2020

Assumed Compliance

Stacey A. Tovino, *University of Oklahoma College of Law*

ASSUMED COMPLIANCE

Stacey A. Tovino

ASSUMED COMPLIANCE

*Stacey A. Tovino**

INTRODUCTION

In response to a series of recent health data acquisitions,[1] investigations,[2] lawsuits,[3] and rulings,[4] federal and state lawmakers are quickly introducing new data privacy and security bills.[5] On December 12, 2018, Senator Brian Schatz (D-HI) introduced the Data Care Act (DCA), which would establish "duties of care, loyalty, and confidentiality" for online service providers that handle personal data.[6] Six months later, Senator Amy Klobuchar (D-MN) introduced the Protecting Personal Health Data Act (PPHDA), which would direct the Secretary of the federal Department of Health and Human Services (HHS) to "promulgate regulations [that would] strengthen privacy and security

* Professor of Law and Faculty Director, Healthcare Law Program, The University of Oklahoma College of Law, Norman, Oklahoma. I thank Lena Rieke for her outstanding research assistance. I also thank Professor Danny Sokol, Professor Benjamin van Rooij, and the participants of the Cambridge Handbook of Compliance Symposium held at the University of Florida Levin College of Law in Gainesville, Florida, for their comments and suggestions on the ideas presented in this Article.

1. *See, e.g.*, Daisuke Wakabayashi & Adam Satariano, *Google to Buy Fitbit for $2.1 Billion*, N.Y. TIMES (Nov. 1, 2019), https://www.nytimes.com/2019/11/01/technology/google-fitbit.html (reporting the acquisition of Fitbit by Google in a "$2.1 billion deal" and highlighting the concern that Google "is gaining private health information about its users").

2. *See, e.g.*, Rob Copeland & Sarah E. Needleman, *Google's 'Project Nightingale' Triggers Federal Inquiry*, WALL ST. J. (Nov. 12, 2019), https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867 (reporting that Ascension, the second largest health system in the United States, disclosed the identifiable health information of fifty million patients to Google and that the federal Department of Health and Human Services is investigating the data privacy concerns raised by the partnership between Ascension and Google).

3. *See, e.g.*, Dinerstein v. Google, L.L.C., No. 19 C 4311, 2020 WL 5296920 (N.D. Ill. Sept. 4, 2020) (suing the University of Chicago Medical Center for disclosing allegedly identifiable patient information to Google without the prior written authorization of the patients who were the subjects of the disclosed information).

4. *See, e.g.*, Letter from Elizabeth Denham, Info. Comm'r, Info. Comm'n Off., to Sir David Sloman, CEO, Royal Free Nat'l Health Serv. Found. Trust (July 3, 2017), https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf [hereinafter ICO Letter] (letter by the U.K. Information Commissioner's Office ruling that the Royal Free National Health Service Foundation Trust failed to comply with the Data Protection Act when it provided the information of 1.6 million patients to DeepMind, a London-based artificial intelligence lab owned by Google's parent company, without prior patient authorization).

5. *See, e.g.*, Protecting Personal Health Data Act, S. 1842, 116th Cong. (2019) (directing the Secretary of the federal Department of Health and Human Services to "promulgate regulations to help strengthen privacy and security protections for consumers' personal health data that is collected, processed, analyzed, or used by consumer devices, services, applications, and software").

6. Data Care Act of 2018, S. 3744, 115th Cong. § 3 (2018).

protections for . . . personal health data that [are] collected, processed, analyzed, or used by consumer devices, services, applications, [or] software."[7]

On October 17, 2019, Senator Ron Wyden (D-OR) introduced the Mind Your Own Business Act (MYOBA), which would require the Federal Trade Commission (FTC) to promulgate regulations obligating certain entities to "implement reasonable cyber security and privacy policies, practices, and procedures to protect personal information."[8] In a final illustrative example, Senator Bill Cassidy (R-LA) introduced, on November 28, 2019, the Smartwatch Data Act, which would prohibit certain entities that collect consumer health information (CHI)[9] from disclosing CHI to information brokers who collect or analyze CHI for profit.[10]

The DCA, PPHDA, MYOBA, and Smartwatch Data Act share a number of common features. All four bills identify the entities to be regulated, the data to be protected, and the restrictions to be applied to the collection, use, disclosure, and/or sale of protected data.[11] These bills also specify the agencies that would be responsible for enforcement. HHS would enforce the PPHDA[12] and the Smartwatch Data Act,[13] for example, while the FTC would enforce the DCA[14] and the MYOBA.[15] Civil and/or criminal penalties for violations are also specified in some bills[16] as are certain rights of action.[17]

These legislative initiatives also beg several important questions. Foremost is whether newly regulated entities will actually comply with these laws with respect to the health data they collect, use, disclose, and sell. Which provisions within these laws are likely to cause confusion among regulated entities resulting in regulatory avoidance or noncompliance? Should any of the provisions in these bills be strengthened? Should any provisions be removed either because they are unlikely to improve data privacy or security or because they will be

7. S. 1842 § 4(a).

8. Mind Your Own Business Act of 2019, S. 2637, 116th Cong. § 7(b)(1)(A) (2019).

9. The Smartwatch Data Act defines consumer health information as "any information about the health status, personal biometric information, or personal kinesthetic information about a specific individual that is created or collected by a personal consumer device, whether detected from sensors or input manually." Stop Marketing and Revealing the Wearables and Trackers Consumer Health (Smartwatch) Data Act, S. 2885, 116th Cong. § 2(6) (2019).

10. *Id.* § 3(a)(1)(A).

11. *See* S. 3744 §§ 2–3; S. 1842 §§ 3–4; S. 2637 §§ 2, 5, 6; S. 2885 §§ 2–3.

12. S. 1842 §§ 3(6), 4.

13. S. 2885 § 4.

14. S. 3744 § 4(a)(2)(A). State attorneys general also have the authority to enforce violations of the DCA on behalf of state residents. *Id.* § 4(b)(1).

15. S. 2637 §§ 3–4.

16. *See* S. 3744 § 4(b)(2) (giving state attorneys general the authority to impose civil penalties for violations of the DCA); S. 2637 §§ 4–5 (establishing civil and criminal penalties for MYOBA violations); S. 2885 § 4 (giving HHS the authority to impose civil money penalties for violations of the Smartwatch Data Act).

17. S. 2637 § 7(e)–(f) (stating that state attorneys general as well as protection and advocacy organizations have a right of action for violations).

difficult or impossible to enforce? More broadly, how can new legislation, or amendments to existing legislation, best protect data privacy and security at a time when health data are being collected, used, disclosed, and sold at an unprecedented rate?

To answer these questions, this Article carefully studies the history of compliance with existing health data privacy, security, and breach notification rules promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[18] as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).[19] As background, the HIPAA Privacy Rule (Privacy Rule),[20] the HIPAA Security Rule (Security Rule),[21] and the HIPAA Breach Notification Rule (Breach Notification Rule)[22] (collectively the HIPAA Rules) were promulgated to protect the privacy and security of individually identifiable health information created or maintained in health care and health insurance contexts and to assist patients and insureds in protecting themselves in the event of a privacy or security breach. Although the HIPAA statute authorizes the federal government to impose civil and criminal penalties for violations of the HIPAA Rules,[23] the HIPAA Rules are limited in application to: (1) health plans, health care clearinghouses, and those health care providers that transmit health information in electronic form in connection with standard transactions, including health insurance claims (collectively covered entities);[24] and, following HITECH, (2) persons or entities that access or use protected health information (PHI) to provide certain services to, or to perform certain functions on behalf of, covered entities (collectively business associates).[25] The HIPAA Rules do not protect the privacy and security of health data collected, used, disclosed, or sold by many technology companies, online service providers, mobile health applications, and other entities and technologies that do not meet the definition of a covered entity or business associate.[26] The DCA,

18. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.).

19. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 115, 226 (2009) (codified as amended in scattered sections of 42 U.S.C.).

20. The HIPAA Privacy Rule is codified at 45 C.F.R. § 164.500–.534 (2019).

21. The HIPAA Security Rule is codified at 45 C.F.R. § 164.302–.318 (2019).

22. The HIPAA Breach Notification Rule is codified at 45 C.F.R. § 164.400–.414 (2019).

23. *See* Health Insurance Portability and Accountability Act §§ 1176–77 (adding 42 U.S.C. § 1320d-5 (establishing civil penalties for violations of the HIPAA Rules) and 42 U.S.C. § 1320d-6 (establishing criminal penalties for violations of the HIPAA Rules)); Health Information Technology for Economic and Clinical Health Act § 13410(d) (revising the amount of the civil penalties authorized by HIPAA).

24. *See* HIPAA Privacy Rule, 45 C.F.R. § 160.103 (2019) (defining covered entity); *id.* § 160.102(a) (applying the HIPAA Rules to covered entities).

25. *See id.* § 160.103 (defining business associate); *id.* § 160.102(b) (applying the HIPAA Rules to business associates).

26. *See, e.g.*, I. Glenn Cohen & Michelle M. Mello, *Big Data, Big Tech, and Protecting Patient Privacy*, 322 JAMA 1141, 1141–42 (2019), https://jamanetwork.com/journals/jama/fullarticle/2748399 (arguing that "HIPAA is a 20th-century statute ill equipped to address 21st-century data practices" in part due to its limited

PPHDA, MYOBA, and Smartwatch Act are designed, in part, to fill these gaps in regulation, as are proposals to expand the application of the HIPAA Rules.[27]

Prior scholars have impliedly assumed, without testing, that new or expanded privacy and security regulation will automatically yield improved data privacy and security protections.[28] But how do we know this assumption is true? What is the relationship between regulation and compliance in the context of health data privacy and security? Is new or expanded regulation the only—or

applicability); I. Glenn Cohen & Michelle M. Mello, *HIPAA and Protecting Health Information in the 21st Century*, 320(3) JAMA 231, 232 (2018), https://jamanetwork.com/journals/jama/issue/320/3 [hereinafter Cohen & Mello, *21st Century*] ("HIPAA 'attaches (and limits) data protection to traditional health care relationships and environments.' The reality . . . is that HIPAA-covered data form a small and diminishing share of the health information stored and traded in cyberspace."); Mark A. Rothstein et. al, *Citizen Science on Your Smartphone: An ELSI Research Agenda*, 43 J. L. MED. & ETHICS 897, 899 (2015) (explaining that health research undertaken by an individual or entity that is not a HIPAA-covered entity, such as a citizen scientist, is not regulated by the HIPAA Rules); Mark A. Rothstein, *The End of the HIPAA Privacy Rule?*, 44 J. L. MED. & ETHICS 352, 352 (2016) (noting that the HIPAA Privacy Rule has fallen into disrepute because of its limited coverage; "it applies only to 'covered entities'"); Nicolas P. Terry & Tracy D. Gunter, *Regulating Mobile Mental Health Apps*, 36 BEHAV. SCI. L. 136, 139–40 (2018) (explaining that mobile medical applications that collect identifiable health data may not be regulated by the HIPAA Rules); Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. 155, 158–59 (2019) (providing examples of individuals and institutions not regulated by the HIPAA Rules).

27. *See, e.g.*, Ashley Bateman, *HHS Urged to Update HIPAA to Protect Patient Medical Records*, HEARTLAND INST. (Feb. 20, 2020), https://www.heartland.org/news-opinion/news/hhs-urged-to-update-hipaa-to-protect-patient-medical-records (reporting that the Citizens' Council for Health Freedom has petitioned HHS to tighten loopholes in HIPAA's substantive protections). It has also been argued that:

> AMIA and AHIMA recommend that lawmakers develop or direct HHS to define HIPAA NCEs [non-covered entities] in law and at minimum extend HIPAA's right of access to such NCEs. The goal of such a policy is to create a uniform data access policy for individuals using technology developed by an entity that produces and/or manages their individually identifiable health information, regardless of commercial or legal status.

AM. MED. INFORMATICS ASS'N & AM. HEALTH INFO. MGMT. ASS'N, EXTENDING THE HIPAA INDIVIDUAL RIGHT OF ACCESS TO NON-COVERED ENTITIES (NCEs) (2020), http://bok.ahima.org/PdfView?oid=302698.

28. Suggestions of new regulations have been made through one of two options:

> One option that has been proposed is to enact a general rule protecting health data that specifies further, custodian-specific rules; another is to follow the European Union's new General Data Protection Regulation in setting out a single regime applicable to custodians of all personal data and some specific rules for health data.

