DOUBLE SECRET PROTECTION: BRIDGING FEDERAL AND STATE LAW TO PROTECT PRIVACY RIGHTS FOR TELEMENTAL AND MOBILE HEALTH USERS

JOSH SHERMAN†

ABSTRACT

Mental health care in the United States is plagued by stigma, cost, and access issues that prevent many people from seeking and continuing treatment for mental health conditions. Emergent technology, however, may offer a solution. Through telemental health, patients can connect with providers remotely—avoiding stigmatizing situations that can arise from traditional healthcare delivery, receiving more affordable care, and reaching providers across geographic boundaries. And with mobile health technology, people can use smart phone applications both to self-monitor their mental health and to communicate with their doctors. But people do not want to take advantage of telemental and mobile health unless their privacy is protected. After evaluating the applicability of current health information privacy law to these new forms of treatment, this Note proposes changes to the federal regime to protect privacy rights for telemental and mobile health users.

INTRODUCTION

Imagine that you are a single parent living in a small town and that your child has just been diagnosed with a serious mental illness. Treatment options in your area are few and far between. A handful of psychiatrists and psychologists practice in your town, but none specializes in treating your child's condition. You would have to drive over fifty miles to reach an appropriate specialist. As a sole provider, this is unworkable with your schedule.

You are thus delighted when you learn that your child will not need to travel at all to be treated by a mental health specialist. From a computer at your home, your child can use videoconferencing

† Duke University School of Law, J.D. expected 2018; Florida State University, B.A. Political Science & Sociology, 2015.

technology to receive treatment. You and your child consult a psychiatrist and a psychologist, and your child begins to meet regularly and develop relationships with each. Your child's prognosis steadily improves, and you are grateful for the technology that has allowed it to happen. But you are horrified when your computer is hacked and a clip from your child's therapy session is exposed over the internet. Your child's classmates learn of the clip and your child, shouldering the burden of mental health's stigma, begins to slip back into the confines of mental illness.

Telehealth,[1] the remote electronic provision of health care, can connect patients and providers, alleviating healthcare access issues such as the one in the above hypothetical. In particular, telehealth expands access to specialists,[2] to mental health providers in geographically rural or sparsely populated areas,[3] and to healthcare

1. Because terminology regarding telehealth is varied in the law and the legal literature, this Note adopts the following definitions at the outset. Telehealth, the broadest term, refers to "the use of advanced telecommunication technologies to exchange health information and provide healthcare services across geographic, time, social and cultural barriers." Jennifer M. Little, *Into the Future: The Statutory Implications of North Carolina's Telepsychiatry Program*, 93 N.C. L. REV. 863, 866 (2015) (internal quotations omitted) (quoting ADAM WILLIAM DARKINS & MARGARET ANN CARY, TELEMEDICINE AND TELEHEALTH: PRINCIPLES, POLICIES, PERFORMANCE, AND PITFALLS 2 (2000)). Whereas telehealth "includes the delivery of *all* health care," telemedicine refers more narrowly to the use of "*medical* treatment to treat a disease." *Id.* (emphasis added). Intuitively, telemental health describes the use of telehealth in mental health treatment. Telepsychiatry and telepsychology both fall under telemental health's umbrella. Telepsychiatry, also a subset of telemedicine, involves the remote delivery of psychiatric care, whereas telepsychology refers to the remote delivery of psychological care. *Id.* Other telehealth variants, such as telepharmacology and teleradiology, are beyond the scope of this Note. For clarification on the distinction between telehealth and mobile health, see *infra* note 9.

2. Sy Atezaz Saeed, John Diamond & Richard M. Bloch, *Use of Telepsychiatry To Improve Care for People with Mental Illness in Rural North Carolina*, 72 N.C. MED. J. 219, 219–20 (2011). Remote technology can also provide greater access to "the right provider in a culturally sensitive context," connecting, for example, Spanish-speaking patients and providers. Jessica Sun Choi, *Mental Health Services Via Skype: Meeting the Mental Health Needs of Community College Students Through Telemedicine*, 25 S. CAL. REV. L. & SOC. JUST. 331, 340 (2016) (quoting Brian J. Grady, Nancy Lever, Dana Cunningham & Sharon Stephan, *Telepsychiatry and School Mental Health*, CHILD ADOLESCENT PSYCHIATRIC CLINIC N. AM. (2011), https://www.e-psychiatry.com/pro/Telepsychiatry-and-School-Mental-Health.pdf [https://perma.cc/M7YM-NFE2]); *see also* Timothy Curtin, *The Continuing Problem of America's Aging Prison Population and the Search for a Cost-Effective and Socially Acceptable Means of Addressing It*, 15 ELDER L.J. 473, 492 (2007) (noting similarly that, for inmates, "something as simple as access to bilingual specialists was greatly improved by telemedicine, with prison health administrators particularly impressed by the improved quality of psychiatric care").

3. Saeed et al., *supra* note 2, at 219–20. This also creates a virtuous cycle—because telehealth providers, wherever located, can reach greater populations of patients, telehealth has "improved recruiting and retention of mental health professionals in underserved or rural areas." *Id.* at 220.

providers generally for homebound patients.[4] In addition, the economic benefits of telehealth are laudable, reducing transaction costs associated with traveling and waiting to see healthcare providers in person.[5] In the telemental health setting, where physical examinations are generally not required to properly diagnose, treat, and monitor patients,[6] the cost-benefit calculus especially favors telehealth. Another benefit is that obtaining treatment remotely heightens anonymity because it reduces the odds of running into your doctor in public and eliminates encounters with other patients in the traditional waiting room setting. Patients can thus circumvent the deterrent effects of stigma by obtaining treatment anonymously.[7] Indeed, the most rapid expansion of telehealth is therefore occurring in the behavioral health setting.[8] Additionally, mobile health applications and devices enable users to self-monitor and track medications and symptoms, access "inferred data" generated from such user inputs, and communicate either or both categories of information to providers.[9]

---

4. *See id.* (discussing how telepsychiatry can increase "access to mental health services in nursing homes, hospice, and other extended care facilities").

5. *Id.* Telehealth also mitigates opportunity costs associated with missing work or school to attend therapy sessions. *Id.* Additionally, these cost reductions translate to a "greater likelihood of compliance with therapy." *Id.* Telehealth also reduces costs for hospitals by providing access to specialists not employed full-time on their campuses. *Id.* These cost benefits are also well distributed, as telehealth has "reduced geographic and socioeconomic health disparities" by affording greater access to medical professionals. *Id.*

6. Arthur J. Fried, Paul A. Gomez & Purvi B. Maniar, *Behavioral Health and Population Health Management: Is It Time for Real Progress?*, 9 J. HEALTH & LIFE SCI. L. 57, 86 (2016). *But see* Choi, *supra* note 2, at 344 ("Although psychiatrists tend to have limited physical contact with patients, in-person examinations may be required in certain situations, such as when prescribing certain medications.").

7. Choi, *supra* note 2, at 340; Saeed et al., *supra* note 2, at 220.

8. Fried et al., *supra* note 6, at 89.

9. David D. Luxton et al., *mHealth for Mental Health: Integrating Smartphone Technology in Behavioral Healthcare*, 42 PROF. PSYCHOL.: RES. & PRAC. 505, 506 (2011); *see also* J. Frazee, M. Finley & J.J. Rohack, *mHealth and Unregulated Data: Is This Farewell to Patient Privacy?*, 13 IND. HEALTH L. REV. 384, 396–97 (2016) ("Inferred data is information that is inferred from existing data through analytic models—for example, analyzing a user's dietary patterns to predict that this particular user will likely develop type 2 diabetes."). For further terminological clarification, mobile health (sometimes referred to as "mHealth") refers to "medical and public health practice supported by mobile devices." Frazee et al., *supra*, at 385 (quoting WORLD HEALTH ORG., MHEALTH: NEW HORIZONS FOR HEALTH THROUGH MOBILE TECHNOLOGIES 6 (2011), http://www.who.int/goe/publications/goe_mhealth_web.pdf [https://perma.cc/PR83-JRNQ]). There are a wide range of mobile health applications dealing with various aspects of physical and mental health. This Note, however, limits the discussion on mobile health technologies to the mental health context. To the extent that information put into mobile health applications is transmitted, whether synchronously or asynchronously, to health care providers,

But in the age of WikiLeaks, Snapchat nudes, and easily compromised email servers, concerns about telecommunication confidentiality could not be more salient. In the healthcare context, security concerns are particularly pressing.[10] In one study, 94 percent of healthcare organizations surveyed experienced a data breach in the previous two years, and 45 percent experienced more than five such breaches.[11] Creating and enforcing laws to safeguard confidential health information is essential. A mental-healthcare breach could expose particularly sensitive information, making patient privacy interests especially prominent.[12]

Privacy and security laws are thus vital to protect patients. The federal landscape is governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the rules promulgated under it, the HIPAA Privacy and Security Rules (the Rules). The Rules are beginning to show signs of age following substantial advances in health technology in the last twenty years.[13] At the same time, states have their

---

the use of such technology properly qualifies as "telehealth" under this Note's definition. To the extent that health information put into or derived from mobile health applications is *not* transmitted to providers (either because the data are not transmitted at all, or because data are transmitted to nonprofessionals, such as the parents of a child user), mobile health falls outside telehealth's umbrella. This final distinction becomes relevant when analyzing the applicability of the HIPAA Security Rule to these technologies. For further discussion, see *infra* Part III.A.3.

10. *See* Pierron Tackes, *Going Online with Telemedicine: What Barriers Exist and How Might They Be Resolved?*, OKLA. J.L. & TECH., Jan. 2015, at 1, 8 (highlighting consumers' privacy concerns and the commonality of health data breaches).

11. *See* Rene Quashie, *Things That Should Keep the Telehealth Community Awake at Night (Part 1)*, EPSTEIN, BECKER, GREEN: TECHHEALTH PERSPECTIVES (June 10, 2013), http://www.techhealthperspectives.com/2013/06/10/things-that-should-keep-the-telehealth-community-awake-at-night-part-1 [https://perma.cc/SX3N-LRFC] (adding that "nothing threatens the future viability of telehealth more than lax privacy and security"). For example, a recent breach involving Emory Healthcare exposed health information of about 80,000 patients. Rachel Z. Arndt, *Emory Healthcare Cyberattack Affects 80,000 Patient Records*, MOD. HEALTHCARE (Mar. 2, 2017), http://www.modernhealthcare.com/article/20170302/NEWS/170309983/emory-healthcare-cyberattack-affects-80000-patient-records [https://perma.cc/X8HT-6C3Y].

12. As one commentator notes:

> [F]ear of security breaches may dissuade patients from disclosing sensitive or stigmatizing information to their physicians. Considering the stigma surrounding mental health treatment, the need to protect medical information in today's age of rapidly advancing technology remains vital to the expanding use of telepsychiatry and telemental health services. Patient privacy is crucial to effective health care services, as medical professionals need maximum information 'to obtain adequate patient histories, make correct diagnoses, and provide patients with appropriate treatments.'

Choi, *supra* note 2, at 351–52 (quoting Keith A. Bauer, *Privacy and Confidentiality in the Age of E-Medicine*, 12 J. HEALTH CARE L. & POL'Y 47, 50 (2009)).

13. For further discussion of how HIPAA does not sufficiently protect telemental health patient privacy, see *infra* Part III.A.

own rules and regulations, often in conflict with one another.[14] Further complicating the picture, the terrain is ever changing, as more than one hundred and fifty telehealth bills were introduced in state legislatures during 2016 alone.[15] Legal ambiguities disincentivize growth that would otherwise be spurred by providers and institutional investors alike.[16] Moreover, patients concerned for their privacy might be deterred from using the technology in the first place.[17] In order to capture all the benefits that telemental health has to offer, the law must account for the privacy interests of telemental health patients.

