R. § 160.103 (2022).

16. *Id.* §§ 160.103, 164.103; *see also HIPAA for Dummies*, THE HIPAA GUIDE, https://www.hipaaguide.net/hipaa-for-dummies (last visited Apr. 22, 2022).

17. 15 U.S.C. § 45(a)(1).

18. 16 C.F.R. § 318 (2022). The Health Breach Notification Rule is meant to regulate how and when companies contact customers and the FTC in the event of a security breach.

security of the data stated in their privacy policy. While the FTC's enforcement action is important in redressing past violations of consumer privacy, it is also closing the barn door after the horse has already bolted. Moreover, the Food and Drug Administration (FDA) tangentially regulates medical health apps as it relates to the quality, safety, and efficacy of the apps but not with regards to protecting privacy and data.[19]

Congress should consider taking a preventative approach to regulating mental health apps. For instance, it can extend the application of HIPAA to include mental health apps as well as extend the definition of psychotherapy notes [20] to also include data generated by mental health app users. As a result, data from mental health apps would require stricter standards of protection under HIPAA which would allow application developers to be more proactive in preventing data breaches. This is in contrast to the reactive response of FTC enforcement actions under section 5 and the Health Breach Notification Rule which are triggered after a breach has occurred. Ultimately, Congress should begin to move mental health apps out of its current "regulatory grey area" in order to better protect mental health app users' privacy and data.

Part I gives an overview of the mental health apps that are commercially available to consumers, such as the types of services offered, the types of data collected, and the extent of the apps' privacy policies. Part II provides an outline of the current data protection under HIPAA, the protection of psychotherapy notes, and how HIPAA interfaces with mobile apps. Part III discusses section 5 of the FTC Act, the FTC's efforts to regulate data privacy under section 5, and Health Breach Notification Rule. Part IV delves into the gaps in protection of consumers' data from mental health mobile app under HIPAA, section 5 of the FTC Act, and Health Breach Notification Rule. Part V advocates for Congress to take a preventative approach to potential data breaches and protection of consumer data. Suggested remedies are to extend the definition of "covered entity" under HIPAA to encompass mental health mobile apps and to revise the definition of psychotherapy notes under HIPAA.

I. OVERVIEW OF MENTAL HEALTH APPS

Mental health applications are part of a broader category of mobile health apps, mHealth apps. mHealth apps encompass applications users can download on a mobile device, such as a tablet or smartphone, to link with wearable

19. *When May A Covered Health Care Provider Disclose Protected Health Information, Without an Authorization or Business Associate Agreement, to a Medical Device Company Representative?*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Aug. 8, 2005), https://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html.

20. Psychotherapy notes are given heightened protection under HIPAA only when generated by a mental health professional. 45 C.F.R. § 164.501 (2022).

technology, or to transform a mobile device into an extension of a medical device.[21] For instance, a Fitbit or an app that monitors heart rate can be categorized as mHealth apps.

In examining available mental health apps in particular for this Note, the majority are consumer-facing, standalone apps available for mobile devices. These apps are generally not linked to wearable technology, nor do they turn mobile devices into extensions of medical devices. Rather, there are a range of different services provided by each mental health application. The mental health applications examined will also not include those that connect users to traditional licensed therapists, such as Talkspace or BetterHelp. Given the variety of apps, this Part provides an overview of the types of services offered by mental health apps, the types of information collected by the apps, and the range of privacy policies provided to users.

A. *Types of Services Offered by Mental Health Apps*

A quick search of "mental health" in Apple's App Store reveals an array of mental health applications. The apps range from providing holistic mental well-being and specific support for a disorder to various types of therapy treatments. For instance, the popular meditation app, Headspace, offers users series of guided mindful meditations meant to address issues from lack of focus to grieving a loved one.[22] Users can pick and choose the topic and length of the guided meditations with no need for the user to input any information about their current mental state.[23]

In contrast, diagnostic, journaling, mood tracker, and behavioral tracker apps require a high level of engagement from users in order for users to receive the purported benefits. For example, Mental Health Tests claim to help users find out whether they have a mental health condition.[24] Users must answer a series of questions regarding their daily emotions and general dispositions to receive a diagnosis. Apps that promote journaling or track mood and behaviors also encourage daily engagement by the users. The journaling app Reflectly states its artificial intelligence will provide users with daily prompts, help users track their progress and gain insight into their feelings, and generate mood correlations with journal entries.[25]

Another category of mental health applications is designed for users to engage in specific types of therapy modalities, such as CBT or dialectical

21. WORLD HEALTH ORG., MHEALTH: NEW HORIZONS FOR HEALTH THROUGH MOBILE TECHNOLOGIES 6 (2011), https://www.who.int/goe/publications/goe_mhealth_web.pdf.

22. HEADSPACE, *supra* note 8.

23. *Id.*

24. *Mental Health Tests*, APPLE APP STORE, https://apps.apple.com/us/app/mental-health-tests/id1276818064 (last visited Apr. 22, 2022).