See, e.g., Cohen & Mello, *21st Century*, *supra* note 26 (not discussing the relationship between regulation and compliance); Daniel J. Solove, *The Myth of the Privacy Paradox* 89 GEO. WASH. L. REV. (forthcoming 2021) ("There is a role for privacy regulation that goes beyond relying heavily on privacy self-management. . . . Highly effective privacy regulation focuses on the architecture of the personal data economy—data collection, use, storage, and transfer.") (not discussing the relationship between regulation and compliance); Aleecia M. McDonald, *Laws Can Ensure Privacy in the Internet of Things*, N.Y. TIMES: THE OPINION PAGES (Sept. 8, 2013), https://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/laws-can-ensure-privacy-in-the-internet-of-things (arguing that "we need new privacy laws that are savvy and wise," but not examining the relationship between new laws and compliance). Even industry insiders believe that new data privacy and security laws are needed. They too fail to examine the relationship between regulation and compliance. *See, e.g.*, Jonny Evans, *'We Need New Privacy Laws,' Urges Apple CEO Tim Cook*, COMPUTERWORLD (Jan. 17, 2019), https://www.computerworld.com/article/3331953/we-need-new-privacy-laws-urges-apple-ceo-tim-cook.html (stating that Apple CEO Tim Cook has urged Congress to enact a comprehensive privacy law but not addressing the relationship between a future law and compliance).

the best—way to protect emerging forms of health data?[29] This Article is the first piece of legal scholarship to answer these questions using history as a guide.

This Article proceeds as follows: Part I briefly reviews the regulatory history of, and the substantive provisions set forth in, the HIPAA Rules.[30] This discussion will place the HIPAA Rules studied in Part II of this Article in their proper context. Part II carefully examines academic, industry, and government studies assessing covered entities' and business associates' compliance with the HIPAA Rules.[31] Despite HHS's provision of considerable guidance and technical assistance to covered entities and business associates regarding their responsibilities under the HIPAA Rules,[32] little is commonly known about the extent of covered entities' and business associates' actual compliance as well as reasons for noncompliance.

Part II reports important findings from the HIPAA Rules compliance literature.[33] These findings relate to the extent to which many covered entities do not comply with the Privacy Rule's plain language requirement, the Privacy Rule's access to protected health information requirement, the Security Rule's addressable encryption standard, and the Security Rule's audit logs and access reports requirement.[34] Additional findings relate to the extent to which covered hospitals and health systems believe they are complying with the HIPAA Rules when they are not, the positive impact of HITECH on data breaches by

29. *See generally* Tovino, *supra* note 26, at 208 (noting, for example, that health data are generated not only by traditional health industry participants, such as doctors, hospitals, and health insurance companies, but also by a variety of non-health industry participants, including independent scientists, citizen scientists, patient researchers, and mobile health applications).

30. *Infra* Part I. In addition to the HIPAA Rules, a variety of other federal, state, and international statutes and regulations impose, or have been interpreted to impose, privacy, security, and breach notification obligations on a wide range of individuals and institutions that collect, use, disclose, or sell data in certain contexts. *See, e.g.*, CAL. CONST. art. I, § 1 (illustrative state constitutional provision establishing a right to pursue and obtain privacy); Gramm–Leach–Bliley Act, Pub. L. No. 106-102, §§ 501–09, 113 Stat. 1338, §§ 1436–45 (1999) (codified as amended at 15 U.S.C. §§ 6801–09 & §§ 6821–27 (1999)) (illustrative federal statute requiring financial institutions to provide notice to customers of privacy policies and practices; regulating financial institutions' disclosure of nonpublic personal information; requiring financial institutions to develop an information security plan); California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (West 2003) (illustrative state statute giving California residents certain rights relating to the privacy and security of their personal data); Data Protection Act of 2018, c. 12 (Eng.) (illustrative international act regulating the processing of personal data); 45 C.F.R. § 46.111(a)(7) (2019) (illustrative federal regulation requiring "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data" generated in the context of human subjects research); 2016 O.J. (L119) 1 (illustrative international regulation protecting natural persons with respect to the processing of their personal data). Whether the entities regulated by these statutes and regulations comply is beyond the scope of this Article.

31. *See infra* Part II.

32. *See, e.g.*, U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 1–23 (2003), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (providing guidance regarding the substance and interpretation of the HIPAA Privacy Rule); U.S. DEP'T HEALTH & HUMAN SERVS., TRAINING AND RESOURCES, https://www.hhs.gov/hipaa/for-professionals/training/index.html (providing information, guides, and video training modules to help covered entities and business associates comply with the HIPA Privacy Rule).

33. *See infra* Part II.

34. *See infra* Part II.

business associates, the varied organizational strategies and institutional environments that influence compliance, the extent to which institutional pressures and internal security needs assessments influence investment in security compliance, and health care professional discourse about patient privacy.[35]

Part II also finds that the HIPAA Rules compliance literature is not as robust as it could—or should—be. Many of the available compliance studies have significant limitations that affect their generalizability and, in some cases, their reliability.[36] For example, most of the available studies focus on small subsets of regulated actors, leaving entire classes of covered entities and business associates unstudied.[37] Many studies focus on compliance with discrete regulatory provisions, ignoring dozens of other HIPAA Rules requirements.[38] Many studies focus on compliance in narrow contexts, such as personal health records or text messaging, overlooking daily interactions between and among workforce members and the large-scale operations of covered entities and business associates.[39] Several studies that rely on self-reported compliance data reveal substantial misunderstandings regarding the HIPAA Rules by regulated actors.[40] Finally, some studies demonstrate misunderstandings regarding the HIPAA Rules by non-lawyer study authors, impacting both study design and data analysis.[41]

Part III refocuses on pending health data privacy and security bills including the DCA, PPHDA, MYOBA, and Smartwatch Data Act, as well as proposals to expand and strengthen the HIPAA Rules.[42] Part III argues that these initiatives assume a perfect relationship between regulation and compliance—an assumption Part II has shown to be untrue. These legislative initiatives also underestimate the power of statutory simplicity as well as stronger frameworks governing the collection, use, disclosure, and sale of health data. Using insights drawn from Part II, Part III proposes specific language for future health data privacy and security legislation that will best protect the privacy and security of health data going forward. Part III also makes concrete suggestions for further developing the compliance literature in this area. It is the author's hope that the proposals set forth in this article will improve generalizable knowledge regarding the relationship between regulation and compliance and, ultimately, health data privacy and security.[43]

35. *See infra* Part II.
36. *Infra* Part II.
37. *Infra* Part II.
38. *Infra* Part II.
39. *See infra* Part II.
40. *Infra* Part II.
41. *Infra* Part II.
42. *Infra* Part III.
43. *Infra* Part III.

I. THE HIPAA RULES

A. The Privacy Rule

The Privacy Rule has its origins in the HIPAA statute, which President Clinton signed on August 21, 1996.[44] Section 264 of HIPAA stated that Congress had thirty-six months to enact federal legislation protecting the privacy of individually identifiable health information.[45] If Congress missed its statutory deadline, HHS had an additional six months to promulgate privacy regulations.[46] When Congress missed its statutory deadline, the responsibility fell to HHS to adopt privacy regulations. HHS responded by issuing a proposed Privacy Rule on November 3, 1999,[47] a final Privacy Rule on December 28, 2000,[48] proposed modifications on March 27, 2002,[49] and final modifications on August 14, 2002.[50]

Although the Privacy Rule remained largely unchanged between 2002 and 2009, the nature and scope of the privacy duties that applied to covered entities and their business associates changed significantly thereafter. On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act (ARRA) into law.[51] Division A, Title XIII of ARRA, better known as HITECH, directed HHS to modify some of the information use and disclosure requirements and definitions set forth in the Privacy Rule, apply certain Privacy Rule provisions directly to business associates, and amend the civil penalty amounts applicable to covered entities and business associates for violations of

44. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.). The author has written a number of prior articles that required a summary of the HIPAA Rules. With technical revisions, conforming changes, and regulatory updates, the summary of the HIPAA Rules set forth in Part I of this article is taken with the author's permission from these prior articles. *See, e.g.*, Tovino, *supra* note 26, at 157–59; Stacey A. Tovino, *A Timely Right to Privacy*, 104 IOWA L. REV. 1361, 1367–74 (2019); Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973, 979–83 (2017); Stacey A. Tovino, *Teaching the HIPAA Privacy Rule*, 61 ST. LOUIS U. L.J. 469, 475–480 (2017); Stacey A. Tovino, *Silence is Golden. . .Except in Health Care Philanthropy*, 48 U. RICH. L. REV. 1157, 1165–70 (2014).

45. Health Insurance Portability and Accountability Act § 264(c)(1).

46. *Id.*

47. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,924 (proposed Nov. 3, 1999).

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

49. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776 (Mar. 27, 2002).

50. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pt. 160 and 164).

51. *See* American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 115 (codified as amended in scattered sections of 42 U.S.C.).

the HIPAA Rules.[52] On January 25, 2013, HHS released a final rule modifying the Privacy Rule in accordance with HITECH.[53]

As modified by HITECH, the Privacy Rule requires covered entities and business associates to protect the privacy of a subset of individually identifiable health information known as protected health information (PHI).[54] Health information that has been properly de-identified, however, is not regulated by the HIPAA Rules.[55] One method of de-identifying health information involves removing eighteen different identifiers including, but not limited to, names,

52. *Id.* §§ 13400–10.

53. 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, 5,688 (Jan. 25, 2013) (codified at 45 C.F.R. pt. 160, 164). HHS issued additional rules and guidance documents in the post-HITECH period that are necessary to have a complete understanding of the Privacy Rule. On September 16, 2013, for example, HHS released a Model Notice of Privacy Practices designed to assist covered entities in complying with HITECH. U.S. DEP'T OF HEALTH & HUM. SERVS., *Model Notice of Privacy Practices*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html (last updated Apr. 13, 2013). On February 6, 2014, HHS released a final rule providing individuals with a right to receive their laboratory test results directly from their testing laboratories. CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports, 79 Fed. Reg. 7,290, 7,290 (Feb. 6, 2014) (codified at 45 C.F.R. pt. 164). On January 6, 2016, HHS released a final rule modifying the Privacy Rule to permit certain covered entities to disclose protected health information to the National Instant Criminal Background Check System, such as the identities of individuals who are disqualified "from shipping, transporting, possessing, or receiving a firearm." Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the National Instant Criminal Background Check System (NICS), 81 Fed. Reg. 382, 382 (Jan. 6, 2016) (codified at 45 C.F.R. pt. 164). And on March 6, 2020, HHS released in advance of *Federal Register* publication a final rule requiring privacy and security in the context of application programming interfaces (API). CTR. FOR MEDICARE & MEDICAID SERVS., U.S. DEP'T OF HEALTH & HUM. SERVS., INTEROPERABILITY AND PATIENT ACCESS FOR MEDICARE ADVANTAGE ORGANIZATION AND MEDICAID MANAGED CARE PLANS, STATE MEDICAID AGENCIES, CHIP AGENCIES AND CHIP MANAGED CARE ENTITIES, ISSUERS OF QUALIFIED HEALTH PLANS ON THE FEDERALLY-FACILITATED EXCHANGES, AND HEALTH CARE PROVIDERS (Mar. 6, 2020). As of this writing, HHS is more than eight years overdue on a proposed rule that would allow civil money penalties and settlements associated with HIPAA Rules violations to be shared with harmed individuals, as required by HITECH. *See* 42 U.S.C. § 17939(c)(3) (2019) ("Not later than 3 years after February 17, 2009, the Secretary shall establish by regulation . . . a methodology under which an individual who is harmed by an act that constitutes an offense . . . may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense."); *see also* Tovino, *A Timely Right to Privacy*, *supra* note 44, at 1393–97 (arguing that HHS's delay in issuing these rules contributes to individuals' inability to enforce their privacy rights in a timely manner).

54. *See generally* 45 C.F.R. § 160.103 (2019) (defining PHI); *id.* (defining individually identifiable health information as a subset of health information that is "created or received by a health care provider, health plan, employer, or health care clearinghouse" and that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"); *id.* (listing the four exclusions from the definition of PHI).

55. U.S. DEP'T OF HEALTH & HUM. SERVS., *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last updated Nov. 6, 2015) ("Regardless of the method by which de-identification is achieved, the Privacy Rule does not restrict the use or disclosure of de-identified health information, as it is no longer considered protected health information."); *see* 45 C.F.R. § 164.514(a) (2019) ("Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."); *see also id.* § 164.514(b)(1)–(2) (setting forth two methods for health information to be considered deidentified).