Part I of this Note traces problems in the infrastructure of mental health care in the United States to the failures of deinstitutionalization. It further examines the rise and promise of telemental and mobile health and posits that privacy concerns threaten the appeal and utility of these treatment and self-care modalities. Part II sketches out the current legal environment, focusing on the Rules and their preemptive status. Part III applies the Rules to telemental and mobile health, identifies both formal and functional failings that render stored and transmitted data inadequately protected, and proceeds to analyze state approaches. Part IV advocates for a federal solution that addresses the current deficiencies of the preemptory Rules as they pertain to telemental and mobile health.

I. INSTITUTIONAL FAILURES AND ALMOST-PROMISING REMEDIES

This Part explores historical and contemporaneous institutional and cultural issues that frustrate the utility of mental health treatment. Current issues with stigma, cost, and access to mental health care can be traced to the mass release of long-term mental health patients from

14. *See* Adam D. Romney & Sean R. Baird, *Skype Sessions: Emerging Legal Issues in Tele-Mental Health Services*, 28 HEALTH L. 32, 32–33 (2015) (explaining the panoply of state privacy and telemedicine laws). In addition, "[u]nlike some fields of healthcare, such as nursing, there is currently not a reliable 'interstate compact' for the allied mental health professionals through which a practitioner's license in one state is recognized as sufficient to permit practice in another state." *Id.* at 32.

15. Most addressed Medicaid reimbursement, professional board standards, and interstate licensing issues. *See, e.g.*, *Telehealth Medicaid & State Policy*, CTR. FOR CONNECTED HEALTH POL'Y, http://cchpca.org/telehealth-medicaid-state-policy [https://perma.cc/F8CN-UCDJ]. For a discussion of other state telehealth laws which address patient privacy and security, see *infra* Part III.B.

16. Romney & Baird, *supra* note 14, at 33; *see also* Tackes, *supra* note 10, at 15 ("[T]he complex matrix of differing state and federal regulation still remains the major barrier to the standardization and widespread use of telemedicine.").

17. Choi, *supra* note 2, at 351–52.

institutional confinement. The insurgent growth in telemental health promises to combat these stigma, cost, and access issues, but for a glaring gap in the current regime—sufficient security with respect to patients' sensitive health information. Securing patient privacy is necessary to realize the benefits of this otherwise promising technology.

A. Deinstitutionalization

The mid-twentieth-century mass release of mental health patients from long-term confinement, known as deinstitutionalization, resulted in major stigma, cost, and access issues for mental health care.[18] Before deinstitutionalization, most mental health care patients received treatment in institutions where patients were "locked away from the public, monitored by doctors and nurses, and often abused by the staff."[19] Expenses largely went toward housing for institutionalized patients rather than their medical treatment—because long-term patients were not expected to recover, they were generally denied treatment altogether.[20]

The process of deinstitutionalization began in 1956 as researchers, medical professionals, law enforcement, and government officials began to doubt the prudence of widespread institutionalized treatment for the mentally ill.[21] Five years later, Congress created the Joint Commission on Mental Health to streamline the process of deinstitutionalization.[22] Deinstitutionalization then progressed rapidly.[23] By the mid-1970s, the vast majority of mental institutions and asylums had been shuttered.[24]

---

18. *See* Samantha M. Behbahani, Ivelisse Barreiro & Patricia Rivera, *The Patient Protection and Affordable Care Act: Will Parity for Mental Health Care Truly Be Achieved in the 21st Century?*, 10 INTERCULTURAL HUM. RTS. L. REV. 153, 155–58 (2015) (discussing the continuing detrimental impacts of deinstitutionalization, such as the vicious cycle of incarceration for the mentally ill); David Chorney, *A Mental Health System in Crisis and Innovative Laws to Assuage the Problem*, 10 J. HEALTH & BIOMEDICAL L. 215, 219–20 (2014) (arguing that telemental health can help solve the nationwide post-deinstitutionalization mental health crisis).

19. Chorney, *supra* note 18, at 219.

20. CHRIS KOYANAGI, LEARNING FROM HISTORY: DEINSTITUTIONALIZATION OF PEOPLE WITH MENTAL ILLNESS AS PRECURSOR TO LONG-TERM CARE REFORM 1, 4 (2007), https://kaiserfamilyfoundation.files.wordpress.com/2013/01/7684.pdf [https://perma.cc/N9HD-FUV3].

21. Chorney, *supra* note 18, at 219.

22. *Id.* The Joint Commission's adopted posture centered around releasing mentally ill patients from institutions into "community health centers." *Id.*

23. *Id.*

24. Matthew Smith, *Deinstitutionalization and After: What Went Right and What Went Wrong With the Closure of Psychiatric Asylums?*, PSYCHOL. TODAY (May 12, 2013),

The Joint Commission's deinstitutionalization posture advocated transferring mental health patients to community health centers designed for social reintegration.[25] However, lacking sufficient funding, the development of these centers lagged far behind the rate at which mentally ill patients were ejected from long-term institutional confinement.[26] The lag had several consequences. For many patients unable to seek or continue treatment in a community health center, their families shouldered the burden of caring for them.[27] But family members were even less proficient at providing patients the medical treatment they needed.[28] Others were not that lucky. Mentally ill patients in resource-deficient communities without family caregivers were fundamentally helpless and exposed, and many were left homeless.[29]

Deinstitutionalization also brought many mentally ill people into the criminal justice system.[30] The capacity- and treatment-related inadequacies of community health centers left many patients with

---

https://www.psychologytoday.com/blog/short-history-mental-health/201305/deinstitutionalization-and-after [https://perma.cc/BB52-KM55].

25. *See generally* THE JOINT COMM'N ON MENTAL ILLNESS AND HEALTH, ACTION FOR MENTAL HEALTH: FINAL REPORT OF THE JOINT COMM'N ON MENTAL ILLNESS AND HEALTH (1961) (advocating for community-based mental health care and against the construction of large scale mental hospitals).

26. Chorney, *supra* note 18, at 220.

27. *Id.*

28. *Id.* Unable to provide actual medical treatment, family members were so helpless in the face of mental illness that law enforcement officers and medical officials often encouraged them to divert their mentally ill relatives into the criminal justice system as their best opportunity for receiving treatment. As the psychiatrist and researcher Dr. Edwin Fuller Torrey found:

> The mentally ill also are sometimes jailed because their families find it is the most expedient means of getting the person into needed treatment. As the public psychiatric system in the United States has progressively deteriorated, it has become common practice to give priority for psychiatric services to persons with criminal charges pending against them. Thus, for a family seeking treatment for an [sic] family member, having the person arrested may be the most efficient way to accomplish their goal.
>
> . . . [In surveys,] numerous family members [have] confided that either the police or mental health officials had encouraged them in pressing charges against their family members to access psychiatric care for them.

E. FULLER TORREY, OUT OF THE SHADOWS: CONFRONTING AMERICA'S MENTAL ILLNESS CRISIS 40 (1997).

29. *See, e.g.*, John M. Quigley, Steven Raphael, Eugene Smolensky, Erin Mansur & Larry A. Rosenthal, *Homelessness in California*, PUB. POL'Y INST. OF CAL. (2001), http://urbanpolicy.berkeley.edu/pdf/ppic_homeless.pdf [https://perma.cc/4528-ABGR] (tracing homelessness in California in part to the failures of deinstitutionalization).

30. Chorney, *supra* note 18, at 221. Mental health patients "deinstitutionalized" during this period were about eight times more likely than the general population to be arrested. Larry Sosowsky, *Explaining the Increased Arrest Rate Among Mental Health Patients: A Cautionary Note*, 137 AMER. J. PSYCHIATRY 1602, 1602–05 (1980).

serious mental illness untreated, leading some to engage in deviant and criminal behavior as a result of their conditions.[31] Others struggled to find work and turned to crime as their only means of income.[32] Still others fell prey to manifestations of mental health stigma. The conduct of mentally ill people can diverge from social norms, often in ways that are not criminal, but in ways that attract attention. "Crime" describes conduct that so departs from social norms it can be described as "anti-social," which is not the same as conduct that is off-kilter from social norms. But "criminal" is in the eye of the beholder, and it is easier to make an inferential leap to find criminal conduct if a degree of socially abnormal conduct already exists.[33] Together, these factors spawned a vicious cycle—the more mentally ill people were seen as acting "criminally," the more they were brought into the criminal justice system, the stronger the association between mental illness and deviant behavior, and so on.[34] The result was effectively *reinstitutionalization*, as the mentally ill found themselves again confined to institutions without much hope that jails or prisons would provide more adequate treatment than the mental health institutions from which they had been released.

Deinstitutionalization therefore failed to provide mental health patients with viable opportunities for treatment. To the contrary, between family caregiving, homelessness, and incarceration, deinstitutionalization exacerbated stigma, cost, and access issues for mental health patients. Today, stigma, cost, and access issues continue to frustrate mental health treatment. Telemental and mobile health could be an important part of overcoming each of these problems and could account for the additional nuances of these problems that have arisen since deinstitutionalization.

---

31. Chorney, *supra* note 18, at 220. While the lack of treatment was not a change from their life inside institutions, these patients had previously been confined and therefore outside the purview of the criminal justice system.

32. *Id.*

33. *Id.*; *see also* Linda A. Teplin, *Criminalizing Mental Disorder: The Comparative Arrest Rate of the Mentally Ill*, 39 AM. PSYCHOLOGIST 794, 794 (1984) ("Data from . . . 1,382 police–citizen encounters . . . suggest[s] that the mentally ill are indeed being criminalized. . . . [F]or similar offenses, mentally disordered citizens had a significantly greater chance of being arrested than non-mentally disordered persons.").

34. Chorney, *supra* note 18, at 220.

B. Mental Health Today

Stigma, cost, and access issues continue to plague mental health care treatment to this day.[35] The stigma associated with mental illness remains strong.[36] On the micro level, stigma can foster self-destructive behavior in mentally ill individuals who end up believing that they cannot effectively treat and manage their conditions.[37] The stigma of mental illness also often prevents such people from seeking treatment in the first place because they do not want to encounter other mentally ill people when they seek treatment and fear being stigmatized

---

35. Mental illness itself has become widespread, now affecting nearly one in four adult Americans. Romney & Baird, *supra* note 14, at 32. In addition, the incidence of mental illness is increasing among high school and college students. Choi, *supra* note 2, at 334. Even if these reported increases stem in part from heightened reporting, the numbers in and of themselves underscore the magnitude of America's mental health problem. What is more, the problem of mental health is not self-contained, as medical studies link mental illness with physical illness and increased mortality. For example, one study found that in eight states,

> public mental health clients had a higher relative risk of death than the general populations of their states. Deceased public mental health clients had died at much younger ages and lost decades of potential life when compared with their living cohorts nationwide. Clients with major mental illness diagnoses died at younger ages and lost more years of life than people with non-major mental illness diagnoses. Most mental health clients died of natural causes similar to the leading causes of death found nationwide, including heart disease, cancer, and cerebrovascular, respiratory, and lung diseases.

Craig W. Colton & Ronald W. Manderscheid, *Congruencies in Increased Mortality Rates, Years of Potential Life Lost, and Causes of Death Among Public Mental Health Clients in Eight States*, PREVENTING CHRONIC DISEASE, Apr. 2006, at 1.

36. "[S]tigmas are cues that elicit stereotypes, knowledge structures that the general public learns about a marked social group." Patrick Corrigan, *How Stigma Interferes with Mental Health Care*, 59 AM. PSYCHOL. 614, 615 (2004). "Commonly held stereotypes about people with mental illness include violence (people with mental illness are dangerous), incompetence (they are incapable of independent living or real work), and blame (because of weak character, they are responsible for the onset of their disorders)." *Id.* at 616 (citations omitted).

37. Professor Corrigan explains the concept of "self-stigma,"

> [l]iving in a culture steeped in stigmatizing images, persons with mental illness may accept these notions and suffer diminished self-esteem, self-efficacy, and confidence in one's future. Research shows that people with mental illness often internalize stigmatizing ideas that are widely endorsed within society and believe that they are less valued because of their psychiatric disorder. Persons who agree with prejudice concur with the stereotype "That's right; I am weak and unable to care for myself!"