25. *Reflectly–Journal & AI Diary*, APPLE APP STORE, https://apps.apple.com/us/app/reflectly-mindfulness-journal/id1241229134 (last visited Apr. 22, 2022); *see also* REFLECTLY, https://reflectly.app (last visited Apr. 22, 2022).

behavioral therapy, or targeted to help specific disorders. These apps may be a blend of educational videos, journaling, surveys, and mood trackers that allow users to track their therapy progress or symptom management. For instance, the app Woebot is advertised as a talk therapy chat bot that will converse with users in order to guide them through CBT techniques.[26] Woebot is described as an on-demand therapist, available even at odd hours of the night when users need to process their emotions.[27] There are also apps that address specific disorders. For example, there are apps that are directed to bipolar disorder, such as eMoods Bipolar Mood Tracker,[28] post-traumatic stress disorder, such as PTSD Coach,[29] and eating disorders, such as Peace with Food.[30]

B. *Range of Information Collected by Mental Health Apps and their Privacy Policies*

Just as the range of services mental health apps offer vary, so do the types of user data that mental health apps collect as well as the length and depth of their respective privacy policies. Generally, the majority of applications reviewed asked users to provide identifiable information, such as name, email address, username, password, or phone number. Alternatively, there are a few apps that allow users to access services without the need for users to provide identifiable information.[31] Many applications will also collect mobile device identification, IP address of mobile device, and frequency of users' visits to the app.[32] For applications with services that require payment, users must also provide financial information. Many privacy policies state that billing or financial information is processed through a third-party company but disclaims any liability in the event the third-party company experiences a data breach. Depending on the type of services provided, some apps, such as Bloom (a CBT therapy and journaling app), explicitly state that mental health

26. Erin Brodwin, *I Spent 2 Weeks Texting a Bot About My Anxiety—And Found It To Be Surprisingly Helpful*, BUSINESS INSIDER (Jan. 30, 2018, 3:05 PM), https://www.businessinsider.com/therapy-chatbot-depression-app-what-its-like-woebot-2018-1.

27. *Id.*

28. *eMoods Bipolar Mood Tracker*, APPLE APP STORE, https://apps.apple.com/us/app/emoods-bipolar-mood-tracker/id1184456130 (last visited Apr. 22, 2022).

29. *PTSD Coach*, APPLE APP STORE, https://apps.apple.com/us/app/ptsd-coach/id430646302 (last visited Apr. 22, 2022).

30. *Peace with Food*, APPLE APP STORE, https://apps.apple.com/us/app/peace-with-food/id1358837136 (last visited Apr. 22, 2022).

31. Mind Matters provides a suite of different mental health apps that link to the same privacy policy. This policy states that "[t]he app does not require you to provide us with personally identifiable information (PII)." *Privacy Policy*, MINDMATTERS, https://www.mind-matters.co/privacy-policy-mh (last visited Apr. 22, 2022).

32. Robby Berman, *Do mHealth Apps Protect User Privacy?*, MEDICAL NEWS TODAY (June 21, 2021), https://www.medicalnewstoday.com/articles/do-mhealth-apps-protect-user-privacy.

information will be collected.[33] In contrast, Happify, an app that allows users to track their moods, does not explicitly state they collect mental health information.[34]

Privacy policies vary widely as well. Some are thorough and user-friendly, some are succinct, and some are sparse. A 2019 study found that only twenty-five out of the thirty-six top-ranked apps for depression and smoke cessation had a privacy policy.[35] Of the twenty-five apps with privacy policies, more than eighty percent shared data with Facebook, Google, or their affiliated companies.[36] Many either did not disclose or did not explicitly state to users that their data was shared with third parties.[37] For instance, Bold CBT, an app that allows users to practice CBT techniques, has a sparse privacy policy. Under privacy and data collection, Bold CBT's privacy policy states: "Your completed exercises are stored locally on your device and do not leave your device. Quite frankly, we don't want to read your thoughts."[38] Overall, the policy is less than a page long and does not provide information regarding whether data is shared with third parties, how data is stored, or what users can expect in the event of a data breach. On the other end of the spectrum, Bloom's privacy policy provides a thorough and at length disclosure of the types of information collected as well as how the information will be used, stored, and shared.[39] Similarly, MindDoc, an app that allows users to log their mental health and mood information, provides a user-friendly, frequently asked question format that allows users to quickly access policy information.[40]

II. BRIEF OVERVIEW OF HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

Based on the amount of information generated by users and collected by mental health mobile apps, some users might assume their health information is protected under HIPAA or that the information has heightened protection since it concerns mental health. However, in many instances that may not be the case. This Part gives an overview of who must comply with HIPAA and

33. *See, e.g.*, *Privacy Policy*, BLOOM, https://www.enjoybloom.com/privacy (last updated June 11, 2021).

34. *Legal*, HAPPIFY, https://www.happify.com/public/legal (last updated July 2020).

35. Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, 2 JAMA NETWORK OPEN, Apr. 2019, at 1, 3 tbl.1, 4.

36. *Id.* at 4; Herzog, *supra* note 4.

37. Herzog, *supra* note 4.

38. *Privacy Policy*, BOLD CBT, https://boldcbt.com/#privacy-policy (last visited Apr. 22, 2022).

39. *Privacy Policy*, *supra* note 33.

40. *Privacy Policy of MindDoc Health GmbH and Schön Klinik MVZ GmbH*, MINDDOC, https://mymoodpath.com/en/privacy-policy (last updated Feb. 1, 2021).

the privacy and security standards that must be followed. Then it delves into the psychotherapist-patient privilege and how mental health information is treated under HIPAA. For instance, it discusses the type of mental health information that qualifies as psychotherapy notes, which *are* given heightened protection. Lastly, it provides examples of how HIPAA interfaces with mHealth apps.