"[a]ll geographic subdivisions smaller than a [s]tate," all elements of dates except for year for individuals eighty-nine years of age and younger, "[f]ull face photographic images and any comparable images," and "other unique identifying number[s], characteristic[s], or code[s]."[56] A second method of deidentifying information requires a "person with appropriate knowledge of" accepted and relevant "statistical and scientific principles and methods" to render a determination "that the risk is very small that the information could be used, alone or in combination with other . . . information, . . . to identify an individual who is a subject of the information."[57]

Once a covered entity or business associate has PHI in its possession, the Privacy Rule contains three sets of regulations—including the use and disclosure requirements,[58] the individual rights,[59] and the administrative requirements[60]—that are designed to help protect the privacy of that PHI. Because several of the studies referenced in Part II study compliance with these regulation sets, a brief summary is necessary here. The first set of regulations, the use and disclosure requirements, obligate covered entities and business associates to adhere to one of three different requirements when using or disclosing PHI depending on the purpose of the use or disclosure.[61] The first use and disclosure requirement allows covered entities to use and disclose PHI with no prior permission from the individual who is the subject of the PHI—but only in certain situations. That is, covered entities may freely use and disclose PHI without any form of prior permission in order to carry out certain "treatment, payment, and health care operations"[62] activities (collectively TPO activities),[63] as well as certain public benefit activities.[64]

Under the second use and disclosure requirement, a covered entity may use and disclose an individual's PHI for certain activities, but only if the individual is informed (orally or in writing) in advance of the use or disclosure and is given the (oral or written) opportunity to agree to, prohibit, or restrict the use or disclosure.[65] The certain activities captured by this provision include, but are

56. 45 C.F.R. § 164.514(b)(2) (2019) (listing all eighteen identifiers that must be removed from protected health information for the information to be considered de-identified).

57. *Id.* § 164.514(b)(1).

58. *Id.* §§ 164.502–.514.

59. *Id.* §§ 164.520–.528.

60. *Id.* § 164.530.

61. *Id.* §§ 164.502–.514 (setting forth the use and disclosure requirements applicable to covered entities and business associates).

62. *Id.* § 164.506(c)(1) (permitting a covered entity to use or disclose PHI for its own treatment, payment, or health care operations); *id.* § 164.501 (defining treatment, payment, and health care operations).

63. 45 C.F.R. § 164.506(c)(1); *id.* § 164.506(c)(2)–(4) (permitting a covered entity to disclose PHI to certain recipients for the recipients' treatment, payment, or health care operations activities, respectively).

64. Covered entities may use and disclose PHI for twelve different public policy activities without the prior written authorization of the individual who is the subject of the information. *Id.* § 164.512(b).

65. *Id.* § 164.510 (explaining the standards for "[u]ses and disclosures requiring an opportunity for the individual to agree or to object").

not limited to, disclosures of PHI: (1) from a health care provider's facility directory; (2) to a person who is involved in an individual's care or payment for care; and (3) for certain notification purposes, such as when an attending physician or a hospital social worker notifies a patient's spouse or partner of the patient's death.[66]

The Privacy Rule's third use and disclosure requirement—a default rule—requires covered entities to obtain the prior written authorization of the individual who is the subject of the PHI before using or disclosing the individual's PHI in any situation that does not fit within the first two rules.[67] The Privacy Rule requires authorizations to contain a number of core elements and required statements, such as: (1) "[a] description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;"[68] (2) the "specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;"[69] (3) the "specific identification of the person(s), or class of persons"[70] authorized to receive the information; (4) a "description of each purpose of the requested use or disclosure;"[71] (5) an "expiration date or an expiration event;"[72] (6) "[s]ignature of the individual and date;"[73] (7) a statement regarding the "individual's right to revoke the authorization in writing;"[74] (8) a statement regarding the ability or inability of the covered entity to condition treatment or other activities on the authorization; and (9) the "potential for information disclosed pursuant to the authorization [form] to be subject to redisclosure by the recipient and no longer be protected by [the Privacy Rule]."[75]

The Privacy Rule further specifies that "authorization[s] must be written in plain language"[76] and that "the covered entity must provide the individual with a copy of [any] signed authorization."[77] Part II.A of this Article reviews a study investigating covered entities' compliance with the Privacy Rule's plain language authorization requirement.[78] This study reported that the average reading level

66. *See id.* § 164.510(a); *id.* § 164.510(b)(1)(i); *id.* § 164.510(b)(1)(ii).

67. *See id.* § 164.508(a)(1).

68. *Id.* § 164.508(c)(1)(i).

69. *Id.* § 164.508(c)(1)(ii).

70. *Id.* § 164.508(c)(1)(iii).

71. *Id.* § 164.508(c)(1)(iv).

72. *Id.* § 164.508(c)(1)(v).

73. *Id.* § 164. 508(c)(1)(vi).

74. *Id.* § 164.508(c)(2)(iii).

75. *Id.* § 164.508(c)(2)(iii) (listing the core elements and required statements of a HIPAA-compliant authorization form). *See generally* OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., GUIDANCE ON HIPAA AND INDIVIDUAL AUTHORIZATION OF USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR RESEARCH (June 2018) (responding to the 21st Century Cures Act's requirement that the Secretary of HHS publish guidance regarding future research authorizations).

76. 45 C.F.R. § 164.508(c)(3).

77. *Id.* § 164.508(c)(4).

78. *Infra* Part II.A.

of the reviewed authorization forms was the 11.6-grade level—well above the average reading level of the American public—notwithstanding the Privacy Rule's plain language requirement.[79] The study authors recommended that HHS issue explicit guidance regarding ways to make authorization forms "easier to read and understand."[80] The study authors also recommended more intense supervision by HHS of covered entity-created authorization forms.[81] Part III of this Article proposes legislation designed to accomplish these goals.

In addition to its use and disclosure requirements, the Privacy Rule contains a second set of regulations establishing certain rights for individuals who are the subject of PHI vis-à-vis their covered entities, including the right to receive a "notice of privacy practices,"[82] the "right to request additional privacy protections,"[83] the right to access PHI,[84] the right to request amendment of incorrect or incomplete PHI,[85] and the "right to receive an accounting of [PHI] disclosures."[86] Part II.B of this Article reviews a study investigating covered entities' compliance with the third individual right, that is, the right of individuals to access their PHI.[87] This study finds that some individuals are: (1) provided with confusing directions regarding how to access their PHI; (2) not given access to their PHI in express violation of the Privacy Rule; and (3) charged too much money for accessing their PHI.[88] The study authors recommended less burdensome and more transparent access policies and procedures.[89] Part III of this Article proposes legislation designed to decrease burden and increase transparency with respect to PHI access rights.

Moreover, Part II.E of this Article reviews a study investigating covered providers' compliance with the Privacy Rule in general, including the fifth individual right, that is, the right to receive an accounting of PHI disclosures.[90]

79. *Infra* Part II.A.

80. *Infra* Part II.A.

81. *Infra* Part II.A.

82. 45 C.F.R. § 164.520(a).

83. *Id.* § 164.522.

84. *Id.* § 164.524.

85. *Id.* § 164.526.

86. *Id.* § 164.528(a)(1).

87. *Infra* Part II.B.

88. *Infra* Part II.B.

89. *Infra* Part II.B.

90. *Infra* Part II.E. The Privacy Rule's accounting of disclosures provision is, in theory, straightforward. The provision gives patients and insureds the "right to [request and] receive an accounting [or list] of disclosures of [their PHI] made by [their] covered entit[ies] in the six years prior to the date on which the accounting is requested." 45 C.F.R. § 164.528(a)(1). What makes the provision difficult, in terms of implementation and compliance, is the long list of disclosures that are excepted from the accounting requirement. Excepted disclosures include: (1) disclosures to carry out TPO; (2) disclosures to individuals of PHI about themselves; (3) disclosures that are incidental to an otherwise permitted use or disclosure; (4) disclosures made pursuant to a prior written authorization; (5) disclosures of facility directory information and disclosures to persons involved in a patient's care; (6) disclosures "[f]or national security or intelligence purposes;" (7) disclosures "[t]o correctional institutions or law enforcement officials;" (8) disclosures "of a

Although the provider respondents reported growing accustomed to the Privacy Rule in the first three years following the compliance date, the respondents also reported that the accounting of disclosures requirement was particularly burdensome and inefficient.[91] Part III proposes ways to simplify the accounting requirement.

The third set of regulations contained within the Privacy Rule is known as the administrative requirements. Under the administrative requirements, covered entities must designate a privacy officer who will oversee compliance with the Privacy Rule, train workforce members regarding how to comply with the Privacy Rule, sanction workforce members who violate the Privacy Rule, establish a complaint process for individuals who believe their privacy rights have been violated, and develop privacy-related policies and procedures, among other similar requirements.[92]

The Privacy Rule established a compliance date of April 14, 2003, for most covered entities.[93] "Small health plans"—those "with annual receipts of $5 million or less"[94]—did not have to comply until April 14, 2004.[95] Part II.F of this Article reviews a study showing that even Ivy League-affiliated study authors had difficulty determining which compliance deadlines applied to covered entities.[96] Part III of this Article proposes legislative text designed to minimize confusion regarding compliance dates going forward.

B. The Security Rule

In addition to the Privacy Rule, HIPAA also directed the Secretary of HHS to promulgate a Security Rule.[97] HHS responded by issuing a proposed Security Rule on August 12, 1998,[98] an initial final Security Rule on February 20, 2003,[99] and a post-HITECH final Security Rule on January 25, 2013.[100] Very broadly, the Security Rule requires covered entities and business associates to implement

limited data set;" and (9) disclosures that occurred prior to the date the covered entity was required to comply with the Privacy Rule. *Id.* § 164.528(a)(1)(i)–(ix).

91. *Infra* Part II.E.

92. 45 C.F.R. § 164.530.

93. *Id.* § 164.534(a), (b)(1).

94. *Id.* § 160.103 (defining small health plan).

95. *Id.* § 164.534(b)(2).

96. *Infra* Part II.F.

97. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, sec. 262, § 1173, 110 Stat. 1936, 2024–26 (codified as amended in scattered sections of 42 U.S.C.).

98. Security and Electronic Standards, 63 Fed. Reg. 43,242 (Aug. 12, 1998).

99. Health Insurance Reform: Security Standards, Final Rule, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164).

100. 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, 5,688 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164).

administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).[101]

In terms of the Security Rule's administrative safeguards, covered entities and business associates must designate a "security official . . . responsible for the development and implementation of the [covered entity's or business associate's security] policies and procedures."[102] These policies and procedures: (1) "prevent, detect, contain, and correct security violations,"[103] including through "audit logs, access reports, and security incident tracking reports;"[104] (2) "ensure that [workforce] members . . . have appropriate access to [ePHI];"[105] (3) "prevent . . . workforce members who [should] not have access [to ePHI] from obtaining access;"[106] (4) create "a security awareness and training program for all [workforce] members;"[107] and (5) address and respond to security incidents, emergencies, environmental problems, and other occurrences such as "fire, vandalism, system failure, and natural disaster" that affect systems containing ePHI and the security of ePHI, among other requirements.[108] Part II.C of this Article reviews a study that attempts to investigate compliance with the Security Rule's audit logs and access reports requirement.[109] However, this study demonstrates misunderstanding by the non-lawyer study authors regarding the Security Rule and/or confusion between the Security Rule and the Privacy Rule.[110] Part III of this Article proposes legislation that would decrease confusion between typical security measures (e.g., audit logs and access reports) and privacy-related rights (e.g., the right to receive an accounting of disclosures).

In terms of physical safeguards, the Security Rule requires covered entities and business associates to implement policies and procedures that: (1) "limit physical access to . . . electronic information systems and the . . . facilities in which they are [located];"[111] (2) address the safeguarding, functioning, and physical attributes of workstations through which ePHI is accessed; and (3) "govern the receipt and removal of hardware and electronic media that contain [ePHI]."[112] Finally, in terms of technical safeguards, the HIPAA Security Rule

101. 45 C.F.R. § 160.103 (2019) (defining ePHI); *id.* §§ 164.302–.312 (establishing the security obligations of covered entities and business associates). *See generally* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 331–86 (2007) (summarizing and critiquing the Security Rule).

102. 45 C.F.R. § 164.308(a)(2).

103. *Id.* § 164.308(a)(i).

104. *Id.* § 164.308(a)(1)(ii)(D).

105. *Id.* § 164.308(a)(3)(i).