Id. at 618 (citations omitted); *see also* Beate Schulze & Matthias C. Angermeyer, *Subjective Experiences of Stigma. A Focus Group Study of Schizophrenic Patients, Their Relatives and Mental Health Professionals*, 56 SOC. SCI. & MED. 299, 299 (2003) ("[S]tigma [is] an '. . . attribute that is deeply discrediting . . .' and makes the person carrying it '. . . different from others and of a less desirable kind.' An awareness of the attribute then results in the belief that '. . . a person with a stigma is not quite human.' Stigma, then, affects the very identity of those the negative attribute is ascribed to, and complicates interaction situations with . . . 'the normals.'" (citation omitted)).

themselves.[38] On the macro level, stigma and false conceptions surrounding the nature of mental illness impede progress toward meaningful solutions.[39]

Stigma also contributes to the problems of cyclical incarceration, as people associate mental illness with deviance and criminality.[40] Just as in the period immediately following deinstitutionalization, many mentally ill Americans wind up imprisoned.[41] Very often, prisons lack

---

38. L.H. Andrade et al., *Barriers to Mental Health Treatment: Results from the WHO World Mental Health Surveys*, 44 PSYCHOL. MED. 1303, 1312 (2014); *see also* Corrigan, *supra* note 36, at 616 ("[P]ublic identification as 'mentally ill' can lead to significant harm . . . . [P]eople with concealable stigmas . . . may opt to avoid the stigma all together [sic] by denying their group status and by not seeking the institutions that mark them (i.e., mental health care). [Through] [t]his kind of label avoidance . . . stigma impedes care seeking." (citations omitted)).

39. Professor Corrigan explains the concept of "structural stigma":

> Stigma as a social-cognitive construct is only one of several stigma-related factors that undermine obtaining mental health care when in need. . . . [O]ther interpersonal, economic, and policy factors . . . also mitigate service use. One manifestation of these factors is structural stigma; namely, economic and political pressures on the culture, rather than psychological influences on the individual, that yield discrimination and undermine care access. . . . [T]he products of these forces are social and institutional structures that rob people of opportunities.

Corrigan, *supra* note 36, at 620 (citations omitted). One pattern of "intended structural stigma as applied to African Americans" was the Jim Crow laws. *Id.* at 621. For the mentally ill, "[t]hreats to confidentiality may also be an example of intended structural discrimination, especially relevant to care seeking." *Id.* In addition, political opponents of mental health parity may perpetuate "unintended structural stigma." *Id.* Such politicians and lobbyists do not "blame [the mentally ill] for their illness," but "they cite financial concerns that are frequently at the root of structural discrimination." *Id.* This "inability to shake business concerns despite evidence to the contrary is an example of the ongoing influence of structural stigma." *Id.*; *see also* Chorney, *supra* note 18, at 220 ("Mental health continues to be socially misunderstood and this misunderstanding continually leads to failed policies.").

40. *See* Nicolas Rüsch, Matthias C. Angermeyer & Patrick W. Corrigan, *Mental Illness Stigma: Concepts, Consequences, and Initiatives to Reduce Stigma*, 20 EUR. PSYCHIATRY 529, 531 (2005) ("In the case of mental illness, angry prejudice may lead to withholding help or replacing health care with the criminal justice system. . . . This association between perceived dangerousness of persons with mental illness, fear, and increased social distance has been validated for different countries, including Germany, Russia and the United States."); Corrigan, *supra* note 36, at 616 ("Criminalizing mental illness occurs when police, rather than the mental health system, respond to mental health crises . . . . Persons exhibiting symptoms and signs of serious mental illness are more likely than others to be arrested by the police." (citations omitted)); Stephanie Hartwell, *Triple Stigma: Persons with Mental Illness and Substance Abuse Problems in the Criminal Justice System*, 15 CRIM. JUST. POL'Y REV. 84, 85 (2004) ("Simply put, suspect populations are groups of individuals who are stigmatized. Thus, they include drug addicts, drug dealers, and the mentally ill. They are stigmatized so their actions and behaviors are non-normative, and public tolerance and policy dictates efforts to contain and manage them.").

41. Chorney, *supra* note 18, at 218; s*ee also* Alexandra Gates, Samantha Artiga & Robin Rudowitz, *Health Coverage and Care for the Adult Criminal Justice-Involved Population*, KAISER FAM. FOUND. 3 (2014), https://kaiserfamilyfoundation.files.wordpress.com/2014/09/8622-health-coverage-and-care-for-the-adult-criminal-justice-involved-population1.pdf

the resources needed to provide adequate treatment for these mentally ill offenders,[42] continuing the vicious cycle in which institutional deficiencies in mental health treatment exacerbate institutional failings of the criminal justice system and vice versa.[43]

The stigmatic association between mental illness and criminality is compounded for homeless mentally ill Americans.[44] The homeless population suffers greater rates of mental illness.[45] The stress of homelessness, in turn, exacerbates the problem of mental illness.[46] And, of course, homeless people suffering from mental illness struggle to afford treatment for their conditions.[47] Further still, due to their public exposure and the stigma of mental illness, homeless people who suffer from mental illness are more likely to "perpetrate criminal acts that are manifestations of their illness" and thus be arrested.[48] Homeless people released from jails and prisons are also more likely to reoffend,[49] and homelessness also carries its own stigma and is itself functionally criminalized. Homelessness thus furthers the vicious cycle of incarceration for the mentally ill, adding a layer of complexity to solutions that attempt to address the stigma-related problems in mental health today.

Additionally, cost-related issues prevent many patients from receiving care.[50] Even those who can afford to seek and receive some level of treatment often cannot afford to continue treatment or pay for

---

[https://perma.cc/37EK-NBR8] ("Over half of prison and jail inmates have a mental health disorder, with local jail inmates experiencing the highest rate (64%).").

42. *See* Curtin, *supra* note 2, at 488 (noting that "[p]rison health care is significantly below the quality of health care in normal society" (quoting Michael Taylor, *California Grapples with Aging Prison Population*, S.F. CHRON., Aug. 2, 1993, at A1) (alteration in original)).

43. Behbahani et al., *supra* note 18, at 167–68; *see* Risdon N. Slate & Laura Usher, *Health Coverage for People in the Justice System: The Potential Impact of Obamacare*, 78 FED. PROB. 19, 20 (2014) ("For people with serious mental illness and other chronic health conditions, interacting with police is often the first step in a long cycle of involvement with the justice system."). In jails particularly, high population turnover rates and a general dearth of reentry planning programs further frustrate inmates' ability to receive mental health treatment. *Id.*

44. One recent national study indicated that in the year prior to their arrest, 15.3 percent of incarcerated adults were homeless. Greg A. Greenberg & Robert A. Rosenheck, *Jail Incarceration, Homelessness, and Mental Health: A National Study*, 59 PSYCHIATRIC SERVS. 170, 170 (2008).

45. *Id.* Homeless people are also more likely to have substance abuse problems and to suffer trauma from past sexual and physical abuse. *Id.* at 173.

46. *Id.* at 170.

47. *Id.*

48. *Id.*

49. *Id.*

50. Chorney, *supra* note 18, at 221.

medication.[51] Budget cuts stemming from the economic recession have compounded these cost issues in recent years, as cuts to Medicaid increase out-of-pocket costs for individuals who qualify for disability benefits due to serious mental disabilities such as schizophrenia and bipolar disorder.[52]

Access-related issues also continue to loom large, adding to the problems stemming from stigma and cost. There remains a dearth of community resources through which patients can access the mental health services that they need.[53] Relatedly, there are major access issues associated with the uneven geographic distribution of available community resources—mental health resources are concentrated in urban areas, exacerbating access issues for mental health patients in rural communities.[54] Many mental health patients seek care only from primary care providers because there are fewer specialists available in their communities.[55] Between such stigma, cost, and access issues, over 40 percent of Americans with mental illness receive no treatment at all.[56]

C. Enter Telemental Health

1. *Introduction and Growth.* Telemental health promises major strides in mental health treatment, and its use is currently proliferating.[57] In its broadest form, telemental health involves the provision of mental health services via telecommunication technology.[58] The two major subcategories of telemental health

51. *See* Ramin Motjabai, *Trends in Contacts with Mental Health Professionals and Cost Barriers to Mental Health Care Among Adults With Significant Psychological Distress in the United States: 1997–2002*, 95 AM. J. PUB. HEALTH 2009, 2013 (2005) (noting increased likelihood for lower income mentally ill individuals "to report forgoing mental health care because of cost" and that such individuals were "almost twice as likely to forego medications").

52. Chorney, *supra* note 18, at 221.

53. *Id.* at 220.

54. *See* Avery Schumacher, *Telehealth: Current Barriers, Potential Progress*, 76 OHIO ST. L.J. 409, 418 (2015) ("Currently, rural areas are experiencing a major shortage of primary care physicians and an even greater shortage of specialists. While 20% of Americans live in rural areas, only 9% of physicians practice in these areas.").

55. Behbahani et al., *supra* note 18, at 166.

56. Romney & Baird, *supra* note 14, at 32.

57. Erin Dietsche, *More and More Businesses Are Offering Telehealth Services as an Employee Benefit*, MEDCITY NEWS (Aug. 9, 2017, 5:44 PM), http://medcitynews.com/2017/08/telehealth-employees/?rf=1 [https://perma.cc/HVX5-P5QW].

58. Bill Marino, Roshen Prasad & Amar Gupta, *A Case for Federal Regulation of Telemedicine in the Wake of the Affordable Care Act*, 16 COLUM. SCI. & TECH. L. REV. 274, 275 (2015).

explored in this Note are telepsychology and telepsychiatry, which use videoconferencing software to connect patients and providers remotely.[59] This Note additionally explores mobile health technology, which enables users to self-monitor their mental health conditions and report information to their providers.

For about a quarter of a century, telemental health has bridged access and cost issues for incarcerated mentally ill patients,[60] and its use is now beginning to grow in the general population.[61] This growth is happening very rapidly. One study estimates that 80 to 90 percent of mental health treatment could be conducted remotely within a decade.[62] Telemental health thus represents the future of mental health treatment—a future that is fast approaching.

Insurers and employers are contributing to this growth spurt. Many major insurance companies are beginning to provide coverage for telehealth and telemental health services,[63] and other large companies are following suit. In 2012, only 7 percent of large companies offered coverage.[64] In 2018, 96 percent of large companies will be offering telehealth coverage as an employee benefit.[65] And in 2018, 56 percent of large companies will be offering telehealth coverage for behavioral health services—an increase of over twofold from 2017.[66] Smaller companies are tagging along as well, with 24 percent of all U.S. employers now offering general telehealth coverage and 42 percent expected to do so by 2018.[67] Moreover, 33 percent of large

59. *See* Little, *supra* note 1, at 867 (explaining how telemedicine connects patients and providers).

60. Brendan R. McDonald, Robert D. Morgan & Patrick S. Metze, *The Attorney-Client Working Relationship: A Comparison of In-Person Versus Videoconferencing Modalities*, 22 PSYCHOL. PUB. POL'Y & L. 200, 201 (2016); *see also* Schumacher, *supra* note 54, at 419 (citing a study showing that telepsychiatry reduces rates of violence in prisons).

61. Romney & Baird, *supra* note 14, at 32.

62. *Id.*

63. Alex Ruoff, *Most Major U.S. Companies Will Offer Telehealth Benefits, Hoping To Please Workers*, BLOOMBERG BNA: HEALTH CARE BLOG (Aug. 10, 2016), https://www.bna.com/major-us-companies-b73014446157 [https://perma.cc/T7HE-MQM5].

64. *Id.*

65. Bill Siwicki, *Almost All Large Employers Plan To Offer Telehealth in 2018, but Will Employees Use It?*, HEALTHCARE IT NEWS (Sept. 18, 2017, 3:33 PM), http://www.healthcareitnews.com/news/almost-all-large-employers-plan-offer-telehealth-2018-will-employees-use-it [https://perma.cc/7BNX-28ZB].

66. *Id.* These numbers underscore the immediate import of a sound legal approach to the unique legal issues posed by telehealth.