A. *Who Must Comply with HIPAA?*

HIPAA aims to create national standards for the protection of sensitive patient health information and to prevent any disclosure of such information without a patients' consent or knowledge.[41] HHS is tasked to implement regulations and standards, such as the HIPAA Privacy Rule and Security Rule.[42] Within HHS, the Office for Civil Rights (OCR) is responsible for ensuring HIPAA requirements are met and to investigate if there is suspected violations or breach of patient information.[43]

HIPAA specifically applies to "covered entities," defined as (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits health information in electronic form in connection with a covered transaction.[44] For example, hospitals, doctors, and similar health care providers would be considered covered entities under HIPAA. In 2013, HIPAA requirements were extended to include "business associates" of covered entities under the Health Information Technology for Economic and Clinical Health (HITECH) Act.[45] HITECH Act was enacted to incentivize increased use of electronic and digital medical records while also strengthening HIPAA privacy and security provisions.[46]

"Business associates" are defined as entities, such as health information organizations or e-prescribing gateways, that have access to protected health information (PHI)[47] in their daily operation in order to provide services to a covered entity.[48] Before a business associate begins to provide services to a

41. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/phlp/publications/topic/hipaa.html (last updated Sept. 14, 2018).

42. *Id.*

43. *HIPAA for Dummies*, *supra* note 16.

44. 45 C.F.R. § 160.103.

45. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, sec. 13301, §§ 13401, 13404 123 Stat. 226, 260, 264 (2009); *What Is the Relationship Between HITECH, HIPAA, and Electronic Health and Medical Records?,* HIPAA JOURNAL (Apr. 2, 2021), https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-health-medical-records.

46. *What Is the Relationship Between HITECH, HIPAA, and Electronic Health and Medical Records?*, *supra* note 45.

47. Under HIPAA, PHI refers to individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. 45 C.F.R. § 160.103.

48. *HIPAA for Dummies*, *supra* note 16; 45 C.F.R. §160.103.

covered entity, both parties complete a business associate agreement.[49] The agreement ensures that the business associate understands they must comply with HIPAA requirements to protect, maintain the integrity of, and restrict the uses and disclosure of any PHI.[50] A covered entity can be the business associate of another covered entity.[51] However, business associates do not include health care provider, plan sponsor, or a government agency.[52] Therefore, covered entities may disclose protected health information to health care provider, plan sponsor, or a government agency without first entering into a business associate contract or written agreement.[53]

B. *Standards for Privacy of Individually Identifiable Health Information*

The Standards for Privacy of Individually Identifiable Health Information, also known as the Privacy Rule, is the component of HIPAA that prescribes how PHI can be used and disclosed.[54] The Privacy Rule attempts to strike a balance between the protection of patient information with the need for secure flow of information between different stakeholders, such as the covered entity, patient, business associates, and regulators.[55] In striking such a balance, the Privacy Rule allows de-identified health information to be used and disclosed without patient authorization.[56] HIPAA provides strict guidance on the standard and types of information that must be removed in order for information to be considered de-identified. [57] For instance, names, geographic subdivisions smaller than a State, birth dates, and date of death are identifiers that must be removed.[58]

A covered entity can use or disclose PHI to the patient, other covered entity, or health care providers for treatment, payment, or health care operations without explicit authorization from the patient.[59] Patients also have the right to access, inspect, and obtain a copy of their own PHI.[60] If patient requests their medical records, covered entities are required to disclose. However, there are certain situations, such as when the records were compiled in

49. *HIPAA for Dummies*, *supra* note 16.
50. *Id.*
51. 45 C.F.R. § 160.103.
52. *Id.*
53. *See* 45 C.F.R. § 164.502(e); *Business Associates*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last visited May 19, 2022).
54. 45 C.F.R. §§ 164.500–164.534; *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Apr. 22, 2022).
55. *Health Insurance Portability & Accountability Act of 1996 (HIPAA)*, *supra* note 41.
56. 45 C.F.R. § 164.514(a).
57. *Id.* § 164.514(b)(2).
58. *Id.*
59. *Id.* § 164.506(c).
60. *Id.* § 164.524(b).

anticipation for civil, criminal or administrative proceedings, where patients are not allowed to access their medical records.[61] Covered entities must also disclose PHI if requested by HHS as part of an investigation, review, or enforcement action.[62]

C. *The Security Standards for the Protection of Electronic Protected Health Information*

In the current digital environment, most health providers store their records and patients' PHI electronically. The Security Standards for the Protection of Electronic Protected Health, also known as the Security Rule, are required safeguards that apply specifically to electronic PHI (e-PHI).[63] The required safeguards range from technical measures, such as transmission safety, to non-technical measures, such as access control and physical workstation layouts.[64] Covered entities and business associates must also meet the general requirements. These include: (1) ensuring the confidentiality, integrity, and availability of all e-PHI the covered entity or business associate creates, receives, maintains, or transmits; (2) protecting against any reasonably anticipated threats or hazards to the security or integrity of the e-PHI; (3) protecting against any reasonably anticipated uses or disclosures of the e-PHI that are not permitted or required under the Privacy Rule; and (4) ensuring compliance with the Security Rule by its workforce.[65]