106. *Id.*

107. *Id.* § 164.308(a)(5)(i).

108. *Id.*

109. *Infra* Part II.C.

110. *Infra* Part II.C.

111. 45 C.F.R. § 164.310(a)(1).

112. *Id.* § 164.310(d)(1).

requires covered entities and business associates to implement (1) "technical policies and procedures for electronic information systems that maintain [ePHI] to allow access only to those persons or software programs that have been granted access rights;"[113] (2) "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use [ePHI];"[114] (3) "policies and procedures to protect [ePHI] from improper alteration or destruction;"[115] (4) "procedures to verify that a person or entity seeking access to [ePHI] is the one claimed;"[116] and (5) "technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network."[117]

The Security Rule established a compliance deadline of April 20, 2005, for most covered entities.[118] Small health plans had an additional year to comply.[119] Part II.G of this Article reviews a study investigating mandatory versus voluntary (early) compliance with these deadlines, finding that non-profit corporations were more likely to engage in voluntary (early) compliance than for-profit corporations.[120] Given that Google and other technology giants entering and/or dominating the health data acquisition space are for-profit,[121] whereas many traditional health care providers regulated by the HIPAA Rules are non-profit,[122] Part III proposes legislation with earlier (i.e., non-extended) compliance deadlines.

C. The Breach Notification Rule

Although the Privacy and Security Rules are regulatory byproducts of HIPAA, signed into law by President Clinton in 1996, the Breach Notification Rule derives solely from HITECH, signed into law by President Obama in 2009.[123] Section 13402 of HITECH requires covered entities and business associates to adhere to certain notification procedures in the event of a breach

113. *Id.* § 164.312(a)(1).

114. *Id.* § 164.312(b).

115. *Id.* § 164.312(c)(1).

116. *Id.* § 164.312(d).

117. *Id.* § 164.312(e)(1).

118. *Id.* § 164.318(a)(1), (b), (c).

119. *Id.* § 164.318(a)(2).

120. *Infra* Part II.G.

121. *See, e.g.*, Copeland & Needleman, *supra* note 2 (noting that for-profit Google will have access to the health data of more than fifty million American patients as a result of a collaboration with Ascension health system).

122. *See, e.g.*, *Fast Facts on U.S. Hospitals, 2020*, AM. HOSP. ASSOC. (Mar. 2020), https://www.aha.org/statistics/fast-facts-us-hospitals (noting that almost 3,000 of the 6,146 hospitals located in the United States are non-profit).

123. American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, § 17932, 123 Stat. 115, 260–263 (codified as amended in scattered sections of 26 U.S.C.).

of unsecured protected health information (uPHI).[124] HHS issued an Interim Breach Notification Rule on August 24, 2009, (Interim Rule)[125] and a final Breach Notification Rule on January 25, 2013.[126] Compliance with the Interim Rule was technically required by September 23, 2009.[127] However, HHS used its technical discretion not to impose sanctions for a failure to make proper notification regarding breaches discovered before February 22, 2010.[128]

The Breach Notification Rule requires covered entities, "following the discovery of a breach of unsecured protected health information" (uPHI),[129] to "notify each individual whose [uPHI] has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach."[130] The notification, which shall be provided without undue delay and within sixty calendar days after the discovery of the breach, shall include (1) a brief description of the nature of the breach, "including the date of the breach and the date of [its] discovery;"[131] (2) "[a] description of the types of [uPHI] . . . involved in the breach;" (3) "[a]ny steps [the] individual[] should take to protect [herself] from potential harm resulting from the breach;"[132] (4) a brief description of the steps taken by the covered entity to investigate the breach, to mitigate harm to individuals whose uPHI was part of the breach, and to protect against future breaches; and (5) contact information sufficient to allow individuals to "ask questions or learn additional information" about the breach.[133]

When a breach involves the uPHI of "more than 500 residents of a [s]tate or jurisdiction," the Breach Notification Rule also requires the covered entity to notify "prominent media outlets serving the [s]tate or jurisdiction."[134] When a breach involves the uPHI of 500 or more individuals, regardless of their state of residency, the covered entity is also required to notify the Secretary of HHS within sixty calendar days after the discovery of the breach.[135] Finally, when the breach involves the uPHI of less than 500 individuals, the covered entity is

124. *Id.*

125. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (Interim Final Rule to be codified at 45 C.F.R. pts. 160 and 164).

126. 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 (Jan. 25, 2013) (codified at 45 C.F.R. pt. 160, 164).

127. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. at 42,753.

128. *Id.* at 42,757.

129. 45 C.F.R. § 164.404(a)(1); *see also id.* § 164.402 (defining breach and uPHI).

130. *Id.* § 164.404(a)(1).

131. *Id.* § 164.404(c)(1)(a)(A).

132. *Id.* § 164.404(c)(1)(a)(C).

133. *Id.* § 164.404(c)(1)(E).

134. *Id.* § 164.406(a).

135. *Id.* § 164.408(b); U.S. DEP'T OF HEALTH & HUM. SERVS., *Submitting Notice of a Breach to the Secretary*, HHS, https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html, (last updated Jan. 15, 2015).

required to notify the Secretary of HHS "not later than [sixty calendar] days after the end of [the] calendar year."[136]

Although several studies referenced in Part II of this Article suggest an uneven relationship between regulation and compliance, Section II.F of this Article examines a study finding that HITECH is associated with a reduction in the number of breaches among business associates[137] and that HITECH "has protected millions of Americans from unwanted privacy exposures."[138] Notwithstanding the imperfect relationship between regulation and compliance, Part III of this Article highlights—and relies on—this finding to support continued health data privacy and security regulation.

II. THE COMPLIANCE LITERATURE

As previewed in Part I, a number of academic, industry, and government studies attempt to assess compliance by covered entities and business associates with all or portions of the HIPAA Rules. These studies are summarized and analyzed below. Part III then addresses the relevance of these studies for future data privacy and security law and policy.

A. The Plain Language Requirement

In its use and disclosure requirements,[139] the HIPAA Privacy Rule requires authorizations for the use and disclosure of PHI to be "written in plain language."[140] One study authored by researchers affiliated with Boston University School of Medicine, Northwestern University Feinberg School of Medicine, Johns Hopkins Berman Institute of Bioethics, and Johns Hopkins Schools of Medicine and Public Health assesses compliance with this plain language requirement.[141] To this end, the study authors searched the websites of the 126 U.S. medical schools then-listed on the Association of American Medical Colleges (AAMC) web page, and between June 2009 and June 2010, obtained HIPAA authorization forms[142] and consent-to-research[143] templates

136. *Id.* § 164.408(c).

137. *See* Niam Yaraghi & Ram D. Gopal, *The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights from an Empirical Study*, 96 MILBANK Q. 144, 161 (2018); *infra* Part II.F.

138. *Id.*

139. *See supra* text accompanying notes 61–70 (summarizing the use and disclosure requirements).

140. 45 C.F.R. § 164.508(c)(3).

141. Michael K. Paasche-Orlow et al., *Readability of Consent Form Templates: A Second Look*, 35 IRB: ETHICS & HUM. RSCH. 12 (2013).

142. *See supra* text accompanying notes 67–70 (discussing when the Privacy Rule requires a covered entity to obtain an individual's prior written authorization before using or disclosing the individual's PHI).

143. Federal regulations outside the HIPAA Rules require researchers to obtain consent from human research participants prior to their research participation. *See* 45 C.F.R. § 46.116 (2019) (establishing general requirements for consent to research); *id.* § 46.117 (regulating consent documentation).

from 100 (79%) and 106 (84%) medical schools' websites respectively.[144] The authors studied the text in these forms and templates and assessed the readability of these forms and templates using the Flesch-Kincaid readability scale, which is automated and available through Microsoft Word.[145]

The study authors found, with respect to the HIPAA authorization forms, that the average reading level was at the 11.6 grade level compared to the average reading level for the consent-to-research forms required by federal research regulations,[146] which was at the 9.8 grade level. The study authors also found that, "[i]n a given medical school, the HIPAA template text is 1.8 grade levels higher than informed consent template text," and that the HIPAA template text of medical schools did not meet the schools' own (internal) readability standards in the vast majority of cases.[147]

The study authors concluded that, "[t]he average reading level of research-related HIPAA template text is much higher than the average reading capacity of U.S. adults and fails to meet these institutions' own stated standards . . . by a large margin."[148] The authors recommended "[m]ore explicit guidance for how to make consent and HIPAA text for research studies easier to read and understand" and "more intense federal supervision."[149] Part III of this Article proposes legislative text that would accomplish these goals.

B. The Access to PHI Requirement

In its individual rights provisions, the Privacy Rule gives patients and insureds a legally enforceable right "to inspect and obtain a copy of [their PHI]."[150] Covered entities must provide patients and insureds with access to their PHI in the form (e.g., paper or electric) and format (e.g., e-mail, flash drive, compact disc, online patient portal) requested if the PHI "is readily producible in [that] form and format."[151] The Privacy Rule does permit covered entities to charge a "reasonable, cost-based [access] fee;" however, the access fee may only include the costs of labor, supplies, and postage.[152] In guidance posted to its website in 2016 (2016 Guidance), HHS stated that covered entities have the option of charging patients and insureds "a flat fee not to exceed $6.50" if they "do not want to go through the process of calculating actual or average . . . costs

144. Paasche-Orlow et al., *supra* note 141, at 12–13.
145. *Id.*
146. *Id.* at 15.
147. *Id.*
148. *Id.* at 17.
149. *Id.* at 18.
150. 45 C.F.R. § 164.524(a)(1).
151. *Id.* § 164.524(c)(2)(i).
152. *Id.* § 164.524(c)(4).

for requests for electronic copies of [ePHI]."[153] Some states more specifically regulate medical record and/or general document access charges through maximum charges codified in statutes or regulations.[154] Recent litigation has further interpreted these requirements and has invalidated some statements made by HHS in its 2016 Guidance.[155]

One study attempts to assess compliance with the Privacy Rule's access to PHI requirement.[156] In a cross-sectional study published in 2018, researchers affiliated with Stanford University, Yale University, the University of California, Davis, and the University of California, San Diego collected medical records release forms from 83 top-ranked U.S. hospitals representing 29 states.[157] The study authors then telephoned each hospital's medical records department to collect information on the health data that are permitted to be requested by patients, the formats of release, as well as access charges and processing times "using a predetermined script to minimize variation and biases across telephone calls."[158] Telephone call respondents were either "employees of the [hospitals'] medical records departments or representatives from an outsourced call center."[159]

The study authors found "discordance" between the information provided by the covered entities on their medical records release forms and the information obtained during the simulated patient telephone calls in terms of information permitted to be requested, formats of release, and costs.[160] In particular, on the medical records release forms, as few as nine hospitals (11%) provided the option of selecting particular categories of PHI to be released and

153. U.S. DEP'T OF HEALTH & HUM. SERVS., *Individuals' Right Under HIPAA to Access their Health Information 45 CFR § 164.524,* HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (last updated Jan. 31, 2020) [hereinafter 2016 Guidance].

154. Alabama has an illustrative statutory provision stating that:

> The reasonable costs of reproducing copies of written or typed documents, or reports shall not be more than one dollar ($1) for each page of the first 25 pages, not more than 50 cents ($.50) for each page in excess of 25 pages, and a search fee of five dollars ($5).

See, e.g., ALA. CODE § 12-21-6.1(b)(2) (2019).

155. *See, e.g.*, Ciox Health, L.L.C. v. Azar, 435 F. Supp. 3d 30, 38 (D.D.C. 2020) (holding that (1) HHS's Post-HITECH Final Rule "compelling delivery of PHI to third parties regardless of the records' format is arbitrary and capricious;" (2) the 2016 Guidance is "a legislative rule that [HHS] failed to subject to notice and comment in violation of the [federal Administrative Procedure Act] APA;" and (3) 2016 Guidance provisions addressing "what labor costs can be recovered . . . is an interpretative rule that HHS was not required to subject to [the APA's] notice and comment" rulemaking process, declaring unlawful and vacating portions of the 2016 Guidance and HHS's Post-HITECH Final Rule); Cross v. Ciox Health, 438 F. Supp. 3d 572 (E.D.N.C. 2020) (concerning additional litigation arising out of the Privacy Rule's right-to-access-PHI provisions).

156. *See* Carolyn T. Lye et al., *Assessment of US Hospital Compliance with Regulations for Patients' Requests for Medical Records*, JAMA NETWORK OPEN (Oct. 5, 2018), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2705850.