67. Genevieve Douglas, *Employers Exploring New Health-Care Options*, BLOOMBERG BNA (Aug. 22, 2016), https://www.bna.com/employers-exploring-new-n73014446679 [https://perma.cc/JVW7-HDS8].

employers now provide their employees telehealth coverage by contracting directly with telehealth vendors even though their insurers do not provide coverage.[68] Extending coverage will lift one of the main impediments to increased telehealth consumption by making it more affordable for patients.[69]

2. *Advantages*. Telemental health promises myriad advantages that work against stigma, cost, and access issues. Given the stigma of mental illness, remote access is particularly helpful for mental health treatment, allowing patients to seek care with greater assurance of anonymity.[70] Telemental health also reduces costs in several ways, including cutting transaction and transportation costs through streamlined healthcare delivery that connects patients and providers remotely.[71] Telehealth generally also saves costs down the road by incentivizing and facilitating preventative care.[72] Research already illustrates the clinical efficacy of telemental health,[73] even pointing to better outcomes from telemental health than conventional health

68. Ruoff, *supra* note 63.

69. *See* Behbahani et al., *supra* note 18, at 155 (explaining that patients experience unaffordability due to lack of coverage as particularly limiting in the mental health context); Fried et al., *supra* note 6, at 89 (noting a general trend by insurers toward placing telehealth coverage on par with coverage for conventional treatment); Little, *supra* note 1, at 872 (citing potential affordability problems stemming from lack of insurance coverage as one of telepsychiatry and telemedicine's main limitations).

70. Choi, *supra* note 2, at 340; Little, *supra* note 1, at 871.

71. Little, *supra* note 1, at 871. In addition, rising costs increasingly prevent Americans from accessing affordable health care. *See, e.g.*, Schumacher, *supra* note 54, at 414–15 (explaining that healthcare spending comprises an increasingly large portion of the U.S. gross domestic product, well outpacing that of other industrialized countries, and yet does not translate to better outcomes).

72. Douglas, *supra* note 67. Employers are expected to save an average of anywhere between $100 and $700 per patient per visit by providing employees telehealth coverage. *See* Jamie Gooch, *Telemedicine Is Poised for Growth*, MANAGED HEALTHCARE EXECUTIVE (Dec. 8, 2014), http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/telemedicine-poised-growth?page=full [https://perma.cc/Y8P7-GALA] ("Cost saving estimates vary . . . [reaching] as much as $700 per consultation. Schoenberg says savings depend on the population and geography, but approximates an urgent care center visit at $150, and an emergency room encounter at $500. By contrast, . . . a telehealth visit costs around $50, including all the technology needed."). *But see generally* J. Scott Ashwood, Ateev Mehrotra, David Cowling & Lori Uscher-Pines, *Direct-To-Consumer Telehealth May Increase Access to Care but Does Not Decrease Spending*, 36 HEALTH AFF. 485 (2017) (suggesting that increased access through teleconferencing-based telehealth platforms may result in increased spending).

73. Little, *supra* note 1, at 871.

treatment—attributable in part to increased access to preventative care and continuity of care.[74]

Telemental health is a particularly effective avenue to bridge access issues, allowing patients to reach mental health professionals electronically where they could not otherwise reach them physically.[75] This is particularly true in rural communities.[76] This makes telehealth particularly advantageous in the context of mental health treatment where access issues are particularly salient.[77] Telemental health can connect patients with providers, and it can also connect providers with other providers. Connecting providers with other providers can improve treatment outcomes on the micro level by allowing providers to obtain remote assistance for individual patients;[78] on the macro level by providing increased education, information, and interconnectedness between doctors.[79] With increased access between providers, telemental health can also reduce unnecessary involuntary commitments by enabling local generalists to connect remotely to a psychiatrist who can determine whether involuntary commitment is necessary.[80] But for all of its strengths, telemental health has yet to overcome a glaring obstacle standing in the way of its full potential—patient privacy.

3. *Privacy Problems Make for a Poison Pill.* In general, privacy and security concerns in health care have become quite extensive, and telemental health solutions that are packaged with new security risks

74. *E.g.*, *id.* Indeed, the American Medical Association (AMA) has not only endorsed the clinical efficacy of telehealth and telemental health treatment but has placed it on par with traditional methods of care, recommending that the same standard of care applicable to doctors in a traditional setting apply in telehealth contexts. Press Release, Am. Med. Ass'n, AMA Adopts New Guidance for Ethical Practice in Telemedicine (June 13, 2016), https://www.ama-assn.org/ama-adopts-new-guidance-ethical-practice-telemedicine [https://perma.cc/9NBG-NC36]. The American Psychiatric Association (APA) has also specifically endorsed telepsychiatry as "a validated and effective practice of medicine that increases access to care." *Telepsychiatry*, AM. PSYCHIATRIC ASS'N, https://www.psychiatry.org/psychiatrists/practice/telepsychiatry [https://perma.cc/EF23-AWQ7]. The APA also points to "a robust evidence base that shows telepsychiatry leading to improved outcomes and higher patient satisfaction ratings." *Id.*

75. Saeed et al., *supra* note 2, at 219–20.

76. *Id.* In addition, this can alleviate access problems stemming from demographic dispersion. *See, e.g.*, Schumacher, *supra* note 54, at 418 ("While 20% of Americans live in rural areas, only 9% of physicians practice in these areas.").

77. Little, *supra* note 1, at 871.

78. Saeed et al., *supra* note 2, at 220.

79. *See id.* (discussing the benefits of "[t]elehealth-facilitated training" and "reduced professional isolation" for mental health professionals).

80. Little, *supra* note 1, at 871.

make them much less attractive to patients.[81] Medical records are increasingly exposed through data breaches.[82] From 2011 to 2016, cyber attacks against healthcare providers increased over twofold.[83] Financial incentives are increasingly driving hackers to target healthcare providers, when in the past hackers mainly targeted the retail and financial sectors.[84] By some estimates, medical information is about ten times more valuable than a credit card number on the black market, largely because the information is just as useful in fraudulent payment schemes and its theft can take much longer to detect.[85]

In telehealth treatment, these concerns are amplified by the increased use of telecommunications technology. First, the volume of health-sensitive electronic transmissions increases significantly through telepsychology and telepsychiatry.[86] Mobile health

---

81. *See* Teresa Piliouras et al., *Impacts of Legislation on Electronic Health Records Systems and Security Implementation*, IEEE LONG ISLAND SYS., APPLICATIONS & TECH. CONF. 7 (2012) ("Healthcare systems require an especially high degree of information security.").

82. Beth Walsh, *Top Legal Issues in Healthcare Include Cybersecurity, HIPAA, Telemedicine*, CLINICAL INNOVATION + TECH. (Feb. 10, 2016), http://www.clinical-innovation.com/topics/ehr-emr/top-legal-issues-healthcare-include-cybersecurity-hipaa-telemedicine [https://perma.cc/67ZV-R952].

83. Bill Yager, *Three Health IT Trends to Watch in 2016: Cybersecurity, Telemedicine and Partnerships*, HEALTHCARE INFORMATICS (Mar. 18, 2016), https://www.healthcare-informatics.com/article/three-health-it-trends-watch-2016-cybersecurity-telemedicine-and-partnerships [https://perma.cc/EB93-RPCN].

84. *Id.*

85. As one article notes,

> The data for sale includes names, birth dates, policy numbers, diagnosis codes and billing information. Fraudsters use this data to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers, according to experts who have investigated cyber attacks on healthcare organizations. Medical identity theft is often not immediately identified by a patient or their provider, giving criminals years to milk such credentials. That makes medical data more valuable than credit cards, which tend to be quickly canceled by banks once fraud is detected. Stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number . . . .

Caroline Humer & Jim Finkle, *Your Medical Record Is Worth More to Hackers than Your Credit Card*, REUTERS (Sept. 24, 2014), http://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 [https://perma.cc/NEC8-Y3TC].

86. *See* Joseph L. Hall & Deven McGraw, *For Telehealth To Succeed, Privacy and Security Risks Must Be Identified and Addressed*, 33 HEALTH AFF. 216, 217 (2014) (noting that the "relevant threats" for a telehealth system "include breach of confidentiality during collection of sensitive data or during transmission to the provider's system; unauthorized access to the functionality of supporting devices as well as to data stored on them; and untested distribution of software and hardware to the patient"). Further, communications between patients and providers often implicate interoperability—"the need to have different systems work together"—such that "telehealth systems may have to accommodate varying versions of critical programs running

applications can also involve extensive data transmissions between patients and providers and leave data stored on patient mobile devices and third-party servers.[87] Patient use creates additional risks, heightening the need for providers to secure their storage and transmissions as much as possible.[88] Because telemental and mobile health treatment amplify privacy and security concerns, the existing legal framework may not be adequate to protect patient and consumer interests.

II. CURRENT LEGAL ENVIRONMENT

This Part examines the law governing patient privacy in health care. It begins with an overview of the first wave of patient privacy legislation and proceeds with a discussion of HIPAA, the seminal piece of legislation in this sphere, along with its amendments and constituent regulations. It concludes by explaining HIPAA's preemptive effect on state laws.

A. Privacy Legislation Pre-HIPAA

In the decades prior to HIPAA, the healthcare industry lacked any generally accepted or legally mandated privacy and security standards.[89] In 1966, the Freedom of Information Act (FOIA) became the first piece of federal legislation to address patient privacy at all, and that fact was incidental to the legislation's primary purpose.[90] The thrust of FOIA was to provide individuals the right to request information regarding the activities of federal agencies, but FOIA carved out an exception to this right for personal medical information relevant to resolving administrative adjudications.[91]

---

across a host of operating systems." Robert A. Heverly, *Telemedicine, Telehealth, and Cybersecurity*, 20 N.Y. ST. BAR. ASSOC. HEALTH L.J. 35, 35 (2015).

87. *See* Frazee et al., *supra* note 9, at 397 (noting that "the bulk of [mobile health] user data is stored on servers."); Hall & McGraw, *supra* note 86, at 218 ("[M]edical and consumer devices typically used by patients for telehealth applications can themselves pose serious risks, as the devices contain numerous security flaws and are constantly under attack from threats such as malware.").

88. Hall & McGraw, *supra* note 86, at 217.

89. Francis Akowuah, Xiaohong Yuan, Jinsheng Xu & Hong Wang, *A Survey of U.S. Laws for Health Information Security & Privacy*, 6 INT'L J. INFO. SEC'Y & PRIVACY 40, 42 (2012).

90. Freedom of Information Act, Pub. L. 89-487, 80 Stat. 250 (1966).

91. *Id.* Thus, this legislation conferred no special privacy protection to health data beyond excluding their content from the newly created window of exposure. *Id.*

In 1974, the Privacy Act became the first law enacted for the express purpose of protecting patient confidentiality.[92] The Privacy Act also granted patients the right to access their medical records and the right to make changes to them.[93]

B. HIPAA

HIPAA finally set the stage for meaningful reform with respect to patient privacy. While enacted primarily to make health care more efficient and affordable,[94] HIPAA also contained provisions that aimed to protect and secure health information.[95] For example, the HIPAA administrative simplification provision standardized the use of electronic health information[96] and mandated the development of privacy and security standards for handling patient health information.[97] Pursuant to HIPAA, the Department of Health and Human Services (HHS) promulgated two comprehensive regulations—designated as the Privacy Rule and the Security Rule for the purposes of this analysis.[98]

Congress and the HHS have amended HIPAA, attempting to respond to the ever-changing technological landscape.[99] In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH) to strengthen HIPAA's Privacy and Security Rules.[100] HITECH was also intended to promote

---

92. 5 U.S.C. § 552(a) (2018).

93. *See id.* (balancing interest in patient privacy with free flow of information). The Privacy Act also required healthcare facilities to document any disclosures of health information. *Id.*

94. As stated in the Act, Congress intended for HIPPA

> to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936, 1936.

95. *See generally id.* §§ 261–264, 110 stat. at 2021–34 (concerning health information privacy and security).

96. *Id.* § 262, 110 stat. at 2021.

97. *Id.* § 264, 110 stat. at 2033.

98. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000).

99. *See* Piliouras et al., *supra* note 81, at 1 ("Privacy legislation is in a state of constant evolution as new technologies, privacy threats, and societal demands come into prominence.").