There is flexibility in how the covered entity or business associates practically implement the Security Rules. [66] Covered entities and business associates may use security measures that are reasonable and appropriate to meet the general requirements.[67] In making reasonable and appropriate decisions, covered entities and business associates must consider several factors. Some of these factors include costs, likelihood of potential risk, criticality of potential risk occurring, and capabilities of covered entity or business associate.[68]

D. *Psychotherapist-Patient Privilege and Psychotherapy Notes*

Jaffe v. Redmond was a seminal case in establishing psychotherapist-patient privilege and influenced the heightened protection psychotherapy notes receive under HIPAA.[69] In *Jaffee*, the Supreme Court recognized that

61. *Id.* § 164.524(a)(ii).
62. *Id.* §160.310; *Summary of the HIPAA Privacy Rule*, *supra* note 54.
63. 45 C.F.R. §§ 164.302–164.318; *Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Apr. 22, 2022).
64. *Summary of the HIPAA Security Rule*, *supra* note 63.
65. 45 C.F.R. § 164.306(a)(1)–(4).
66. *Id.* § 164.306(b)(1).
67. *Id.*
68. *Id.* § 164.306(b)(2).
69. Jaffee v. Redmond, 518 U.S. 1, 10–15 (1996).

effective psychotherapy "depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fear."[70] Based on the need for confidentiality, as described in *Jaffe*, HIPAA defines "psychotherapy notes" as records (in any medium) produced by (1) a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that (2) are kept separate from the rest of the individual's medical record.[71]

Due to the sensitive nature of psychotherapy notes, use or disclosure requires patient authorization.[72] In comparison, general medical records can usually be used or disclosed by a covered entity for treatment, payment, and health care operations without explicit authorization.[73] However, a whole swath of medical information related to mental health is not considered psychotherapy notes and are not provided heightened protection. For instance, records about medication prescription, counseling session start and stop times, modalities and frequencies of treatment, results of clinical tests, and progress to date are not considered psychotherapy notes.[74]

E. *HIPAA and mHealth Apps*

Given the increasing number of mHealth app developers, including mental health apps, HHS developed several resources to help guide developers in determining whether they must comply with HIPAA. If a developer is creating an mHealth app as a business associate or subcontractor of a business associate on behalf of a covered entity, then they must comply with HIPAA.[75] For instance, HHS provides the scenario in which an app developer was contracted by a covered entity to develop an app for patient management services and information patients input into the app are integrated with the covered entity's electronic health records.[76] Here, the app developer is considered a business associate of the covered entity and must comply with HIPAA.[77] HHS also provided a scenario in which an app developer creates an app offered by a health plan and another "direct-to-consumer" version of the same app.[78] If the developer is able to keep the data from each version separate, the version offered by the health plan must comply with HIPAA as the developer

70. *Id.* at 10.
71. 45 C.F.R. § 164.501.
72. *Id.* § 164.524(a)(i); *Summary of the HIPAA Privacy Rule, supra* note 54.
73. 45 C.F.R. § 164.502(a)(ii).
74. *Summary of the HIPAA Privacy Rule, supra* note 54.
75. U.S. DEP'T OF HEALTH & HUM. SERVS., HEALTH APP USE SCENARIOS & HIPAA 1 (2016), https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf.
76. *Id.* at 3.
77. *Id.*
78. *Id.*

is considered as a business associate while the "direct-to-consumer" version does not need to comply with HIPAA.[79]

III. OVERVIEW OF FEDERAL TRADE COMMISSION ENFORCEMENT ACTIONS

Since many of the mHealth apps are not captured by the regulations of HIPAA, the FTC has stepped into the role of regulating privacy and cybersecurity of mHealth apps. This Part provides an overview of the FTC's enforcement power under the deceptive and unfair prong of section 5 of the Federal Trade Commission Act, how the FTC laid the foundation of its consumer data privacy protection powers, and its enforcement power under the Health Notification Breach Rule. This Part tracks the FTC's enforcement actions under the deceptive prong from the early days of the internet against GeoCities for failure to protect users' data[80] to 2021 when the FTC brought enforcement actions against mHealth app Flo Health. It then delves into the FTC expanding its data privacy protection powers under the unfair prong during its enforcement action against Wyndham Worldwide.[81]

A. *Section 5 of the Federal Trade Commission Act*

The FTC derives its enforcement power from section 5 of the Federal Trade Commission Act (FTC Act).[82] Specifically, the FTC is empowered to prevent persons or businesses from "using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[83] The scope of the FTC's power to declare an act or practice unfair is dependent on whether the act is "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers" and if the declaration is "not outweighed by countervailing benefits to consumers or to competition."[84]

1. Deceptive Acts or Practices

The FTC began regulating online commercial activities and consumer online privacy as early as the mid-1990s under the "deceptive acts or

79. *Id.*

80. Rachel Withers, *Before Facebook, There Was GeoCities*, SLATE (Apr. 16, 2018, 8:07 AM), https://slate.com/technology/2018/04/the-ftcs-1998-case-against-geocities-laid-the-groundwork-for-facebook-debates-today.html.

81. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 243–49 (3rd Cir. 2015).

82. 15 U.S.C. § 45(a)(2).