157. *Id.* at 2.

158. *Id.*

159. *Id.*

160. *Id.* at 1.

"only 44 hospitals (53%) provided patients the option to acquire [their] entire medical record[s]."[161] During the telephone calls, "all 83 hospitals stated that they were able to release entire medical records to patients."[162]

The study authors also found discrepancies in terms of information given during telephone calls compared to information provided on the medical records release forms between the formats hospitals stated that they could use to release information: "69 [83%] vs 40 [48%] for pick up in person, 20 [24%] vs 14 [17%] for fax, 39 [47%] vs 27 [33%] for email, 55 [66%] vs 35 [42%] for [compact disc], and 21 [25%] vs 33 [40%] for online patient portals."[163] The study authors stated that their findings demonstrated noncompliance with the Privacy Rule provision[164] prohibiting a covered entity from refusing to provide an individual with access to PHI in the form and format requested by the individual.[165]

The study authors also found that forty-eight respondent hospitals had costs of release (as much as $541.50 for a 200-page record) above HHS's 2016 Guidance recommendation of $6.50 for electronically maintained records.[166] In addition, "[a]t least [six] of the hospitals (7%) were noncompliant with state requirements for processing times."[167] The study authors concluded that there are "discrepancies in the information provided to patients regarding the medical records release processes and noncompliance with federal and state regulations and recommendations. Policies focused on improving patient access may require stricter enforcement to ensure more transparent and less burdensome medical records request processes for patients."[168] Part III of this Article proposes new statutory language that would encourage transparency and decrease burden in the context of the right of patients and insureds to access their PHI.

C. The Audit Log and Access Report Requirements

The Security Rule requires covered entities and business associates to "[i]mplement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."[169] The Security Rule also requires covered entities and business associates to "[i]mplement hardware, software, and/or procedural mechanisms

161. *Id.* at 1, 4.
162. *Id.*
163. *Id.* at 4.
164. *See* 45 C.F.R. § 164.524(c)(2)(i).
165. Lye et al., *supra* note 156, at 1–2.
166. *See* 2016 Guidance, *supra* note 153.
167. Lye et al., *supra* note 156, at 1, 6.
168. *Id.* at 2.
169. *See* 45 C.F.R. § 164.308(a)(1)(ii)(D).

that record and examine activity in information systems that contain or use [ePHI]."[170] On the other hand, and with several exceptions, the Privacy Rule (not the Security Rule) gives individuals the "right to receive an accounting of disclosures [but not uses of PHI] . . . made by a covered entity in the six years prior to the date on which the accounting is requested."[171]

One study attempts to investigate compliance with these Security and Privacy Rule requirements, although it is not clear that the study authors correctly understand them. In particular, study authors affiliated with the University of Murcia in Spain reviewed the privacy policies of twenty free, web-based personal health records (PHRs) with available privacy policies and purported to extract and assess privacy and security characteristics according to certain unreferenced standards within the Privacy and Security Rules.[172] The study authors reported that 14/20 (70%) of the PHRs studied allowed individuals access to their PHI as required by the Privacy Rule,[173] whereas 6/20 (30%) did not. The study authors also found, however, that only 2/20 (10%) of the PHRs "provide the individual with the ability to view a log of who has accessed his/her PHR."[174] The study concluded that many of the PHRs do not meet HIPAA standards and that "[s]ome improvements can be made to current PHR privacy policies to enhance the audit and management of access to users' PHRs."[175]

The University of Murcia study has several limitations. First, not all PHRs are regulated by the HIPAA Rules. PHRs that are offered to patients by covered entities are regulated by the HIPAA Rules, whereas PHRs offered to patients by non-covered entities are not regulated by the HIPAA Rules.[176] To the extent that any of the PHRs studied by the University of Murcia authors are not offered by covered entities,[177] the HIPAA Rules do not apply to those PHRs.[178]

170. *Id.* § 164.312(b).

171. *Id.* § 164.528(a)(1).

172. *See* Inmaculada Carrión et. al, *Assessing the HIPAA Standard in Practice: PHR Privacy Policies*, 33rd ANN. CONF. OF THE IEEE EMBS 2380, 2380–83 (Aug.–Sept. 2011).

173. *Id.* at 2382.

174. *Id.* at 2383.

175. *Id.* at 2380.

176. *See* OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., PERSONAL HEALTH RECORDS AND THE HIPAA PRIVACY RULE 1–3 (June 8, 2020) [hereinafter HHS on PHRs].

177. The University of Murcia study authors do not address which PHRs they reviewed are offered by covered entities and which PHRs are not offered by covered entities. *See* Carrión et al., *supra* note 172, at 2380–83. To the extent that some of the PHRs reviewed by the authors are not offered by covered entities, the study authors' claims regarding HIPAA non-compliance are invalid with respect to those PHRs. For example, Doclopedia, one of the PHRs reviewed by University of Murcia study authors, states on its website that, "What about HIPAA Compliance? HIPAA is a government law ensuring the privacy or information about you held by others. The heath records on doclopedia belong to you and therefore do not fall under the jurisdiction of HIPAA." FAQs, DOCLOPEDIA, https://www.doclopedia.com/Faq.aspx (last visited Feb. 28, 2020).

178. HHS ON PHRS, *supra* note 176, at 1–3.

Second, the study authors appear to misunderstand the requirements set forth in the Privacy and Security Rules. Although covered entities have an obligation to review information system activity through audit logs and access reports under the Security Rule,[179] individuals only have a right to request and receive an accounting of disclosures (but not uses) under the Privacy Rule.[180] The study authors appear to think that the Security Rule gives individuals the right to access any audit logs and access reports involving their PHI:

> Does the PHR provide the individual with the ability to view a log of who has accessed his/her PHR?: Only two of the PHRs reviewed (10%) meet this requirement. The majority of the PHRs analyzed (65%) do not allow the individual to see who has accessed his/her data. Our requirements are not being met by the PHRs analyzed.[181]

Part III proposes legislative text that would clarify—and minimize confusion between—typical security standards (e.g., the requirement of covered entities to generate and regularly review audit logs and access reports) and typical privacy rights (e.g., the right of individuals to request and receive an accounting of their PHI disclosures).

A third limitation of the University of Murcia study is that it only examines the PHRs with respect to a few HIPAA standards, ignoring dozens of other important standards. For example, the study authors did not assess the PHRs with respect to the HIPAA Privacy Rule's notice of privacy practices requirement,[182] additional privacy protections requirement,[183] or amendment of incorrect or incomplete PHI requirement.[184] The study authors also did not assess the PHRs with respect to the majority of the administrative, physical, and technical safeguards set forth within the HIPAA Security Rule.[185]

D. Sharing PHI by Text

The individual rights provisions within the Privacy Rule[186] permit the use and disclosure of PHI for treatment purposes without the patient's prior written authorization.[187] For example, the Privacy Rule permits a resident physician to share PHI with a teaching physician if the purpose of the communication is to obtain guidance regarding the treatment of a patient or to otherwise share

179. 45 C.F.R. § 164.308(a)(1)(ii)(D).

180. *Id.* § 164.528(a)(1).

181. Carrión et al., *supra* note 172, at 2383.

182. *See* 45 C.F.R. § 164.520.

183. *See id.* § 164.522.

184. *See id.* § 164.526.

185. *See id.* §§ 164.308–.312.

186. *See supra* Part I.A text accompanying notes 82–88 (discussing the individual rights provisions within the Privacy Rule).

187. 45 C.F.R. § 164.506(c)(1)–(2).

information regarding the treatment of a patient.[188] Likewise, the Privacy Rule permits a teaching physician to share PHI with a resident if the purpose of the data sharing is to train the resident or to assist with the treatment of the patient.[189] With respect to the method of PHI sharing, the Security Rule contains an addressable encryption standard. In particular, the Security Rule requires a covered entity to implement encryption only if, after a risk assessment, the covered entity has determined that encryption is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity, and availability of ePHI.[190] "If the [covered] entity decides that [encryption] is not reasonable and appropriate, [the covered entity] must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate."[191]

Three studies have attempted to assess HIPAA compliance in the context of text messaging, although it is not clear that the authors of (and/or the respondents to) these studies understand the Privacy and Security Rule treatment and encryption provisions discussed above. The first text-messaging study involved a cross-sectional survey of the American Society for Surgery of the Hand membership in March and April 2016.[192] The study authors, affiliated with Vanderbilt University, Brown University, and Johns Hopkins University, found that 63% of the 409 respondent hand surgeons reported that they believe that text messaging does not comply with the Security Rule and that 37% of hand surgeons reported that they do not use text messaging to communicate PHI.[193] According to the study authors, younger surgeons and respondents who believed that their texting complied with the Security Rule were significantly more likely to report text messaging of PHI.[194]

The second text-messaging study, published in 2018 by study authors affiliated with Vanderbilt University, involved three rounds of a direct email survey of U.S.-designated institutional officials (DIOs).[195] DIOs oversee and administer medical residencies and fellowships that are accredited by the Accreditation Council for Graduate Medical Education (ACGME).[196] The survey was designed to investigate electronic communication practices among

188. *See id.* § 164.506(c)(1) (allowing covered entities to use and disclose PHI for treatment).

189. *See id.*

190. *Id.* § 164.308(a)(1)(ii)(A); *id.* § 164.312(a)(2)(iv).

191. *See* OFF. FOR C.R., *Is the Use of Encryption Mandatory in the Security Rule?*, HHS (last updated July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html (explaining the addressable, but not mandatory, encryption standard).

192. Brian C. Drolet et al., *Electronic Communication of Protected Health Information: Privacy, Security, and HIPAA Compliance*, 42 J. HAND SURGERY 411, 411 (2017).

193. *Id.*

194. *Id.*

195. Robert E. Freundlich, et al., *Pagers, Smartphones, and HIPAA: Finding the Best Solution for Electronic Communication of Protected Health Information*, 42 J. MED. SYS. 1, 1 (2018).

196. *Id.*

residents and teaching physicians, not the DIOs.[197] Respondents represented ACGME-accredited programs located in all fifty states, the District of Columbia, and Puerto Rico.[198]

The authors of the second text-messaging study found that more than half of respondent institutions (202/339, 59.6%) still provide medical residents with one-way text pagers for clinical communication, including communication of PHI and ePHI regulated by the Privacy and Security Rules, respectively, while 121/339 (35.7%) of institutions provided a cell phone instead.[199] The study authors also found that more than two-thirds of respondents (231/339, 68.1%) reported that their institutions prohibit text messaging of PHI using personal cell phones.[200] The authors concluded, "There is ongoing debate about the appropriate use of SMS under the [HIPAA] at academic institutions and this is reflected in the survey results."[201]

Interestingly, respondents to the second text-messaging study were evenly split in their beliefs that HIPAA prohibited (167/339, 49.3%) or did not prohibit (172/339, 50.7%) the use of personal cell phones for text messaging of PHI.[202] According to the study authors, "[t]his disparity amongst institutional and academic leaders highlights a concerning lack of clarity on legislation guiding electronic transmission of PHI."[203] In terms of the respondents who believed that text messaging violates the HIPAA Rules, 94/167 (56.3%) answered that their schools only use one-way text paging.[204] The study authors concluded that this "great paradox may represent an inertial phenomenon or miseducation regarding new technology. Regardless, clarification is needed regarding appropriate use parameters for electronic communication."[205]

The third text-messaging study, published in 2016 by authors affiliated with the University of California, San Diego, also purported to study self-reported HIPAA compliance in the context of texting by medical residents, medical fellows, and attending physicians at ACGME-accredited training institutions.[206] This third study involved a digital survey the authors sent to 678 academic medical institutions over a thirty-day period.[207] The study authors reported that 58% of all resident respondents self-reported "violating HIPAA" by sending PHI by text, with 27% reporting they do it "often" or "routinely" compared to

197. *Id.*

198. *Id.*

199. *Id.* at 1–2.

200. *Id.* at 2.

201. *Id.*

202. *Id.*

203. *Id.*

204. *Id.*

205. *Id.* at 3.

206. Randall McKnight & Orrin Franko, *HIPAA Compliance with Mobile Devices Among ACGME Programs*, 40 J. MED. SYS. 1, 2 (2016).