100. *See* Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, tit XIII, 123 Stat. 226 (2009) (enacted as part of the American Recovery and Investment Act of 2009, Pub. L. 111–5, 123 Stat. 115). The descriptions of the Rules, *supra*, are current post-

widespread use of electronic health records (EHRs) by 2014, so it created incentives for providers to increase the rate of EHR adoption.[101] In 2013, the HHS finalized the Omnibus Rule, making significant regulatory changes pursuant to HITECH.[102]

As it stands today, the Privacy Rule[103] regulates the use and disclosure of "protected health information" (PHI)[104] by "covered entities,"[105] which includes most healthcare providers, and their "business associates."[106] Providers can generally disclose PHI to other providers without patient consent for treatment purposes.[107] Mental and behavioral health records have no additional protection as compared with health information generally.[108] However, psychotherapy notes are excepted from the general rule of permissive disclosure for treatment purposes—their disclosure requires patient

HITECH. HITECH extended the Rules to covered entities' business associates, created new breach notification requirements, and incorporated disclosure requirements into the use of electronic health records (EHRs).

101. *Id.* §§ 13301, 13410, 123 Stat. at 246–58, 271–76.

102. *See* Press Release, US Dep't of Health & Human Servs., New Rule Protects Patient Privacy, Secures Health Information (Jan. 17, 2013), https://wayback.archive-it.org/3926/20150618191254/http://www.hhs.gov/news/press/2013pres/01/20130117b.html [https://perma.cc/2Q4X-FFGN] (describing regulatory changes pursuant to HITECH, including increased penalties for noncompliance, strengthening HITECH's breach notification requirements, granting patients the rights to access their EHRs in electronic form and to prevent treatment information from reaching insurer's hands when patients pay in cash, and prohibiting the unauthorized sale of protected health information (PHI)). The HHS also streamlined procedures for patients to consent to the use of their health information for research purposes in response to a 2007 report by the Institute of Medicine arguing that HIPAA had frustrated its own purposes in striking the balance between privacy and information flow by making such research too difficult. *See* Akowuah et al., *supra* note 89, at 44 ("Research findings indicate HIPAA has complicated healthcare process steps. It has also brought about increased documentation which defeats its initial intent of reducing administrative process. Critical researches have been hindered or discontinued as HIPAA has restricted the flow of needed information." (citations omitted)).

103. 45 C.F.R. §§ 164.500–164.534 (2017).

104. PHI refers to "individually identifiable health information . . . that is (i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium." *Id.* § 160.103; *see also id.* (defining "[i]ndividually identifiable health information" as "a subset of health information"); *id.* § 164.514(a) (excluding "de-identifi[ed]" data from the definition of PHI). Typical examples of PHI include medical and billing records. *Id.* § 160.103.

105. Covered entities include providers, hospitals, insurers, and healthcare clearinghouses. *Id.* § 164.501.

106. Business associates include independent contractors of covered entities that receive and process PHI. *Id.*

107. *Id.* § 164.506(c); *see also id.* § 164.501 (defining "treatment").

108. *See, e.g.*, *id.* § 164.502(a) (referring generally to "protected health information").

authorization.[109] The Privacy Rule seeks to balance respect for patient privacy with the therapeutic advantages conferred by the free flow of information between providers.[110]

The Security Rule[111] complements the Privacy Rule. Applicable only to electronically processed PHI,[112] the Security Rule establishes standards for administrative,[113] physical,[114] and technical safeguards[115] to ensure that patient privacy is protected.[116] These standards operate flexibly in several important ways. Some of these standards have "implementation specifications," which lay out different aspects of the process to secure electronic records. For example, implementation specifications for the standard of "[f]acility access controls" include "[c]ontingency operations," a "[f]acility security plan," "[a]ccess

---

109. *Id.* § 164.508(a)(2). "Psychotherapy notes" are defined as:

> notes recorded (in any medium) by 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 that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: [d]iagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Id. § 164.501 (emphasis in original). The requirements for "authorization" are much stricter than for consent. *See id.* § 164.508(b) (distinguishing "[v]alid" and "[d]efective" authorizations and generally prohibiting both "[c]ompound" and "condition[ed]" authorizations).

110. Akowuah et al., *supra* note 89, at 42–43. This is embodied in and exemplified by the minimum necessity principle that governs certain disclosures of PHI. *See* 45 C.F.R. § 164.514(d) (delineating varying "minimum necessary requirements" depending on type, target, and frequency of disclosure that restrict the amount of information that can be disclosed). Thus, the Privacy Rule also affords patients the right to access, *id.* § 164.524, and amend their PHI, *id.* § 164.526. *But see* Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM. J.L. & MED. 416, 436 (2014) ("HIPAA tends to err towards safeguarding patients' privacy . . . .").

111. 45 C.F.R. §§ 164.302–164.318.

112. *Id.* § 164.302.

113. *Id.* § 164.308. "Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." *Id.* § 164.304.

114. *Id.* § 164.310. "Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." *Id.* § 164.304.

115. *Id.* § 164.312. "Technical safeguards means [sic] the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." *Id.* § 164.304.

116. *See id.* § 164.306(a)(1) ("Covered entities must . . . [e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.").

control and validation procedures," and "[m]aintenance records."[117] These implementation specifications are categorized as measures the entities must treat as either required or "addressable."[118] Covered entities must meet required specifications;[119] but where specifications are "addressable," covered entities may determine for themselves whether a particular implementation is contextually "reasonable and appropriate" to further the protection of PHI.[120] If so, the entity should implement the specification.[121] If not, the entity should document the reasons for its determination and "[i]mplement an equivalent alternative measure if reasonable and appropriate," affording covered entities an additional layer of discretion.[122] In addition, even where specifications are required, covered entities have flexibility with respect to the *means* they choose to achieve conformity.[123] Finally, some standards do not have any associated implementation specifications, affording entities even more flexibility in adopting security measures or not.[124]

C. Complexities of Telemental Health Compliance Under State Law

Federal law here exists in tandem with state law. HIPAA preempts state law whenever state law is less stringent with respect to protecting patient privacy.[125] State law can be formally inadequate, where compliance with state law is insufficient to comply with HIPAA, or functionally inadequate, where the federal purpose is frustrated.[126] There are a range of state laws and regulations governing patient privacy and security in the healthcare context that can come into play.

---

117. *Id.* § 164.310(a)(2).

118. *Id.* § 164.306(d)(1).

119. *Id.* § 164.306(d)(2).

120. *Id.* § 164.306(d)(3)(i).

121. *Id.* § 164.306(d)(3)(i)(A).

122. *Id.* § 164.306(d)(3)(ii)(B)(2) (emphasis added).

123. *Id.* § 164.306(b).

124. *See, e.g.*, *id.* § 164.312(b) ("Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.").

125. 45 C.F.R. § 160.203(b) (2017); *see also* 42 U.S.C. § 1320d-2(c)(2) (2018) ("A regulation promulgated under paragraph (1) shall not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.").

126. 42 U.S.C. § 1320d-2(c)(2); 45 C.F.R. § 160.203(b). State law that is more stringent, that is, state law that confers greater protections to patients than HIPAA, is not preempted, adding to the complexity of the legal interplay.

States have laws governing privacy and security in healthcare generally and also specifically relating to mental health care. Certain states also have specific rules governing privacy and security in the context of telehealth. Some states also have narrowly tailored rules specifically for telemental health.[127] Because HIPAA sets a preemptive floor, these state laws may therefore provide patients with more protection than they might otherwise have under current federal law.

III. DIAGNOSING INADEQUATE LEGAL PROTECTIONS

Part III analyzes how HIPAA applies to telemental and mobile health. First, it explains why HIPAA does not apply to transmission security in telepsychology and telepsychiatry sessions, but that transmission security *is* covered when mobile health applications asynchronously transmit information from patients to providers. Next it discusses how, for telemental health, the Security Rule is formally applicable to stored data but functionally inadequate—and for mobile health, it is inadequate both formally and functionally because the data is not stored by covered entities. Similar data storage security inadequacies exist for psychotherapy notes because HIPAA protections do not extend to archived psychotherapy sessions, despite the fact that the policy rationale for the former ought strongly to extend to the latter. This is because there is an inherent tradeoff between keeping patient health information confidential and allowing providers to access the information for treatment purposes—and with archived psychotherapy sessions, as with psychotherapy notes, the confidentiality consideration is particularly strong, and the access consideration particularly weak. This Part finishes by outlining and broadly categorizing state laws addressing privacy and security concerns in health care generally, as well as state laws that specifically address mental health care, telehealth, and telemental health.

A. Telemental Health Under HIPAA

Several aspects of telemental and mobile health implicate unique privacy and security concerns. In telepsychiatry and telepsychology sessions, all information disclosed in the course of treatment is

127. For examples of state laws governing privacy and security in general health care, mental health care, telehealth, and telemental health, see *infra* Part III.B.

channeled synchronously through electronic transmissions.[128] The same information is also transmitted in asynchronous communication through mobile and other web-based health platforms that allow patients to update their providers about their treatment or condition.[129] Mobile health applications also generate inferred data from user inputs, which can be transmitted to and stored by providers.[130] Not all mobile health data reaches providers; for example, mood-tracking applications allow users to report their mood at given times and track fluctuations themselves.[131] Finally, providers may choose to archive telepsychotherapy sessions for patients or other providers to access for treatment purposes or as evidence to protect themselves in medical malpractice actions.[132] Applying the HIPAA Rules to these innovative developments reveals the ways in which the Rules are both formally and functionally outdated.

1. *Synchronous Transmissions in Telepsychiatry and Telepsychology Sessions*. In its current form, the Security Rule does not apply to telemental health sessions conducted with videoconferencing software. Whereas the Privacy Rule protects all PHI,[133] the Security Rule only protects PHI that is "[t]ransmitted by . . . [or] [m]aintained in electronic media,"[134] or "e-PHI."[135]According to the HHS's website, "[e]-PHI does not include . . . video teleconferencing . . . because the information being exchanged did not exist in electronic form before the transmission."[136]

128. *See* Schumacher, *supra* note 54, at 416 ("Real time, or synchronous communication . . . is instantaneous, and includes the use of interactive telecommunications devices such as audio and video equipment.").

129. *See id.* ("Store-and-forward, or asynchronous communication, refers to services that transmit medical data, including clinical information and images, to a practitioner for later assessment . . . typically . . . for diagnosis and treatment decisions . . . [and] remote monitoring, . . . [which] can be useful in the management of chronic diseases.").

130. *See* Frazee et al., *supra* note 9, at 396–97 (referring to "information that is inferred from existing data through analytic models—for example, analyzing a user's dietary patterns to predict that this particular user will likely develop type 2 diabetes").

131. *Id.* at 393.

132. Jeremy Henley, *Healthy Privacy and Security Practices for Telemedicine*, IDEXPERTS (Mar. 23, 2016), https://www2.idexpertscorp.com/knowledge-center/single/healthy-privacy-and-security-practices-for-telemedicine [https://perma.cc/EV7C-4DJT].

133. 45 C.F.R. § 164.502(a) (2017).

134. *Id.* § 160.103.

135. *Id.* § 164.306(a)(1).

136. *Does the Security Rule Apply to Written and Oral Communications?*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/2010/does-the-security-rule-apply-to-written-and-oral-communications/index.html?language=es

Similar language and reasoning in the Security Rule's preamble limits its scope to exclude "video teleconferencing."[137] The preamble also cross-references the HHS's definition of "electronic media,"[138] which includes "[e]lectronic storage material" and "[t]ransmission media used to exchange information already in electronic storage media."[139] The HHS's most recent redefinition of "electronic media" suggests that while "digitally produced [or recorded]" audio content should now fall under the Security Rule's protections for purposes of asynchronous communication, discussed in greater detail below, live audio or video teleconferencing is still excluded.[140] The Security Rule will not apply to the synchronous transmissions that occur during telepsychiatry and telepsychology sessions because the data transmitted therein "did not exist in electronic form immediately before the transmission."[141]

[https://perma.cc/L5WE-ASDV]. The information exchanged through teleconferencing exists in electronic form only *as* it is being transmitted.

137. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334, 8,342 (Feb. 20, 2003) ("[B]ecause 'paper-to-paper' faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by this rule."). Some online telehealth vendors currently rely on this language from the preamble in claiming not to be subject to the Security Rule. *See, e.g.*, Jenny Peddicord, *Between Two Screens: Demystifying HIPAA Compliance for Telepractice*, HELLO FOUND. (Dec. 15, 2014), http://thehellofoundation.com/clinic/between-two-screens-demystifying-hipaa-compliance-for-telepractice-4 [https://perma.cc/AK8V-3NU3] (informing telehealth providers that their videoconferencing software need not comply with the HIPAA Security Rule).

138. Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8,342.

139. 45 C.F.R. § 160.103. Unlike in the preamble and on the HHS's website, there is no explicit exclusion of video teleconferencing from the definition of "electronic media" in the rule itself. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8,374 ("Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form immediately before the transmission.").

140. More specifically, the HHS

> proposed to change the word 'because' to 'if' in the . . . definition of 'electronic media.' The definition assumed that no transmissions made by voice via telephone existed in electronic form before transmission; the evolution of technology has made this assumption obsolete since some voice technology is *digitally produced* from an information system and transmitted by phone. . . . One commenter specifically supported the change in language from 'because' to 'if,' noting the distinction was important to provide protection for *digital* audio *recordings* containing protected health information.

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,566, 5,575 (Jan. 25, 2013) [hereinafter 2013 HHS Report] (emphasis added).

141. 45 C.F.R. § 160.103. *But see* Tatiana Melnik, *Can Doctor's [sic] Use Skype for Telemedicine? Not in Oklahoma*, 16 J. HEALTH CARE COMPLIANCE 55, 57 (2014) (discussing Oklahoma Board of Medical Licensure and Supervision's decision, applying state law subjecting

Even if the HIPAA Security Rule were *formally* modified to include audio and video teleconferencing, its protections would be *functionally* inadequate to secure the PHI transmitted during online treatment sessions. The implementation specifications about requirements for secure transmission of this information under the Security Rule are merely addressable.[142] This means that telemental health providers can avoid requirements to secure synchronous transmissions simply by documenting why doing so would not be "reasonable and appropriate."[143] Providers would thus have the more attractive option not to implement integrity controls[144] and not to encrypt transmitted data.[145] Encrypting these transmissions is vital in order to keep the information from unwanted eyes.[146] The lack of a firm

telehealth treatment to HIPAA's requirements, and deeming a particular videoconferencing software impermissible because, in addition to other deficiencies, it did not encrypt transmissions). Thus, Oklahoma interpreted the HIPAA Security Rule to require encryption. If anything, Oklahoma's misapplication of HIPAA further highlights the need for a unified federal approach.

142. 45 C.F.R. § 164.312(e)(2).

143. *Id.* § 164.306(d)(3)(ii)(B)(1). Despite the apparent unreasonableness of neglecting to take such basic precautions, governmental data suggest that health entities too often exploit the lax documentary requirements in place to shirk their responsibilities to their patients, and failure is not addressed by law enforcement until it is too late. One example of this failure is that

> [l]arge numbers of covered entities and business associates—including many sophisticated and well-heeled enterprises—clearly are not bothering to encrypt their laptops and other mobile devices. . . . [T]he plethora of reported breach incidents . . . suggests that covered entities and business associates are treating encryption and other addressable Security Rule implementation specifications as if they were optional. . . . OCR's statistics regarding unencrypted laptops and removable storage technology, along with descriptions of the underlying breaches, suggest that most covered entities do not have current risk-assessment documentation to justify overriding the addressable encryption specification.

Patricia A. Markus, *Data Breach Reporting After HITECH: Welcome to the Land of Oz* § 7:42, *in* HEALTH LAW HANDBOOK 266–67 (Alice G. Gosfield ed., 2012).

144. 45 C.F.R. § 164.312(e)(2)(i). "*Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner." *Id.* § 164.304 (emphasis in original).

145. *Id.* § 164.312(e)(2)(ii). "*Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *Id.* § 164.304 (emphasis in original).

146. Heverly, *supra* note 86, at 38; Diane Hoffmann & Virginia Rowthorn, *Legal Impediments to the Diffusion of Telemedicine*, 14 J. HEALTH CARE L. & POL'Y 1, 39 (2011); *see also* Hall & McGraw, *supra* note 86, at 217–18 ("Data encryption—where data are electronically 'locked' using complex mathematics and encryption 'keys'—can ensure that if an attacker gains access to the raw data, those data will be meaningless."); Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 LOY. U. CHI. L.J. 175, 218–20 (2014) (advocating for *required* encryption standards, arguing that encryption is cost-effective, and highlighting several examples of prominent health data breaches of stolen devices wherein the breached data were not encrypted).

requirement to encrypt e-PHI transmissions thus further weakens the Security Rule's protections for telemental health patients.

2. *Asynchronous Transmissions*. Online and mobile health applications also present ample opportunity for the asynchronous transmission of health information between patients and providers.[147] For example, mobile health applications let patients update their psychologists about how they are feeling or update their psychiatrists about medication compliance, side effects, or perceived efficacy. As discussed above, electronically transmitted information only counts as e-PHI if it "exist[ed] in electronic form immediately before the transmission."[148] Fortunately, this should not be a problem in the context of asynchronous electronic communication insofar as a patient must necessarily input any information into an electronic device prior to its transmission.[149] To the extent that providers are on the receiving end of e-PHI transmissions, the Security Rule thus formally governs data transmitted asynchronously. Still, the Rule suffers the exact same functional inadequacies as for synchronous transmissions.

In addition, some mobile health applications can transmit data directly from users' devices into their EHRs.[150] Direct transmission to EHRs requires "interoperability," which, as a practical matter, requires some level of industry standardization.[151] Ironically, by circumventing providers, the transmission of such data would fall outside the Security Rule's protections. Stricter standards here could thus carry a triple benefit of providing more security for patients, incentivizing greater use of mobile health applications that transmit data directly to EHRs, and reducing the well-documented EHR burden for providers, all while adhering to HITECH's objectives to standardize and maximize EHR usage. Moreover, the fix here is easy—the Security Rule would just need to be narrowly extended to apply to transmissions where data fall into EHRs on the back end.

---

147. *See*, *e.g.*, Daniel F. Schulke, *The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing*, 93 B.U. L. REV. 1699, 1711 (2013) (explaining that most private health information sent in this way is unencrypted).

148. 45 C.F.R. § 160.103.

149. The same would be true for inferred data generated based on inputted, and thus electronically stored, information. The only exception would be audio and video recordings through mobile health applications, which do not appear to be a prominent feature of such applications.

150. *See, e.g.*, Schulke, *supra* note 147, at 1712 (considering this to be "[o]ne of the more important functionalities of [mobile health] applications").

151. *Id.*

3. *Data Storage*. The Security Rule's formal applicability to stored data does not run into the same wrinkles as for transmitted data. If PHI is stored electronically, it is e-PHI, and the Security Rule applies.[152] This means that providers must secure any health data they receive from their patients through mobile health technology.[153] Functionally, however, the Security Rule's protections appear inadequate. As with transmission security, the implementation specifications requiring specific security measures for access control are addressable and easy to avoid by way of documentation.[154] Thus, the Security Rule does not require covered entities to encrypt stored e-PHI.[155] This is a gross oversight, as failing to encrypt stored data significantly increases the probability of a data breach.[156]

---

152. 45 C.F.R. § 164.302. However, one possible wrinkle here concerns the varied regulatory usage of "electronic storage media" and "electronic storage material":

> [The HHS] replace[d] the term "electronic storage media" with "electronic storage material" to conform the definition of "electronic media" to its current usage, as set forth [by] the National Institute for Standards and Technology . . . in recognition of the likelihood that the evolution of the development of new technology would make use of the term "electronic storage media" obsolete in that there may be "storage material" other than "media" that house electronic data.

2013 HHS Report, *supra* note 140, at 5,575. Thus, the first subset in the definition of "[e]lectronic media" now refers to "[e]lectronic storage material" instead of "[e]lectronic storage media." 45 C.F.R. § 160.103. However, other aspects of the definition of "electronic media" appear inconsistent with this terminological change. First, the second subset of "electronic media"—the one that deals with transmission rather than storage—refers to "[t]ransmission media used to exchange information already in electronic storage media." *Id.* The HHS thus removed the term "electronic storage media" in the storage context but not in the transmission context. This is confusing because the HHS's reason for the terminological change in the first subset of "electronic media" is that the term "electronic storage media" is "obsolete." 2013 HHS Report, *supra* note 140, at 5,575. It is unclear whether this difference is intentional or an oversight. Second, although the HHS suggested that the terminological change was intended to account for more technologically-advanced means of storage, the first subset of "electronic media" provides by way of example the same old-school technology as before. *See* 45 C.F.R. § 160.103 (referring to "devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card"). The definition thus provides no clarification with respect to what specific types of storage "material" the terminological change is meant to sweep in. Third, the definition of "electronic storage material" falls *under* the definition of "electronic media," *id.*, which runs directly counter to the HHS's reasoning that "material" would include certain things that "media" excludes. The HHS should thus clarify its intentions with respect to this terminology.

153. 45 C.F.R. § 164.306(a) ("Covered entities must . . . [e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.").

154. *Id.* § 164.312(a)(2)(iv).

155. *Id.*

156. For a discussion of the importance of encrypting stored data, see *supra* note 146 and accompanying text.

Even more troubling is the extent to which patient privacy is protected when providers are not in the picture. Data put into a mobile health application and not shared with a provider are not protected under HIPAA, regardless of whether PHI is shared in the process.[157] In other words, data stored by mobile health vendors or their business associates fall outside of HIPAA's scope. This means that mobile health application developers are free to do whatever they want with user reports of medication compliance, current moods, and any other behavioral health information.[158] Moreover, to the extent that passively generated and inferred data from patient inputs—which provide an additional window of exposure into patients' mental well-being—are not collected and shared with providers, those data are similarly devoid of HIPAA protections.[159] What is more, little else serves to restrict application administrators from freely using this data. Mobile health entities often sell sensitive health information to big data developers, which can result in users being bombarded with advertisements targeted to their mental health conditions.[160]

4. *Archived Telepsychology Sessions*. The HHS comments in recent revisions to the HIPAA Rules make clear that digitally archived content falls within the Security Rule's protections, though with all the aforementioned functional inadequacies.[161] With respect to the Privacy Rule, however, archived telepsychology sessions warrant closer examination given the special protection that HIPAA confers to psychotherapy notes.[162] Formally, the special protection for

157. *See* 45 C.F.R. § 164.302 (applying only to "covered entitit[ies]" and their "business associate[s]"); *see also id.* § 160.103 (defining "[c]overed entity" and "business associate"); *id.* § 160.103 (narrowly defining "health information," and thus "e-PHI" for purposes of the Security Rule, only to include information "created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse"). Insofar as a mobile health entity does not fall within this definition, any data stored by the entity, or a third party with whom the entity contracts for data storage purposes, are outside the scope of "e-PHI," rendering the Security Rule inapplicable.

158. *See* Flaherty, *supra* note 110, at 426.

159. 45 C.F.R. § 164.306. In contrast, when such data are shared with providers, such transmission falls within the Security Rule.

160. *See, e.g.*, Hall & McGraw, *supra* note 86, at 217 ("A mobile health app may be financed by sharing potentially sensitive data from the app with third-party advertisers that target ads to patients based on app use."). This would be impermissible if mobile health suppliers had to comply with HIPAA, which prohibits the "[s]ale of protected health information." 45 C.F.R. § 164.508(a)(4)(i).

161. For arguments that permissive encryption requirements leave stored data functionally unprotected, see *supra* Part III.A.3.

162. 45 C.F.R. § 164.508(a)(2).

psychotherapy notes does not extend to archived sessions because the definition of "psychotherapy notes" only covers "notes recorded . . . by a health care provider."[163] Quite simply, recorded sessions do not fit this definition.