83. *Id.*

84. *Id.* § 45(n).

practices" prong of 15 U.S.C. §45(a).[85] Business practices would be deemed deceptive if they failed to provide the level of privacy or data security promised in their privacy policies.[86] In addition, it is considered deceptive business practice if a company collected, stored, used, or shared data in any way that was different than its disclosure to consumers in its privacy policy.[87] While businesses were not required to provide a privacy policy, as time went on it became a standard practice.[88]

One of the first consumer online privacy action the FTC brought under the deceptive prong was against GeoCities in 1999.[89] GeoCities was a website that allowed users to create their own personal webpages and to interact with other users via forums.[90] The FTC alleged that GeoCities deceived its users when it sold users' data to third party entities, such as "personal identifying, demographic, and/or interest information collected from consumers who register."[91] This violated the website's privacy policy which stated to users that information collected about them would not be sold without users' consent.[92] GeoCities settled the case with the FTC under a consent order, which required GeoCities to prominently display a privacy policy that would fully disclose to users how data will be collected and used.[93]

Since 1999, the FTC's enforcement actions against deceptive practices has grown to encompass mobile apps, including mHealth apps. For instance, the FTC brought enforcement actions against Flo Health, Inc., a mHealth app that allows users to track their menstrual and fertility cycles.[94] The FTC alleged Flo Health violated regulations when the company shared users' health information with outside data analytics providers despite promising users that the information collected would be kept private.[95] Flo Health, like GeoCities, settled the case with the FTC under a consent order.[96] The FTC's consent order required Flo Health, among other things, to disclose to consumers how

85. PETER P. SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 48 (3rd ed. 2020).

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. Complaint at para. 2, Geocities, F.T.C. Matter No. 9823015, Docket No. C-3850 (Feb. 12, 1999), https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm.

91. *Id*. para. 6.

92. *Id.* paras. 12–14.

93. Decision and Order, Geocities, F.T.C. Matter No. 9823015, Docket No. C-3850 (Feb. 5, 1999), https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do_.htm.

94. Complaint, Flo Health, Inc., F.T.C. Matter No. 1923133, (Jan. 13, 2021), https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

95. *Id.* at 1.

96. *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations That It Misled Consumers About the Disclosure of Their Health Data*, FED. TRADE COMM'N (Jan. 13, 2021), https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc.

much control they have over data use, how the company collects, maintains, uses, discloses, deletes, or protects users' personal information.[97] Flo Health must also instruct third party entities to destroy users' health information they may have received.[98]

2. Unfair Acts or Practices

Under the unfairness acts or practice prong of 15 U.S.C. § 45(a), the FTC "carries out its Section 5(a) mission to prevent unfair acts or practices in two ways: formal rulemaking and case-by-case litigation."[99] If an act or practice is litigated and adjudicated to be unfair, "the act or practice becomes in effect—like an FTC-promulgated rule—an addendum to Section 5(a)."[100] Recently, the FTC began regulating cybersecurity practices and protection of consumer online privacy and data under the unfairness prong. For instance, the FTC initiated enforcement actions against Wyndham Worldwide, which operates hotels and resorts throughout the United States, after the company experienced three separate data breaches of its servers.[101] As a result, numerous consumers' data was exposed, such as credit card numbers and home addresses.[102] Along with alleged deceptive practices, the FTC also alleged unfair practices because Wyndham failed to implement "reasonable and appropriate measures" to protect consumer data against unauthorized access.[103] Due to the breaches, consumers suffered substantial injuries that they "cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition."[104]

On Wyndham's motion to dismiss, it countered that the FTC did not have the authority to regulate cybersecurity under the unfairness prong and that they did not receive fair notice their cybersecurity practices could fall short of FTC provisions.[105] The Third Circuit Court of Appeals in 2015 affirmed the FTC's authority to regulate cybersecurity issues under unfair practices.[106]

---

97. Agreement Containing Consent Order at 3–4, Flo Health, Inc., F.T.C. Matter No. 1923133, (Jan. 13, 2021), https://www.ftc.gov/system/files/documents/cases/flo_health_order.pdf.

98. *Id.* at 4.

99. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1231 (11th Cir. 2018).

100. *Id.* at 1232.

101. Complaint for Injunctive and Other Equitable Relief at 2–3, Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 2:12-cv-01365-SPL (D. Ariz. June 26, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf.

102. *Id.* at 12–18.

103. *Id.* at 19.

104. *Id.*

105. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

106. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 243–49 (3rd Cir. 2015); *see also* Lesley Fair, *Third Circuit Rules in FTC v. Wyndham Case*, FED. TRADE

The Court also resoundingly rejected Wyndham's claim that they did not receive fair notice given the fact that their servers were breached on three separate occasions.[107]

B. *FTC and the Health Breach Notification Rule*

In February 2010, the FTC began enforcing the Health Breach Notification Rule (HBNR),[108] which is meant to regulate how and when companies contact customers and the FTC in the event of a security breach.[109] HBNR was promulgated as a result of the American Recovery and Reinvestment Act of 2009, which aimed to strengthen privacy and security protections for web-based businesses.[110] The HBNR is also meant to cover businesses that handle medical information but may not fall under the purview of HIPAA.[111]

Under the HBNR, vendors of personal health records (PHRs), PHR-related entities, or third-party service providers for a vender of PHRs or a PHR-related entity must comply with the regulations.[112] HBNR defines vendor of PHR as a business that "offers or maintains a personal health record" that is not a HIPAA-covered entity or is an entity that engages in actives as a business associate of a HIPAA-covered entity.[113] "PHR" is defined as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[114]

A breach of security occurs when there has been an "unauthorized acquisition of PHR-identifiable health information that is unsecured and in a personal health record."[115] PHR-identifiable health information is information that can potentially identify an individual or could reasonably be used to identify an individual.[116] For instance, an individual's address, health information, and date of birth, but not their names, are acquired without a company's authorization. While the individual's name is not included in the information

---

COMM'N (Aug. 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/08/third-circuit-rules-ftc-v-wyndham-case.