207. *Id.*

15–19% of attending physicians.[208] According to the study authors: (1) 5% of respondents "often" or "routinely" used HIPAA-compliant mobile apps (HCApps) with no significant differences related to training level; (2) 20% of residents admitted to using non-encrypted email at some point; and (3) 53% of attending physicians and 41% of medical residents used encrypted email routinely.[209] The study authors also found that physicians from surgical specialties compared to non-surgical specialties demonstrated higher rates of "HIPAA violations" with text-messaging use (35% vs. 17.7%), standard photo or video messages (16.3% vs. 4.7%), HCApps (10.9% vs. 4.9 %), and non-HCApps (5.6% vs. 1.5%).[210]

The study authors of the third text-messaging study also assessed barriers to the respondents' compliance with the HIPAA Rules. In particular, the authors reported that the most significant self-reported barriers to compliance were inconvenience (58%), lack of knowledge (37%), unfamiliarity (34%), inaccessibility (29%), and habit (24%).[211] The authors concluded:

> Medical professionals must acknowledge that despite laws to protect patient confidentiality in the era of mobile technology, over 50 % of current medical trainees knowingly violate these rules regularly despite the threat of severe consequences. The medical community must further examine the reason for these inconsistencies and work towards possible solutions.[212]

The three text-messaging studies have several limitations, one of which is worth highlighting here. In particular, the text-messaging study authors as well as the study respondents lacked perfect information regarding the prohibitions and permissions set forth in the HIPAA Rules. As explained above, encryption is not a required implementation specification in the Security Rule; instead, encryption is just addressable.[213] Neither the study authors nor the respondents appear to understand the difference between a required and an addressable implementation specification in the Security Rule. The fact that a study respondent uses a non-encrypted technology to share PHI is not an automatic violation of the Security Rule. In addition, the fact that a study respondent shares PHI with a fellow resident or teaching physician for treatment or educational purposes without prior patient permission does not violate the Privacy Rule.[214] In fact, the Privacy Rule expressly permits health care providers,

208. *Id.* at 1.

209. *Id.*

210. *Id.*

211. *Id.*

212. *Id.*

213. 45 C.F.R. §§ 164.312(a)(2)(iv), 164.312(e)(2)(ii).

214. *See* 45 C.F.R. § 164.506(c)(1) (permitting a covered entity to use and disclose PHI for treatment purposes without the patient's prior written authorization); *id.* § 164.506(c)(2) (permitting a covered entity to disclose PHI to another health care provider for the recipient provider's treatment activities without the patient's prior written authorization); *id.* § 164.506(c)(1) (permitting a covered entity to use or disclose PHI for health care operations activities without the patient's prior written authorization); *id.* § 164.501 (defining

including residents and teaching physicians, to share PHI for treatment purposes and for educational purposes.[215]

To this end, the residents', fellows', and teaching physicians' self-reports of their beliefs regarding their behaviors (e.g., that they believe they are texting using HCApps or non-HCApps, or that they believe that they are violating the HIPAA Rules or are not violating the HIPAA Rules) may be accurate; however, their beliefs regarding whether their behaviors comply with the HIPAA Rules, or whether particular technologies comply with the HIPAA Rules, may be incorrect. Part III proposes legislative text designed to: (1) address the lack of understanding regarding permissible disclosures for treatment between and among health professional trainees and teaching faculty; (2) improve understanding of the encryption standard set forth in the Security Rule; and (3) respond to the third text-messaging study's finding that HIPAA compliance is hindered by health care providers' lack of knowledge of, unfamiliarity with, and inability to access the HIPAA Rules.

E. General Compliance Data

In Parts II.A–II.D, above, study authors affiliated with prestigious academic institutions investigated certain entities' compliance with particular provisions within the HIPAA Rules. In addition to academic studies, professional associations and trade groups also have sought to study HIPAA compliance, but the focus of these studies is on compliance with the HIPAA Rules in general. Less than one year after most covered entities were required to comply with the Privacy Rule, for example, the American Health Information Management Association (AHIMA) sent an email to AHIMA members "who were considered most likely to have participated significantly in the HIPAA implementation process and to non-members who had participated in various HIPAA-related educational opportunities provided by AHIMA."[216] AHIMA received 1,192 qualified responses, 56% of which came from individuals working in the hospital setting.[217] The other responses came from individuals who work in non-hospital settings, such as physician offices, behavioral health care clinics, home health agencies, and long-term care facilities such as nursing homes.[218] In terms of geographic diversity, qualified responses were received from all fifty states, the District of Columbia, and

health care operations to include "training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers . . .").

215. *See* 45 C.F.R. §§ 164.506(c)(1)–(2), 164.501.

216. AM. HEALTH INFO. MGMT. ASS'N, THE STATE OF HIPAA PRIVACY AND SECURITY COMPLIANCE 12–13 (2004) [hereinafter AHIMA 2004].

217. *Id.* at 13.

218. *Id.*

Puerto Rico.[219] Of the 1,192 qualified respondents: (1) 58% were designated privacy or security officials; (2) 11% were functioning as privacy or security officials without formal titles; and (3) the remaining 31% served on HIPAA privacy and security teams or committees but were neither designated officials nor functioning as such officials.[220]

After analyzing the data it received, AHIMA stated in an April 2004 report that: (1) 23% of respondents felt their organizations were "fully compliant" with the Privacy Rule; (2) 68% of respondents felt their organizations were "currently between 85 to 99 percent compliant;" and (3) 8% of respondents reported being "50 percent or less compliant at this time."[221] Seventy percent of survey respondents agreed that attempts to comply with the Privacy Rule uncovered privacy problem areas within their organizations.[222] Two of the most common "problem areas" identified by AHIMA related to the lack of standardized practices for the release of PHI in accordance with 45 C.F.R. § 164.524 within the Privacy Rule's individual rights provisions[223] and public access to PHI in accordance with 45 C.F.R. § 164.510 within the Privacy Rule's use and disclosure requirements.[224]

When asked by AHIMA about difficulties associated with HIPAA compliance, "no single area was identified by more than 39 percent of respondents."[225] However, four areas emerged as more problematic than all of the other areas: (1) the accounting of disclosures requirement under 45 C.F.R. § 164.528 (39%);[226] (2) obtaining PHI from other providers as permitted by 45 C.F.R. § 164.506(c) (33%); (3) access and release of information to relatives or significant others pursuant to 45 C.F.R. § 164.510 (32%); and (4) the business associate requirements set forth in 45 C.F.R. §§ 164.502–.504 (25%).[227]

Three years after most covered entities were required to comply with the Privacy Rule, AHIMA conducted a second study that essentially repeated the study conducted two years earlier.[228] In the second study, published in 2006, AHIMA found that nearly 39% of hospitals and health systems self-reported "full privacy compliance," a "considerable increase" over the 23% finding from

219. *Id.*

220. *Id.*

221. *Id.* at 5.

222. *Id.*

223. *See supra* Part II.B at text accompanying notes 150–154 (discussing the individual rights provisions within the Privacy Rule).

224. *See supra* Part I.A at text accompanying notes 65–66 (discussing 45 C.F.R. § 164.510 within the Privacy Rule's use and disclosure requirements).

225. AHIMA 2004, *supra* note 216, at 5.

226. *See supra* text accompanying note 90 (providing detailed information regarding the accounting of disclosures requirement).

227. AHIMA 2004, *supra* note 216, at 5.

228. AM. HEALTH INFO. MGMT. ASS'N, THE STATE OF HIPAA PRIVACY AND SECURITY COMPLIANCE, 2006 (2006) [hereinafter AHIMA 2006].

the 2004 study.[229] "[F]ifty-five percent of respondents indicated that resources are their most significant barrier to full privacy compliance."[230] AHIMA also found that, in the two years since its first study, "a lack of resources and competing priorities have led some hospital and health system staff to slack off regarding all aspects of the privacy rule."[231]

With respect to the particular relationship between financial resources and HIPAA compliance, AHIMA found in its second study that financial resources "appear[] to impact the level of privacy training and monitoring that a privacy officer or staff are capable of providing."[232] Privacy officers report sensing a loss of support from senior management, both in ensuring the facility staff is aware of the need for privacy as well as ensuring sufficient budgeting for education.[233] With respect to whether the passage of three years had made HIPAA compliance more manageable, "most providers [grew] accustomed to the various provisions" in the Privacy Rule; however, the accounting of disclosures requirement codified within the Privacy Rule's individual rights provisions[234] still proved difficult for many respondents.[235] The second AHIMA study reported that when a patient requested an accounting of disclosures, the accounting was burdensome and difficult for providers to produce.[236] In addition, few patients actually requested accountings, suggesting little patient return on the significant provider investment in developing a process to produce, and actually producing, accountings of disclosures.[237]

The 2004 and 2006 AHIMA studies have several limitations. First, the compliance data collected and analyzed by AHIMA were self-reported by the respondent hospitals and health systems.[238] Given the dozens of standards set forth in the Privacy and Security Rules and the lack of perfect legal and compliance knowledge on the part of the respondent covered entities not trained in law, self-reported data (in this context) should be viewed with skepticism. HIPAA compliance is an ongoing concern, and non-compliance is not readily detectable by one individual at any point in time. In addition, a majority of the AHIMA study respondents were affiliated with hospitals,[239]

229. *Id.* at 3.

230. *Id.*

231. *Id.*

232. *Id.*

233. *Id.*

234. *See supra* Part I.A at text accompanying note 86 (referencing the accounting of disclosures requirement).

235. AHIMA 2006, *supra* note 228, at 3.

236. *Id.* at 3.

237. *Id.*

238. *See* AHIMA 2004, *supra* note 216, at 5 (noting, for example, that "68 percent of respondents feel their facilities are currently between 85 to 99 percent compliant while only 8 percent report being 50 percent or less compliant at this time.") (underlined emphasis added); AHIMA 2006, *supra* note 228, at 6 (noting that data are "as reported by the respondents").

239. AHIMA 2004, *supra* note 216, at 4; AHIMA 2006, *supra* note 228, at 3.

leaving other types of covered entities (e.g., health plans, health care clearinghouses, and non-hospital health care providers) unstudied.

In addition to general compliance data reported by AHIMA, the federal government also has released to the public reports assessing HIPAA compliance as well as enforcement data.[240] In a compliance report covering years 2015, 2016, and 2017 (2018 Report), for example, HHS summarily discusses: (1) the number of HIPAA-related complaints received by HHS from the public; (2) the number of complaints resolved informally, a summary of the types of complaints so resolved, and the number of covered entities that received technical assistance from HHS during each of the three years covered by the report; (3) the number of complaints that have resulted in the imposition of civil money penalties or that have been resolved through monetary settlements, including the nature of the complaints involved and the amount paid in each penalty or settlement; (4) the number of compliance reviews HHS conducted and the outcome of each such review; (5) the number of subpoenas or inquiries issued by HHS relating to HIPAA; (6) the number of HIPAA audits performed as required by HITECH; and (7) HHS's plan for improving HIPAA compliance and enforcement going forward.[241] In addition to the information set forth in its 2018 Report, HHS also makes available on its website a significant amount of complaint and enforcement data that are current through January 31, 2020.[242]

These reports and data reveal that the compliance issues that are investigated most by HHS are, in order of frequency: (1) the impermissible use and disclosure of PHI as prohibited by 45 C.F.R. §§ 164.502–.514 of the Privacy Rule; (2) a lack of safeguards of PHI as required by 45 C.F.R. § 164.530(c) of the Privacy Rule; (3) a lack of patient access to PHI as required by 45 C.F.R. § 164.524 of the Privacy Rule; (4) a lack of administrative safeguards for ePHI as required by 45 C.F.R. § 164.308 of the Security Rule; and (5) the use or disclosure of more than the minimum necessary amount of PHI as prohibited by 45 C.F.R. § 164.502(b) of the Privacy Rule.[243] These reports and data also reveal that the types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency, general hospitals, private practices and physicians, outpatient facilities,

240. *See, e.g.*, OFF. FOR C.R.., U.S. DEP'T HEALTH & HUM. SERVS., REPORT TO CONGRESS ON HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION RULE COMPLIANCE FOR CALENDAR YEARS 2015, 2016, AND 2017 2 (2018), https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2015-2016-2017.pdf [hereinafter HHS 2018] (responding to section 13424(a) of HITECH, which required HHS to prepare and submit an annual report to three congressional committees addressing compliance with the Privacy, Security, and Breach Notification Rules); OFF. FOR C.R., *Enforcement Highlights*, U.S. DEP'T HEALTH & HUM. SERVS. (last updated Sept. 11, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html [hereinafter HHS 2020] (providing the public with HIPAA compliance and enforcement data current through July 31, 2020).