A functional examination of the special rule for psychotherapy notes arguably justifies some sort of special treatment for archived psychotherapy sessions. The extra protection for psychotherapy notes is justified on two grounds. First, the information contained within is particularly sensitive, warranting extra privacy protection.[164] This same rationale certainly extends to the information contained within the session itself. Moreover, a patient's personal disclosures, which can contain objective and highly sensitive statements of fact, may be inherently more revelatory than the provider's subjective impressions about the patient based upon those disclosures. If anything, then, a patient's privacy interest in safeguarding archived sessions is stronger than it is for psychotherapy notes.

The second justification for conferring special protection to psychotherapy notes is that the information contained within is less useful to other providers because it reflects the personal notes and observations of the treatment provider.[165] This accessibility interest is thus considered weaker for information more subjective than PHI. In other words, in striking a balance between securing the privacy of health information and making such information available and accessible to providers, the HHS found it prudent to provide extra privacy protections for psychotherapy notes because the information contained within is not particularly useful for other providers.

For other providers, the informative value of recorded sessions is different than that of psychotherapy notes. Other providers could form their own subjective impressions of patients from watching recorded sessions more so than with psychotherapy notes. But other providers could presumably also elicit the same objective information from that patient more efficiently in sessions of their own. In contrast, without access to the original therapist's notes, another provider would be unable to obtain the subjective impressions of other therapists about their patients. In this respect, recorded sessions would be less informative for other providers.

---

163. *Id.* § 164.501.

164. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,623 (Dec. 28, 2000).

165. *Id.*

There are thus two possibilities here. If recorded sessions are seen as less valuable to providers than psychotherapy notes, and the accessibility interest is weaker, then both the privacy and accessibility interests justify keeping this information at least as private as psychotherapy notes. If recorded sessions are seen as more valuable to providers than psychotherapy notes, then the needle moves in both directions: both the privacy *and* accessibility concerns are stronger. While it is possible, in the abstract, that the proper balance would be struck already without extra protection, the underlying functional considerations on the privacy side would at least warrant a deeper examination into the question of whether archived sessions ought to receive special protection.

B. Complexities of Telemental Health Compliance Under State Law

Privacy and security laws and regulations that apply to telemental health vary widely state by state. One important set of laws are those governing medical privacy generally. Some states have privacy regimes intended to be comprehensive like HIPAA.[166] The detail and specificity of these laws increases the likelihood that HIPAA preempts them. Each state also has some sort of statute governing the treatment of mental health records.[167] Some states have laws that apply only to hospitalized or institutionalized mental health patients,[168] many have laws for those who are involuntarily committed,[169] several states have laws applicable only to mental health providers like psychologists or social workers,[170] and many have some sort of generally applicable mental health privacy statute.[171] State privacy laws applicable

166. *See, e.g.*, CAL. CIV. CODE D. 1, pt. 2.6 (2007); MONT. CODE § 50-16-529 (2009); N.Y. PUB. HEALTH § 18(6) (2017); VA. CODE § 32.1-127.1:03(D) (2015); WASH. REV. CODE § 70.02.050(1)(a) (2012).

167. 1 Am. Health Lawyers Ass'n, HEALTH LAW PRACTICE GUIDE § 17:30 (2017); *see id.* at app. 17:3 (providing an exhaustive list of state laws concerning the privacy of mental health records).

168. *E.g.*, IDAHO CODE § 9-340C(8) & (13) (2016); N.Y. MENTAL HYG. 33.13 (2017); N.C. GEN. STAT. § 122C-55 (2014).

169. *E.g.*, IDAHO CODE § 66-348 (2017); NEB. REV. STAT. § 71-961 (2007); TEN. CODE ANN. § 33-6-601 (2016); WASH. REV. CODE § 71.05.360 (2016).

170. *E.g.*, COLO. REV. STAT. § 12-43-218 (2016); MASS. GEN. LAWS ch. 112 § 129A (2017); MO. REV. STAT. § 337.636 (2016); NEB. REV. STAT. § 38-2136 (2007); N.M. STAT. ANN. § 61-9A27 (2016); UTAH CODE ANN. 58-61-602(2)(c) (2011).

171. *E.g.*, ALA. CODE §§ 22-56-4(b)(6) (2017), 22-56-10 (1995); LA. STAT. ANN. § 28.171(A) (2017).

specifically to mental health patients are usually more stringent than HIPAA and therefore not preempted.[172]

State telemedicine laws complicate things further, as many states have separate laws governing privacy and security in the telehealth context. For patient privacy, many states have laws mandating confidentiality for telehealth patients generally.[173] New York protects the confidentiality of mentally disabled patients treated via telepsychiatry,[174] while South Carolina's protections kick in only for "licensee[s] who establish[] a physician-patient relationship solely via telemedicine."[175] With respect to security, Delaware requires identity verification for telebehavioral health practitioners,[176] and Texas has enacted broad technology and security standards that are more stringent than HIPAA.[177] Oklahoma simply requires telehealth providers to comply with HIPAA.[178]

In parallel, state laws that govern information sharing vary widely. Unlike HIPAA, many states allow information sharing for treatment purposes without patient consent only in limited circumstances, such as within a given hospital department,[179] among providers jointly participating in coordinated care programs,[180] or among state treatment

172. *See* LISA J. ACEVEDO & JENNIFER L. RATHBURN, MEDICAL PRIVACY ENFORCEMENT AND PENALTIES: HIPAA GETS TEETH 8 (2011) ("The state laws governing more sensitive types of health information . . . are almost always more stringent than HIPAA.").

173. *E.g.*, ARIZ. REV. STAT. ANN. § 36-3602 (2005); ARK. CODE ANN. § 17-80-404(e) (2017); CAL. BUS. & PROF. CODE § 2290.5(b), (f) (2016); IDAHO ADMIN. CODE r. 22.01.15.012–22.01.15.015 (2017); KY. REV. STAT. ANN. § 310.200(1) (2000); MD. CODE REGS. 10.32.05.05, 06 (2017); 30-026 MISS. CODE R. § 2635:5.3–5.6 (LexisNexis 2017); NEB. REV. STAT. § 71-8505 (1999); N.M. STAT. ANN. § 24-25-4 (2004).

174. N.Y. COMP. CODES R. & REGS. tit. 14, §§ 596.5–596.6 (2016).

175. S.C. CODE ANN. § 40-47-37(C) (2016).

176. DEL. CODE ANN. tit. 24, § 1769D (2017).

177. 22 TEX. ADMIN. CODE §§ 174.2–174.12 (2017); TEX. OCC. CODE ANN. §§ 111.002–03 (2005).

178. OKLA. ADMIN. CODE § 435:10-7-13 (2017). However, for why this congruence is not so simple after all, see *supra* note 141, which explains how an Oklahoma agency misapplied HIPAA in a telehealth case.

179. *See* OHIO REV. CODE ANN. § 5122.31(A)(6) (2017) (allowing "hospitals and other institutions and facilities within the department of mental health and addiction services [to] exchange psychiatric records and other pertinent information with other hospitals, institutions, and facilities of the department" without patient authorization).

180. *See* D.C. CODE § 7-1203.01 (2015) (allowing unauthorized disclosure of mental health information for treatment purposes within an "individual mental health facility" but requiring patient authorization for disclosure "to another health care provider").

programs.[181] Other states follow HIPAA's lead in allowing disclosure for treatment purposes without consent but diverge from HIPAA in limiting the amount of information that can be disclosed.[182] HIPAA would not preempt these laws because they more stringently protect patient privacy. But these laws upset the balance that HIPAA strikes between privacy and information sharing.

IV. PRESCRIPTIONS

Part IV suggests federal changes that could improve patient privacy for telemental and mobile health and explores a number of ways in which the HIPAA Rules can be made more stringent. For example, the HHS should extend the Security Rule to cover transmissions during telemental health sessions and require encryptions in all relevant contexts. Further, mobile health entities should be subject to the HIPAA Rules, and the HHS should provide special protection for archived psychotherapy sessions just as for psychotherapy notes. This Part then argues that Congress or the HHS should preempt the field with such changes, at least in the spheres of telemental and mobile health. With such sensitive information at stake, floor preemption is inappropriate and a state-by-state regime is impractical because patients increasingly seek treatment in different states—making national solutions the best contenders. The inherent balance underlying the formulation of the Rules further justifies field preemption. Simple "floor" preemption does not mesh with the fact that the Rules embody legislative and regulatory choices made to strike a balance in the face of competing policy considerations.

A. Strengthening the Federal Regime

The analysis in Part II identifies a number of gaps within the HIPAA Rules in the context of telemental health. Congress or the HHS should strengthen the Security Rule, extend the Privacy and Security Rules to cover mobile health applications, and except recorded psychotherapy sessions from the Privacy Rule in the same mold as currently for psychotherapy notes. The Security Rule's

181. *See* DEL. CODE ANN. tit. 16, § 5161(13)(f) (2017) (allowing unauthorized disclosure "[t]o Departmental contractors to the extent necessary for professional consultation or services").

182. *See* OKLA. STAT. tit. 43A, § 1-109(A)(2) (2013) ("The information available to persons actively engaged in the treatment of the consumer or in related administrative work shall be limited to the minimum amount of information necessary for the person or agency to carry out its function.").

limitation to e-PHI makes it formally inapplicable to information transmitted during telemental health sessions because patients communicate PHI, but not e-PHI, to providers. Transmitting data to providers through mobile health applications falls formally under the Security Rule's protections but suffers the same functional inadequacies as for synchronous communication generally. More troubling, such transmissions may be completely unprotected if the information is transmitted directly to a patient's EHR. To close these gaps, PHI stored by telehealth and other medical providers must be safeguarded under the Security Rule, but even then, the rule still fails to require encryption of such information, rendering it functionally inadequate. Archived telepsychology sessions receive basic HIPAA protection but lack the special protections granted to psychotherapy notes. Further still, would-be PHI stored by mobile health entities, companies that produce mobile health applications, or the business associates of these mobile health entities falls outside of HIPAA altogether, leaving broad categories of sensitive information completely unprotected. Patients aware of these security risks will be less inclined to take advantage of this technology.[183]

Certain modifications to the Rules could ameliorate these problems. First and foremost, the Security Rule must be extended to cover transmissions during telemental health sessions. In light of the emergence and rapid growth of online therapy sessions, no justifiable reason exists for preserving the technical distinction between PHI and e-PHI that renders the Security Rule inapplicable in this context. Congress or the HHS could remedy this oversight in a couple of ways. One option would be to eliminate the definitional requirement that PHI is only e-PHI in transmission if it "exist[ed] in electronic form immediately before the transmission."[184] Thus, the Security Rule would apply to any transmissions of e-PHI, including in real-time communication. Changing the definition of e-PHI in this way, however, would extend the coverage of the Security Rule to one category of transmissions that the HHS has expressed an intention not to protect—specifically, facsimile transmissions of printed copies of information that existed "in electronic form" but did not exist in this form

183. For an explanation of the centrality of privacy considerations in users' evaluations of the utility of health information technology, see *infra* note 188. Thus, even with the limited extent such information might be useful to hackers, in contrast with the lucrative value of more objective health data, the utility of this technology is unlikely to be maximized without addressing these concerns.

184. 45 C.F.R. § 160.103 (2017).

"immediately before transmission."[185] The better option would thus simply be to legislate or promulgate an agency rule extending the Security Rule to telemental health sessions.

Second, encrypting PHI when it is being stored and transmitted should be required rather than optional. The Security Rule is technologically outdated in this respect, promulgated to protect PHI transmitted electronically between providers and for administrative purposes. Now, telehealth sessions also implicate the electronic exchange of information during the actual course of treatment, making transmission security much more pressing. Additionally, mobile health applications dramatically increase the amount of data transmitted and stored with covered entities. This is a simple fix, as Congress or the HHS would merely need to switch the designation from "addressable" to "required."[186] This would give the Security Rule more bite while preserving the underlying flexibility that covered entities have in choosing how to implement even required specifications.[187] Whether such a change is necessary in the health or mental health context broadly is beyond the scope of this Note, but securing communication channels for telemental health sessions is undeniably vital.