107. FTC v. Wyndham, 799 F.3d at 249–59; Fair, *supra* note 106.

108. 16 C.F.R. § 318.

109. *Health Breach Notification Rule*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/health-breach-notification-rule (last visited Apr. 22, 2022).

110. *Id.*

111. *Complying with the FTC's Health Breach Notification Rule*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule (last visited Apr. 22, 2021).

112. 16 C.F.R. § 318.3.

113. 16 C.F.R. § 318.2(j).

114. 16 C.F.R. § 318.2(d).

115. *Complying with the FTC's Health Breach Notification Rule, supra* note 111; *see also* 16 C.F.R. § 318.2(a).

116. 16 C.F.R. § 318.2(e).

acquired, the information that was taken could reasonably be used to determine the name of the individual.

Companies that experience breaches must notify all customers whose information was affected without "unreasonable delay" within sixty days since awareness of the breach.[117] In cases where five hundred or more individuals' information is affected, the company must also notify the media of the breach.[118] In terms of the FTC, if the breach affected five hundred or more individuals then the company must notify the FTC no later than ten business days after the discovery of the breach.[119] If the breach affects fewer than five hundred individuals then the company can maintain a log of each breach and submit them annually to the FTC.[120]

IV. APPLICATION OF REGULATIONS TO MENTAL HEALTH APPS

In reviewing the protections afforded by HIPAA and the reach of the FTC to protect consumer data privacy, gaps begin to emerge that leave mental health mobile apps and, more broadly, mHealth apps in its current "regulatory grey area." The following sections highlight such gaps in regulations that either lead to confusion among patients and app users about what information is protected or the regulations are so narrowly defined that whole swaths of information are not protected. This Part also spotlight the limitations of the FTC's enforcement power as well as the advantages and disadvantages of the Health Breach Notification Rule.

A. *Gaps in HIPAA Protection and Mental Health Apps*

1. Narrow Definition of PHI and Patient Confusion

Under HIPAA, PHI is narrowly defined to only include information generated by a covered entity.[121] However, if a patient discloses PHI to a third-party, non-covered entity, the information is no longer protected by HIPAA. This definition of PHI creates confusion for patients who may incorrectly believe that their mental health information continues to receive the same level of protection by a mental health app as it does by their therapist, who is a covered entity. However, most mental health apps are not considered covered entities because they were not created by or at the direction of a health plan, health care clearinghouse, or a health care provider. Therefore, the mental health apps do not need to comply with HIPAA's standard of protection. Similarly, patients may be confused that data from using an app's "direct-to-

117. *Id.* § 318.4(a).
118. *Id.* § 318.5(b).
119. *Id.* § 318.5(c).
120. *Id.*
121. 45 C.F.R. § 160.103.

consumer" version will not receive the same protection as the health plan version of the same app. Patients' misunderstanding of when HIPAA applies means that "consumers may not be equipped to evaluate the privacy and security implications that attach to" apps from non-covered entities.[122]

2. Narrow Definition of Covered Entity

As aforementioned, most mental health apps are not created on behalf of covered entities or business associates.[123] As a result, many mental health apps do not have to comply with HIPAA and may have a lower level of protection and scrutiny of how user data is handled. This is despite most apps soliciting identifiable medical and psychological information from users in order for the user to receive its intended benefits. If data from mental health app users is considered HIPAA protected health information, developers may more likely be on alert from the start to provide stronger protection of such data.

3. Narrow Definition of Psychotherapy Notes

HIPAA also provides a narrow definition for the types of medical records that are considered psychotherapy notes. Not only do psychotherapy notes need to be kept separate from a patient's general medical records, but only notes created by a therapist are designated as psychotherapy notes.[124] However, this definition appears to be rooted in an overly traditional understanding of how mental health services are provided and how patients engage with their mental health today. For instance, the definition conjures an image of a patient on a couch talking about their mental state while a therapist diligently listens and writes on a notepad. In contrast, even prior to the pandemic, many individuals have been taking more involved approaches to managing and coping with their mental illness. For instance, patients use apps, such as Feelmo: Mental Health Support,[125] to track their emotional state across time and want to see for themselves their emotional patterns rather than require a therapist to be the gatekeeper of their own mental health information.

As a result of the narrow definition of psychotherapy notes, users' mental health app data is not considered psychotherapy notes. Unlike under HIPAA, which require covered entities to obtain explicit consent prior to disclosure of psychotherapy notes, mental health apps may not need such an explicit consent from users before disclosing mental health data to third party entities. Instead, many users unknowingly agree to sharing their data to third party

122. U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 11, at 4.

123. Thomas Germain, *Mental Health Apps Aren't All as Private as You May Think*, CONSUMER REPS. (Mar. 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244.