241. HHS 2018, *supra* note 240, at 2.

242. HHS 2020, *supra* note 240.

243. *Id.* at *Enforcement Highlights*.

pharmacies, and health plans.[244] Part III of this Article uses these findings to suggest privacy and security requirements that should be prioritized in new or expanded legislation.

In addition to compliance reports and enforcement data, HHS also has made available to the public information regarding HHS's HIPAA compliance audits.[245] In 2011, HHS began auditing covered entities for compliance with the HIPAA Rules.[246] Since 2011, HHS has audited 115 and 166 covered entities through its first and second rounds of HIPAA audits, respectively.[247] Although HHS's audit results are helpful to academics and practitioners who wish to understand enforcement trends, the audits can neither be understood as a meaningful deterrent of HIPAA Rules violations nor as generalizable to the millions of covered entities across the United States.[248] That said, HHS found through its HIPAA compliance audits that 65% of the covered entities audited had significantly deficient notices of privacy practices in violation of the Privacy Rule and that 89% of covered entities had inadequate access to their PHI, also in violation of the Privacy Rule.[249] Part III proposes legislative text designed to assist regulated entities in drafting their privacy policies and improving patient and insured access to health data.

F. Effect of HITECH on Business Associates

Parts II.A through II.E, above, have focused on compliance with the HIPAA Rules by covered entities. Compliance with the HIPAA Rules by business associates[250] also has been studied. Recall that HITECH extended the application of the use and disclosure requirements within the HIPAA Privacy Rule and the administrative, physical, and technical safeguards within the HIPAA Security Rule to business associates.[251] HITECH also obligated

244. *Id.*

245. *See, e.g.*, Dennis P. Begley, *April 14th Has Passed and You're Not HIPAA Compliant. . .Now What?*, HEARING REV. (Apr. 9, 2003), https://www.hearingreview.com/practice-building/marketing/april-14th-has-passed-and-youre-not-hipaa-compliant-now-what (last visited Sept. 11, 2020) (noting that there are "literally millions of covered entities in the country").

246. *See* OFF. FOR C.R., *HIPAA Privacy, Security, and Breach Notification Audit Program*, HHS (Dec. 1, 2016), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html [hereinafter *HHS Audits*] (providing information to the public about HHS's HIPAA compliance audits). *See generally* Tovino, *A Timely Right to Privacy*, *supra* note 44 (discussing these audits).

247. *HHS Audits*, *supra* note 246 (stating the number of covered entities (115) audited during HHS's first, or pilot, audit phase); Drew Gantt et al., *Preliminary Results for Covered Entities Participating in the Phase 2 HIPAA Audit Program*, HEALTH L. STAT. (Dec. 20, 2017), https://www.healthcarestat.com/2017/12/preliminary-results-covered-entities-participating-phase-2-hipaa-audit-program (stating the number of covered entities (166) audited during HHS's second audit phase).

248. *See, e.g.*, Begley, *supra* note 245 ("With literally millions of covered entities in the country, the odds of a random audit are slim.").

249. *See, e.g.*, Gantt et al., *supra* note 247 (providing these statistics).

250. *See supra* text accompanying note 25 (defining business associate).

251. *See* HITECH § 13404(a).

business associates to adhere to certain notification procedures in the event of a breach of uPHI.[252] One study attempts to empirically examine the effects of HITECH's direct regulation of business associates on the frequency of privacy breaches by business associates. The particular goal of this study, published in 2018 by authors affiliated with the University of Connecticut and the Brookings Institution, was to shed light on whether and how shifts in regulatory application protect patient privacy.[253] To this end, the study authors used data made publicly available by HHS's Office for Civil Rights (OCR) on breaches of uPHI that occurred between October 2009 and August 2017.[254] During the time period studied, 2,010 uPHI breach incidents occurred, 291 of which occurred among business associates.[255] The remaining incidents occurred among covered entities, including covered health care providers (1,410 incidents), health plans (253 incidents), and health care clearinghouses (4 incidents).[256] Fifty-two incidents were not categorized as involving a covered entity or business associate.[257]

The study authors found that HITECH "had a strong and immediate effect on reducing the number of breaches among business associates by 14.41 units."[258]

> Our results indicate that implementation of the [HITECH] rules could have led to a significant decrease in the number of incidents and thus has protected millions of Americans from unwanted privacy exposures. Therefore, we conclude that the federal policy appears to have achieved its intended goal of enhancing privacy protection efforts and reducing the number of breach incidents among business associates.[259]

Although some of the studies discussed above show that not all covered entities comply with all provisions in the HIPAA Rules, Part III of this Article relies on the HITECH study to support continued health data privacy and security regulation. Stated another way, this HITECH study suggests that regulation is associated with compliance and, perhaps, increased data privacy and security protection.

G. Factors Influencing Compliance

Parts II.A through II.F, above, reference studies investigating rates of compliance by covered entities and business associates with the HIPAA Rules.

252. *Id.* § 13402(b).
253. Yaraghai & Gopal, *supra* note 137, at 144.
254. *Id.* at 144, 147.
255. *Id.* at 149.
256. *Id.*
257. *Id.*
258. *Id.* at 153.
259. *Id.* at 161.

Additional studies attempt to investigate the factors that influence compliance with the HIPAA Rules. Using data from the 2003 Health Information and Management Systems Society (HIMSS) Analytics Database, study authors affiliated with Dartmouth College, Vanderbilt University, and the University of Texas, Houston School of Public Health studied compliance with the Privacy and Security Rules by 3,221 non-federal, medium and large, acute-care hospitals in 2003, which was the initial year of mandatory compliance for the HIPAA Privacy Rule and the initial year of voluntary, but not mandatory, compliance for the HIPAA Security Rule.[260]

The study authors found that approximately two-thirds of hospitals self-reported that they had achieved mandatory compliance with the HIPAA Privacy Rule in 2003, with for-profit hospitals being significantly more likely than non-profit hospitals to be compliant.[261] "In contrast, only 16 percent of hospitals" studied self-reported that they had achieved voluntary compliance with the HIPAA Security Rule in 2003, "with for-profit hospitals being significantly less likely to be early compliant than not-for-profit hospitals."[262] "Consistent with a market logic," the authors suggested that, in 2003, for-profit hospitals were probably "less likely than not-for-profit[] [hospitals] to invest in costly compliance activities with unclear benefits" with respect to the Security Rule because compliance was not yet required, but "more likely to devote resources to mandatory compliance" with respect to the Privacy Rule that same year.[263]

The study authors also found that hospitals that were located in competitive markets were more likely to engage in voluntary compliance with the Security Rule.[264] With respect to this finding, the authors suggested that perhaps these hospitals saw a competitive advantage in achieving early security compliance or were interested in gaining recognition as a technology leader in a competitive market.[265] The study authors formally concluded that "organizational strategies and institutional environments influence hospital compliance," thus "contributing to compliance variation across the U.S. health care system."[266]

This study has several limitations. As with other studies referenced in this Article, the compliance data analyzed by the authors were self-reported by the respondent covered entities. Given the dozens of standards set forth in the Privacy and Security Rules and the lack of legal knowledge and compliance

260. Denise L. Anthony, et al., *Institutionalizing HIPAA Compliance: Organizations and Competing Logics in U.S. Health Care*, 55 J. HEALTH & SOC. BEHAV. 108, 114 (2014).

261. *Id.* at 116.

262. *Id.*

263. *Id.* at 117.

264. *Id.* at 118.

265. *Id.* at 118–19.

266. *Id.* at 108.

knowledge on the part of the covered entities, self-reported data (in this context) should be viewed with skepticism.

Second, the non-lawyer study authors made a legal error that impacted their study design and may have impacted the reliability of their results. Recall that all covered health care providers (regardless of size) were required to comply with the Privacy Rule by April 14, 2003.[267] Small health plans (i.e., those health plans with $5 million or less in annual receipts) had one additional year to comply (i.e., not until April 14, 2004).[268] The study authors misunderstood these rules, thinking that the later (2004) deadline applied to small health care providers, not small health plans: "[B]ecause the HIPAA regulations gave small hospitals extended time to achieve compliance, we restrict our analysis to hospitals with 50 or more beds (n = 3,321)."[269] Therefore, the study authors incorrectly excluded small hospitals from their study. That said, the study authors' findings that medium and large for-profit hospitals are less likely to engage in voluntary (or early) compliance with privacy and security rules suggests that new privacy and security legislation applicable to for-profit entities acquiring health data at a rapid rate, such as Google, should contain earlier (i.e., non-extended) compliance deadlines.

Third, the study authors only included acute-care hospitals in their study.[270] The Privacy and Security Rules apply to dozens of other types of health care provider entities that electronically bill public and private insurers, including most specialty hospitals, nursing homes, home health agencies, hospices, durable medical equipment providers, physician clinics, health care clearinghouses, and health plans, just to name a few.[271] The study authors' findings are thus limited to non-small, acute-care hospitals and are not generalizable to all covered entities, and post-HITECH, to all business associates.

H. Investment in Security Compliance

One study attempts to particularly investigate the factors that influence investment in data security compliance. "[D]rawing upon the resource-based view (RBV) of the firm," authors affiliated with the University of Texas at Dallas, the University of British Columbia, and Yonsei University in South Korea "examined the nature of organizational resources deployed for better

267. *See supra* text accompanying note 93.

268. *See supra* text accompanying notes 94–95.

269. Anthony et al., *supra* note 260, at 114.

270. *See id.* at 109 ("This article examines compliance with the HIPAA Privacy and Security Rules among medium and large acute-care hospitals . . . .").

271. *See* 45 C.F.R. § 160.103 (broadly defining health care provider).

security"—that is, information security control resources (ISCR).[272] The study authors defined ISCR to include three distinct but interrelated sets of resources, including information security technologies (i.e., tangible resources), qualified information security personnel (i.e., human resources), and security awareness of organizational users (i.e., intangible resources).[273] The study authors posited that "organizations heterogeneously respond to institutional pressures related to information security by making different levels of investment in ISCR."[274]

Based on data collected through a survey of one individual at each of 241 small and large for-profit organizations set in a variety of industries including, but not limited to, the health care industry, the study authors found that "[i]nstitutional pressures and internal security needs assessment[s] (ISNA) significantly explain the variation in organizational investment in ISCR."[275] According to the study authors, coercive pressures such as the HIPAA Rules and the European Union General Data Protection Regulation as well as normative pressures (i.e., beliefs regarding what is appropriate among members of social networks) were "found to have not only a direct impact but also an indirect impact through ISNA on organizational investment in ISCR."[276]

With respect to coercive pressures, the study authors specifically stated that they "influenc[ed] an organization's decision to invest in ISCR. This result is consistent with the emerging view that government regulations significantly affect organizations' information security practices."[277] According to the study authors, "coercive pressure has a strong effect on ISNA. Coercive pressure from government regulatory agencies and business partners seems to be successful in making a business case for organizational investment in ISCR and in determining how to address information security risks."[278]

The study authors also found that "coercive pressure has a significant impact on information security technologies [i.e., tangible resources] and qualified security personnel [i.e., human resources] but not on security awareness of organizational users [i.e., intangible resources]"[279]:

> This is presumably because government regulations and requests from business partners generally focus on security technologies and standards. To comply with such government regulations and business partner requests, we would expect that organizations also need to invest in qualified information security personnel with expertise and skills. However, such regulations and

272. Huseyin Cavusoglu et al., *Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources*, 52 INFO. & MGMT. 385, 385 (2015).

273. *Id.* at 386.

274. *Id.*

275. *Id.* at 385.

276. *Id.* at 385, 395–96.

277. *Id.* at 395.

278. *Id.* at 395–96.

279. *Id.* at 396.

> requests did not have a direct impact on the extent of security awareness of knowledge workers in our sample organizations.[280]

This study has a number of limitations in terms of its contributions to the HIPAA compliance literature. For example, it is not clear from the published study how many of the respondent organizations were required to comply with the HIPAA Rules and which provisions within the HIPAA Rules (e.g., the administrative safeguards, the technical safeguards, the physical safeguards, the use and disclosure requirements, the individual rights, or the administrative requirements) were found to have applied coercive pressure to the HIPAA-regulated respondents. In addition, the study contains little discussion of the laws, or the content of such laws, that allegedly provided coercive pressure to the studied organizations.