Third, the Privacy and Security Rules should be extended to cover mobile health entities. Currently, patients using mobile health applications share sensitive health information with mobile health entities, and HIPAA protects neither the privacy nor security of such information. This could be achieved by amending the definitions of "covered entity" and "individually identifiable health information" to include mobile health entities. The Security Rule would then apply to the storage and transmission of data through mobile health applications. Moreover, mobile health entities would be barred by the Privacy Rule from sharing any information beyond what is minimally necessary for the provision of or payment for healthcare, which would curtail profit-motivated disclosures by such entities to big data developers.[188]

---

185. *See* 2013 HHS Report, *supra* note 140, at 5,576 ("[I]nclud[ing] the word 'immediately,' to exclude transmissions when the information exchanged did not exist in electronic form immediately before transmission . . . clarifies that . . . accepting a hardcopy document for transmission is not a covered transmission even though the document may have originated from printing from an electronic file.").

186. 45 C.F.R. § 164.306(d)(1).

187. *Id.* § 164.306(b).

188. Such regulatory pressure would likely increase the operating costs of mobile health entities. In particular, mobile health entities may be less inclined to make their applications freely

Fourth, Congress or the HHS should confer on archived psychotherapy sessions the same special protection given to psychotherapy notes. This protection is justified by the particularly sensitive nature of the information and its lack of informative value based on its personal nature. Given the highly sensitive nature of archived sessions, the associated privacy concerns are even stronger than for psychotherapy notes. Evidence shows that patients find therapeutic value in watching archived sessions,[189] so the law ought to allow and not overly deter these archived sessions. Given general patient privacy concerns and more specific mental health stigma concerns, patients would be more amenable to recorded sessions if they knew that the recording could not be transmitted without their permission. And, ultimately, getting patients to consent to recorded sessions in the first place is a threshold requirement for maximizing such value to be gained from the use of this technology. Altogether, these considerations warrant special protection for archived psychotherapy sessions.

Lastly, Congress or the HHS should strengthen requirements that covered entities periodically review their security practices under the Security Rule. As it stands, HIPAA regulations mandate such periodic review but do not specify how often it must occur.[190] However, because the telemental health and cybersecurity industries continue to develop

---

available because they would lose out on their revenue streams vis-à-vis selling information extracted from consumers with mental health problems. In other words, consumers would likely have to pay more to use mobile health applications if the entities responsible for these applications are no longer allowed to profit from selling their sensitive health information. But given the centrality of privacy concerns with respect to consumers' perceived utility of health information technology like mobile health, consumers would likely prefer this tradeoff. *See* Heather Landi, *Survey: Patients Skeptical of Health IT Due to Privacy, Security Concerns*, HEALTHCARE INFORMATICS (Jan. 3, 2017), https://www.healthcare-informatics.com/news-item/cybersecurity/survey-patients-distrust-health-it-due-privacy-security-concerns [https://perma.cc/CQH9-2FAQ] ("57 percent [of consumers] with contact experience to [medical] technology this past year report being skeptical of the overall benefits of health information technologies such as patient portals, mobile apps, and electronic health records . . . because of recently reported data hacking and a perceived lack of privacy protection by providers . . . .").

189. Luxton et al., *supra* note 9, at 506.

190. *See* 45 C.F.R. § 164.306(e) ("A covered entity or business associate *must* review and modify the security measures implemented under this subpart *as needed* to continue provision of reasonable and appropriate protection of electronic protected health information . . . .") (emphasis added). *But see* 42 U.S.C. § 17931(c) (2018) ("[T]he Secretary of Health and Human Services shall, after consultation with stakeholders, *annually* issue guidance on the most effective and appropriate technical safeguards . . . and . . . security standards . . . .") (emphasis added). The inconsistency between the regulatory and statutory review requirements further warrants reconsideration of the appropriate standards for periodic review.

rapidly, regularly revising industry practice with respect to the privacy and security of sensitive information is vital.[191] Instituting a time frame under the Security Rule for mandatory periodic review by covered entities of their own practices would strengthen the rule and better account for the rapid technological growth in this field and the law's general inability to keep up.[192] This would remain in keeping with the intended flexibility of the Rule[193] by allowing covered entities to conduct their own reviews.[194]

B. Streamlining the Federal Regime by Preempting the Field

After modifying the Rules as suggested above, Congress or the HHS should ensure that HIPAA preempts the state rules that currently share the same space, at least in the telemental health domain.[195] Preempting state law before updating the Rules would make things worse, because it would risk stifling further legal development and leaving citizens in states with more stringent privacy and security laws than the Rules even less protected than they are now. If the Rules were modified in the ways suggested above, however, Congress or the HHS should make it so that they preempt the field—at least in the context of telemental health. Field preemption is necessary given the possibilities of interstate telemental health treatment. Field preemption also makes more sense than floor preemption because the Rules are not one dimensional; rather, they reflect an intended balance between competing policy considerations.

First, telemental health for the first time makes interstate treatment a real and prevalent phenomenon, which lends further credence to preempting the wide variety of state law that could otherwise apply here. Under a state-by-state regime, providers treating

---

191. Heverly, *supra* note 86, *passim*.

192. *See* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY *passim* (2014) (arguing that the law has been slow to keep up with technological advancements in data analytics, threatening consumer privacy with respect to health and other information).

193. *See* 45 C.F.R. § 164.306(b) ("Flexibility of approach.").

194. Although requiring more revision could increase compliance costs, such costs would be offset by other proposed changes. For example, *requiring* encryption standards as opposed to deeming them merely "addressable" would eliminate the risk-analysis costs associated with reassessing whether neglecting to implement addressable safeguards would be "reasonable and appropriate." In addition, periodic-review requirements could vary temporally based on such factors as the size and longevity of the regulated entity as well as the sensitivity and magnitude of the health information they manage.

195. Congress or the HHS can accomplish this simply by including a provision clearly expressing the intention to preempt the field.

patients in other states will have to know which laws govern the treatment relationship in order to comply with them,[196] and there are essentially two options for the governing law.[197] One would be to apply the law of the provider's state, which would make the provider's job safer and more efficient but would leave patients without the protections that they would otherwise expect.[198] The other option is to apply the law of the patient's state, which would ensure that the patient receives any expected protections but would create an opportunity cost for the provider in having to deal with administrative matters rather than treating patients.[199] Additionally, providers having to deal with a variety of state laws may be deterred either from offering telehealth services in the first place or from offering those services to patients in certain states, which would restrict access and hamper progress in the industry.[200] Furthermore, neither state-by-state solution would do much to help industry actors seeking to innovate, because they must still navigate the complex web of state law. Streamlining the federal regime by preempting the field would add clarity and facilitate innovation vis-à-vis greater predictability.

---

196. The implications of interstate treatment have led many commentators to advocate for federal licensure standards for telehealth providers. *See* Marino et al., *supra* note 58, *passim*; Schumacher, *supra* note 54, at 431–32.

197. The two basic options contemplated above are simply to apply the laws either of the patient's or provider's state to all parties involved in treatment. There is, however, at least one more option that could be explored that would adequately accommodate interests in federalism, involving "reciprocity statutes" or interstate compacts through which multiple states band together, as in the Nurse Licensure Compact. *See* Schumacher, *supra* note 54, at 423 ("The [Nurse Licensure Compact] allows a nurse with a valid license to practice in other states party to the compact, both in person and through telecommunications technology, subject to the other states' practice laws and discipline."). However, Professor Schumacher argues that "the slow rate of adoption among the states prevents the model from significantly affecting licensure portability." *Id.* at 424. In addition, such a system makes far less sense in the context of patient privacy, which confers substantive protections to healthcare consumers, than in licensure, which fulfills largely administrative functions.

198. One of federalism's hallmarks is that state diversity engenders legal innovation and experimentation. Health-information privacy, however, is not an appropriate subject for experimentation given the sensitivity of the information involved. Legal experimentation is particularly inappropriate for mental health given the high risks of privacy breaches and the *de facto* permanence of potential data exposures. Finally, experimentation is even more inappropriate with respect to telemental and mobile health, where information can be exposed more easily over the internet.

199. This would also frustrate one of HIPAA's main objectives—streamlining EHR usage.

200. *See* Schumacher, *supra* note 54, at 420 ("The biggest barrier preventing the widespread implementation of telehealth services in the United States is the fact that states regulate the practice of medicine within their own boundaries.").

In addition, the balancing function of the Rules is already inconsistent with floor preemption. The Rules' purposes are not singular; rather, they aim to strike a balance between information privacy and availability.[201] The Rules recognize patient interests in maintaining the confidentiality of sensitive medical information but also the utility of having records available to other providers for treatment and efficiency purposes.[202] Though HIPAA's regulatory and statutory texts explicitly set a floor rather than preempt the field,[203] the balancing function calls into question the propriety of considering their requirements in a one-dimensional way, as a floor. With respect to the Privacy Rule, for example, more stringent state laws frustrate the purpose of the federal regime by making information sharing more difficult.[204] It is thus already illogical for the Rules to be treated for preemption purposes as setting a floor rather than occupying the field.

The emergence of telemental health shakes up the underlying policy considerations on each side of the scale, which makes reexamination of the proper preemptive function of the Rules all the more logically compelled. In particular, with conventional treatment, no security concerns arise regarding the treatment setting itself—the security concerns arise after the fact, with data storage and transmission. But privacy and security concerns are inherent in the provision of telemental health treatment.[205] The privacy and security risks associated with telehealth thus implicate policy considerations with respect to access to treatment. Thus, floor preemption makes even less sense in the context of telemental health because privacy and security considerations cannot be balanced with information availability along a single continuum.

In other words, a reformulation of HIPAA that properly accounted for the policy considerations at play would not simply be

---

201. *See, e.g.*, 45 C.F.R. § 164.502 (2012) (conferring general privacy protections to patients' health information but allowing disclosure for treatment purposes).

202. Specifically, the Omnibus Rule contemplates that the most cost-effective way to make health information accessible is through EHRs and electronic health tools generally. For further discussion of the Omnibus Rule, see *supra* note 102.

203. 42 U.S.C. § 1320d-2(d) (2018); 45 C.F.R. § 160.203(b).

204. As applied to conventional treatment modalities, this paradoxical effect may have been largely mitigated given the limited utility of sharing treatment information with providers in other states—as well as limited instances of providers treating out-of-state patients. Telehealth, however, flips this on its head, further justifying reexamination of the functional inconsistencies of HIPAA's preemptive status.

205. For example, unlike in a conventional face-to-face therapy session, a telepsychology session *itself* implicates privacy and security considerations.

able to balance privacy with accessibility; additionally, it would have to incorporate access to treatment into the policy calculus. This necessary balancing of multiple policy considerations in reformulating the Rules increases the likelihood that treating the Rules as simple "floors," which only above or below a state's rule could lie, would obfuscate at least part of the functional purpose of the Rules. Congress or the HHS should therefore preempt the field with the changes to HIPPA suggested in this Note.

CONCLUSION

Mental health care in the United States is saturated with problems, ranging from stigmatic concerns that deter patients from seeking treatment in the first place to cost and access issues that moderate the ability to begin and continue regular treatment for all patients. Telemental and mobile health platforms offer promising ways to overcome these central problems in mental health care, but privacy and security concerns stand in the way of fully taking advantage of these emergent technologies. The current legal landscape is ill-equipped to secure patient privacy given the dramatic increases in transmitted and stored health information. To the extent that HIPAA even applies, covered entities are free to leave this stored and transmitted data unencrypted, rendering the information unacceptably exposed. Worse still, HIPAA is outdated, which leaves telemental health sessions and stored mobile health data totally unprotected. And a complex web of state laws and regulations creates inefficiencies regarding provider practices, industry innovation, and legal administrability. The changes to the HIPAA Rules identified in this Note would dramatically improve patient privacy rights. Preempting the field with such changes would create a landscape more readily navigable by providers and industry members alike, facilitate interstate treatment, and enable while enabling the federal government to strike an appropriate balance between information availability and privacy.