124. 45 C.F.R. § 164.501.

125. FEELMO, https://www.feelmo.com (last visited Apr. 22, 2022).

entities when they sign up for the app since the disclosure may be buried in lines of legalese in the privacy policy. On the other hand, given that many mental health apps do not have a comprehensive privacy policy or a sparse policy in the first instance, [126] users' data about their mental health may be shared and exploited by third party entities without users' knowledge or consent.

B. *Limits of Protection Under Section 5 of FTC Act and Mental Health Apps*

While the FTC was successful in asserting the unfairness prong in *FTC v. Wyndham Worldwide Corporation*,[127] the claim still requires the FTC to "stretch its interpretation of Section 5 even further to justify its enforcement actions."[128] In fact, the FTC has been accused of being vague and overly broad in its assertions of violations of the "unfair acts or practice" prong in relation to data security. [129]In comparison, the FTC has been more successful in asserting the deceptiveness prong claim against mHealth apps, such as Flo Health. However, the FTC's authority is ultimately limited in regulating privacy since the FTC Act does not explicitly grant the agency authority to oversee privacy and cybersecurity.[130] In addition, FTC enforcement action under the deceptiveness prong may be limited given many mental health apps have very sparse privacy policies. Thus, it may be argued that a mental health app cannot deceive users if it does not promise them anything.

The FTC's enforcement action against LabMD, a medical testing laboratory, exposed the limits of the unfairness prong in regulating poor data security measures. A LabMD employee inadvertently shared patients' health information through a peer-to-peer sharing platform.[131] The FTC alleged LabMD engaged in an unfair act when the company failed to "provide reasonable and appropriate security for personal information on its computer networks."[132] The FTC cited security measures LabMD failed to perform, such as not adequately securing the company's computer network, using suitable risk-assessment tools, or providing data security training to employees.[133] The Eleventh Circuit Court of Appeals determined that while LabMD's failure to maintain a reasonable data-security program constitutes

126. *See*, *Privacy Policy*, *supra* note 38.

127. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 243–49 (3rd Cir. 2015).

128. Jianyan Fang, *Health Data at Your Fingertips: Federal Regulatory Proposals for Consumer-Generated Mobile Health Data*, 4 GEO. L. TECH. REV. 125, 150 (2019).

129. *See* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018).

130. Fang, *supra* note 128, at 150–51.

131. *FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy*, FED. TRADE COMM'N (Aug. 29, 2013), https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

132. *LabMD, Inc.*, 894 F.3d at 1225.

133. *Id.* at 1227.

an unfair act or practice under section 5(a), the FTC's cease and desist order also lacked specificity.[134] Therefore, the cease and desist order was unenforceable since it failed to state acts or practices LabMD should stop engaging in.[135] Rather, the cease and desist mandated an overly broad overhaul of LabMD's security system.[136]

C. *Progress and Drawbacks of Health Breach Notification Rule*

While the enactment of the HBNR marks a step towards more protection of health information, it also has several drawbacks. HBNR demonstrates that regulatory agencies recognized the need to monitor entities that hold patient health information but are not considered a covered entity under HIPAA.[137] HBNR is a step towards shifting non-covered entities, such as mHealth apps, away from the "regulatory grey area" they inhabit.

However, HBNR remains a reactive approach to data security and privacy rather than a preventative approach. The rule is triggered only when protected health information is breached[138] rather than providing increased protection and regulation for the collection, use, and storage of health information. Therefore, users' information and privacy still remain at risk of exploitation by third party entities and potential breaches. The difference now is that under HBNR, users must be notified, and the FTC can potentially bring enforcement actions in the event of a breach.

However, in the ten years since HBNR was enacted, the FTC has failed to bring any enforcement actions under the rule. In fact, it was noted in a letter to the FTC from Senator Bob Menendez, House Representative Bonnie Watson Coleman, and House Representative Mikie Sherrill that "despite several high-profile cases of period-tracking apps disclosing personal health information to third parties without their users' authorization, the FTC has never taken any enforcement actions related to the Health Breach Notification Rule."[139] For instance, while the FTC brought enforcement actions against Flo Health, one of the period-tracking apps referenced by the lawmakers, the agency failed to allege violation of HBNR.[140]

---

134. *Id.* at 1237.
135. *Id.* at 1236.
136. *Id.* at 1237.
137. *Complying with the FTC's Health Breach Notification Rule*, *supra* note 111.
138. *Health Breach Notification Rule*, *supra* note 109.
139. Jessica Davis, *Congress Urges FTC Crackdown on Health Apps Via Breach Notice Rule*, HEALTHITSECURITY (Mar. 8, 2021), https://healthitsecurity.com/news/congress-urges-ftc-crackdown-on-health-apps-via-breach-notice-rule.
140. Elizabeth G. Litten, *Flo Health App Fallout: HIPAA-Like Breach Notification Rule Not Enforced by FTC*, FOX ROTHSCHILD LLP (Jan. 14, 2021), https://hipaahealthlaw.foxrothschild.com/2021/01/articles/breach-notification/flo-health-app-fallout-hipaa-like-breach-notification-rule-not-enforced-by-ftc.

V. PUBLIC POLICY: PREVENTATIVE VS. REACTIVE APPROACHES

Many of the current regulations take a reactive, or ex post, approach in which the regulations are triggered after users' privacy or data has been violated. This approach places regulatory agencies one step behind app developers and would-be hackers, leaving users in a vulnerable position. For instance, under the deceptiveness prong of the FTC Act, a violation must first occur before enforcement action can be made but at this point users' information are already compromised.[141] The FTC's attempt to implement preventative measures in businesses' data security under the unfairness prong was met with resistance and a need for specificity.[142] Similarly, the HBNR is a reactive measure that is triggered after a health information data breach.

While reactive regulations under the FTC are important tools in addressing violations that have occurred, there also needs to be a preventative approach to protecting mental health app users' privacy and data. Moreover, a reactive approach often leaves app developers with little guidance when creating mental health apps, such as the standard of protection collected data must receive. In contrast, a preventative approach can generate clearer guidelines regarding the standards mental health app developers must follow to reduce users' vulnerability to privacy and data violations.

There is much Congress can do to increase mental health app users' privacy and data protection given the limitations and gaps in existing federal regulations regarding mHealth apps generally. A crucial preventative step is for Congress to extend HIPAA to apply to mental health app developers and move them away from the "regulatory grey area." In turn, mental health app developers are on notice that their product must have heightened protection and regulation on collection and use of users' data.

In addition, Congress should extend the definition of psychotherapy notes under HIPAA to keep pace with how mental health services are provided today. The definition should encompass not just notes created by therapists, but also notes and information generated by the patient as part of receiving mental health treatment or in managing mental illness symptoms, as many of the mental health apps include functions for users to journal about their emotions, track their moods, and manage daily symptoms. In many respects, the data generated by users is even more voluminous and up to date than most therapy notes, especially as more people turn to mental health apps. Patients may see their therapists only once a week, but they can interact with a mental health app every day. Therefore, it appears antiquated to only protect information a therapist generates.

In extending the definition of psychotherapy notes, the data generated will also receive an even more heightened standard of protection than general medical records. For instance, currently under HIPAA, patients must consent

141. SWIRE & KENNEDY-MAYO, *supra* note 85, at 48.
142. *See LabMD, Inc.*, 894 F.3d.

to any disclosure or use of psychotherapy notes.[143] If the definition is extended, the health information generated by mental health app users must by default also require consent before disclosure to third parties. Therefore, mental health app developers must obtain user consent even if the app does not have a privacy policy or a privacy policy that does not disclose whether information is shared with third parties.

Alternatively, legislators can work to pass laws that specifically address mHealth mobile apps to bridge the gap in consumer data protection not covered by HIPAA and FTC Act. For instance, Senator Amy Klobuchar and Senator Lisa Murkowski first introduced the bill, "Protecting Personal Health Data Act," on June 13, 2019.[144] While it failed to pass in 2019, the bill was re-introduced on January 22, 2021.[145] The proposed bill is meant to address the concerns of how "current law does not adequately address the emerging privacy concerns presented by these new technologies [such as home DNA testing kits and health data tracking apps]."[146] For instance, the proposed bill empowers the Secretary of Health and Human Services to promulgate regulations in consultation with the FTC and other stakeholders to "help strengthen privacy and security protections for consumers' personal health data that is collected, processed, analyzed, or used by consumer devices, services, applications, and software."[147] In addition, the bill calls for the creation of a national task force on health data protection meant to, among other purposes, advice on cybersecurity threats, development in security standards, and privacy concerns and protection standards related to consumer and employee health data.[148] The introduction of this bills is a hopeful sign that Congress is taking steps to address the need for more regulations in how health information is collected, used, and shared in the field of emerging technologies.

CONCLUSION

As more and more people turn to mental health apps as a convenient means to cope with daily stresses or manage mental illness symptoms, an increasingly vast wealth of users' psychological information is being generated. The additional impact of the COVID-19 pandemic on individual's mental health and mental health providers' ability to give care also means that mental health apps are likely to continue increasing in popularity. Thus,

143. 45 C.F.R. § 164.524(a)(i); *Summary of the HIPAA Privacy Rule, supra* note 54.

144. Protecting Personal Health Data Act, S. 1842, 116th Cong. (2019).

145. Protecting Personal Health Data Act, S. 24, 117th Cong. (2021).

146. *Klobuchar, Murkowski Introduce Legislation to Protect Consumers' Private Health Data*, U.S. SENATOR AMY KLOBUCHAR (June 14, 2019), https://www.klobuchar.senate.gov/public/index.cfm/2019/6/klobuchar-murkowski-introduce-legislation-to-protect-consumers-private-health-data.

147. Protecting Personal Health Data Act, S. 24, 117th Cong. § 4(a) (2021).

148. *See id.* § 5.

Congress and federal agencies must ensure federal regulations keep pace in order to protect users' privacy and data.

Given the highly sensitive nature of mental health records and the stigma surrounding mental illness, mental health app users must be provided heightened protections. *Jaffe* noted that in a relationship between a patient and a therapist there is a need for "an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fear."[149] A mental health app developer should now provide the same atmosphere of confidence to the relationship between a user and a mental health app.

149. Jaffee v. Redmond, 518 U.S. 1, 10 (1996).