I. Professional Discourse about Privacy Compliance

Finally, one study investigates health care professionals' discourse about patient privacy, including the definition and importance of patient privacy in health care as well as the role of data privacy in day-to-day work. This study has interesting insights in terms of the impact of HIPAA (compared to longstanding privacy norms) on the behavior of different types of health care and health information professionals. In particular, authors affiliated with Dartmouth College and Union College "conducted in-depth, semi-structured interviews" with a total of eighty-three individual respondents, including thirty physicians, thirty-one nurses, and twenty-one health-information professionals.[281] The respondents were affiliated with "two academic medical centers and one veteran's administration hospital/clinic" in the U.S. Northeast.[282] "Interview responses were qualitatively coded for themes and patterns across groups were identified."[283]

The study authors reported privacy discourse differences across the health professional groups.[284] In particular, the study authors noted that the health information professional respondents actively adopted legal standards, whereas the physician and nurse respondents were more likely to resist or be neutral regarding legal changes.[285] For example, one health information professional respondent stated that health information professionals "very strictly live and die by HIPAA . . . . It is a big deal, and it's very well respected, and everybody

280. *Id.*

281. Denise L. Anthony & Timothy Stablein, *Privacy in Practice: Professional Discourse about Information Control in Health Care*, 30 J. HEALTH ORG. & MGMT. 207, 207 (2016).

282. *Id.*

283. *Id.*

284. *Id.* at 207, 211.

285. *Id.* at 212–15.

is very conscious of it."[286] In comparison, one nurse stated, "A patient has a right to receive medical care and have his privacy maintained. There is a federal law [HIPAA] that addresses it. There are other laws that address it."[287]

When specifically asked by the study authors about how new laws governing health information, including the Privacy Rule, affect privacy, some respondents stated that such laws did not change anything. For example, one physician respondent stated, "I just continue what I have always done [regarding patient privacy]."[288] Similarly, one nurse respondent stated, "I think you use your best judgment as a professional [regarding patient privacy]."[289] Other respondents stated that HIPAA and other laws "highlighted the importance of patient privacy, but did not necessarily or dramatically change [their] practices":[290] "I think HIPAA introduced that we have to get serious about [patient privacy]."[291] Still other respondents "felt that new legal regulations actually undermined existing professional ethics and practices of privacy in health care by inserting federal law over and above the professional standards that already existed": "The law [HIPAA] suggests to the patient that before this, physicians weren't respecting [privacy], and now they have to because it's the law. I think that is absolutely not accurate."[292] This study suggests that professions with longstanding ethical standards relating to patient privacy and health information confidentiality may not view new rules as behavior altering. However, companies such as Google that are new to health care may respond more favorably.

III. LEGISLATIVE PROPOSALS

A. Future Compliance Studies, Compliance Audits, Non-Compliance Investigations, and Rules Enforcement

This Article has carefully reviewed academic, industry, and government studies and reports that assess compliance with the Privacy, Security, and Breach Notification Rules. Insights that may be drawn from these studies relate to the extent to which not all covered entities comply with the Privacy Rule's plain language requirement, the Privacy Rule's access to protected health information requirement, the Security Rule's addressable encryption standard, and the Security Rule's audit logs and access reports requirement. Additional insights relate to the extent to which covered entities and business associates

286. *Id.* at 214.
287. *Id.*
288. *Id.* at 218.
289. *Id.*
290. *Id.*
291. *Id.*
292. *Id.*

believe they are complying with the Privacy and Security Rules when they are not, the positive impact of HITECH on lessening data breaches by business associates, the varied organizational strategies and institutional environments that positively influence compliance, the extent to which institutional pressures and internal security needs assessments influence investment in security compliance, and professional discourse about patient privacy.

The studies referenced in this Article do have several limitations that impact their generalizability and are worth noting. Most of the available studies focus on compliance by a limited group of regulated actors or institutions, such as medium and large acute-care hospitals,[293] top-ranked hospitals,[294] medical schools,[295] academic medical centers,[296] small and large for-profit organizations,[297] hand surgeons,[298] companies offering personal health records,[299] and business associates.[300] However, other studies (or data sets) focus on (or could be used to assess) compliance by a wider range of regulated actors and institutions.[301] Many of the studies focus on particular uses and disclosures of PHI, such as uses and disclosures of PHI through personal health records[302] and text messaging,[303] but not on other ways in which PHI is used or disclosed on a daily basis. Some studies focus on particular provisions within the HIPAA Rules, such as the plain language authorization requirement in the Privacy Rule[304] and the access to PHI requirement, also in the Privacy Rule.[305] The narrow classes of respondents and the discrete regulatory provisions studied affect the generalizability of these research findings.

The HIPAA compliance literature is not as robust as one might expect, especially given the length of time since the general compliance date for the Privacy Rule (i.e., seventeen years), the Security Rule (i.e., fifteen years), and the Breach Notification Rule (i.e., eleven years). In addition to limitations inherent in studies of this type (e.g., limitations regarding the number of respondents, the type of respondents, the survey questions and/or the availability of data, and the self-reported nature of much of the data), the non-lawyer authors' study designs and data analyses were significantly impacted by the authors' and/or

293. *See* Anthony et al., *supra* note 261, at 109.

294. *See* Lye et al., *supra* note 156, at 1–2.

295. *See* Paasche-Orlow et al., *supra* note 141, at 12–13.

296. *See* McKnight & Franko, *supra* note 206; Freundlich et. al, *supra* note 195.

297. *See* Cavusoglu et al., *supra* note 272.

298. *See* Drolet et al., *supra* note 192.

299. *See* Carrión et al., *supra* note 172.

300. *See* Yaraghi & Gopal, *supra* note 137.

301. *See* AHIMA 2004, *supra* note 216; AHIMA 2006, *supra* note 228; HHS 2018, *supra* note 240; HHS 2020, *supra* note 240.

302. *See* Carrión et al., *supra* note 172.

303. *See* Drolet et al., *supra* note 192; Freundlich et al., *supra* note 195; McKnight & Franko, *supra* note 206.

304. *See* Paasche-Orlow et al., *supra* note 141.

305. *See* Lye et al., *supra* note 156; Carrión, et al., *supra* note 172.

the respondents' lack of perfect information regarding the Privacy and Security Rules and/or their institutions' actual compliance with such rules.

Going forward, academic, industry, and government researchers investigating HIPAA compliance should attempt to study the compliance of health plans, health care clearinghouses, and non-hospital or non-academic medical-center covered entities, which have been largely ignored by the literature to date. Researchers who are intimately familiar with the proper application of the HIPAA Rules should develop, lead, and/or participate in these studies so as to avoid errors in study design. Note that none of the studies or reports referenced in this Article, other than the studies conducted by HHS itself, included a lawyer as an author. Given that the HIPAA Rules are federal regulations, studies interpreting and applying the HIPAA Rules may require attorney design and implementation assistance.

Most importantly, future researchers should attempt to obtain and evaluate non-self-reported compliance data. Other than the compliance data obtained and analyzed by HHS through its enforcement efforts and audit initiatives, most of the academic and industry compliance data were self-reported by the respondent covered entities and business associates. In the context of data privacy and security, covered entities and business associates have a significant interest in self-reporting that they comply with federal regulations given that such regulations are enforceable through civil and criminal penalties. Self-reported data should be interpreted with knowledge of this self-interest and weighed accordingly.

Given its lack of self-interest and its superior knowledge regarding the content and interpretation of its own Rules, HHS is perhaps in the best position to conduct compliance research going forward. However, it should be noted that HHS's past enforcement efforts and compliance research are very limited when viewed in light of the thousands of HIPAA complaints filed since the compliance dates for the various HIPAA Rules and the millions of covered entities located in the United States.[306] In a recent study, for example, the Author of this Article found that a timely-filed consumer complaint involving an actual violation of the HIPAA Rules over which HHS has jurisdiction has a one-tenth of one percent (.1%) chance of triggering a settlement or civil money penalty.[307] The Author also showed that in those few cases that go to settlement or penalty, the federal government takes a significant amount of time—more than seven years in some cases—to execute the settlement agreement or to impose the civil money penalty.[308] The Author concluded that federal desire and/or capacity to enforce the HIPAA Rules appears to be low, resulting in a

306. *See generally* Tovino, *A Timely Right to Privacy*, *supra* note 44 (critiquing HHS's enforcement efforts in the context of health data privacy and security breaches).

307. *Id.* at 1406.

308. *See id.* at 1388–90.

lack of timely attention to the privacy and security rights of individuals.[309] Earlier in this Article, the Author also showed that HHS has audited fewer than 300 covered entities even though millions of covered entities are located in the United States.[310] To respond to these limitations, this Article formally proposes that new or expanded data privacy and security legislation must be supported by federal appropriations that are sufficient to cover the costs associated with meaningful compliance research, more robust compliance audits, more timely compliance investigations, and more frequent enforcement of non-compliance.

B. New or Expanded Privacy and Security Legislation

This Article opened by identifying a number of recent health data acquisitions,[311] investigations,[312] lawsuits,[313] and rulings[314] suggesting that new or expanded health data privacy and security legislation would be both timely and appropriate. In late fall 2019, for example, Google announced plans to acquire Fitbit (a wireless-enabled wearable technology that collects and measures data such as the number of steps walked, heart rate, quality of sleep, steps climbed, and other personal metrics) in a record $2.1 billion deal.[315] With this acquisition, Google not only expanded its current lineup of hardware products, which already included smartphones, tablets, laptops, and smart speakers, but also collected a significant amount of new health data.[316]

Also in late fall 2019, the American public learned that Ascension, the second largest health system in the United States, disclosed the identifiable health information of approximately fifty million patients to Google without the patients' prior authorization.[317] A few months before that, a private plaintiff, on behalf of a class of patients treated at the University of Chicago Medical Center (UC) between 2009 and 2016, sued UC for disclosing allegedly identifiable patient information to Google without the prior written authorization of the patients who were the subjects of that information.[318] In a final illustrative example, the U.K. Information Commissioner's Office recently

309. *See id.* at 1406.

310. *See* OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION AUDIT PROGRAM (2016), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html [hereinafter HHS Audits] (stating the number of covered entities (115) audited during HHS's first, or pilot, audit phase); Drew Gantt et al., *supra* note 247 (stating the number of covered entities (166) audited during HHS's second audit phase).

311. *See, e.g.*, Wakabayashi & Satariano, *supra* note 1.

312. *See, e.g.*, Copeland & Needleman, *supra* note 2.

313. *See, e.g.*, Class Action Complaint and Demand for a Jury Trial, Dinerstein v. Google et al., No. 1:19-cv-04311 (N.D. Ill. June 26, 2019) [hereinafter University of Chicago Lawsuit].

314. *See, e.g.*, ICO Letter, *supra* note 4.

315. *See* Wakabayashi & Satariano, *supra* note 1.

316. *See id.*

317. *See* Copeland & Needleman, *supra* note 2.

318. *See* University of Chicago Lawsuit, *supra* note 313.

ruled that the Royal Free National Health Service Foundation Trust failed to comply with the U.K.'s Data Protection Act when it provided the information of 1.6 million patients to DeepMind, a London-based artificial intelligence lab owned by Google's parent company, without prior patient authorization.[319]

In response to these health data acquisitions, investigations, lawsuits, and rulings, federal and state lawmakers in the United States quickly introduced new data privacy and security bills.[320] On December 12, 2018, for example, Senator Brian Schatz (D-HI) introduced the Data Care Act (DCA), which would establish duties of care, loyalty, and confidentiality for online service providers that handle personal data.[321] Six months later, Senator Amy Klobuchar (D-MN) introduced the Protecting Personal Health Data Act (PPHDA), which would direct the Secretary of HHS to promulgate regulations that would "strengthen privacy and security protections for consumers' personal health data that is collected, processed, analyzed, or used by consumer devices, services, applications, and software."[322]

On October 17, 2019, Senator Ron Wyden (D-OR) introduced the Mind Your Own Business Act (MYOBA), which would require the FTC to promulgate regulations obligating certain entities to "implement reasonable cyber security and privacy policies, practices, and procedures to protect personal information."[323] In a final illustrative example, on November 28, 2019, Senator Bill Cassidy (R-LA) introduced the Smartwatch Data Act, which would prohibit certain entities that collect consumer health information (CHI)[324] from disclosing CHI to information brokers who collect or analyze CHI for profit.[325]

As noted in the Introduction to this Article, these legislative proposals beg several important questions. Foremost is whether newly regulated entities will actually comply with these laws. Additionally, other questions must be answered: (1) Whether the provisions within these laws are likely to cause confusion among regulated entities, resulting in regulatory avoidance or non-compliance; (2) whether any of the provisions in these bills should be strengthened; and (3) whether any provisions should be removed, either because they are unlikely to improve data privacy or security or because they will be difficult or impossible to enforce.

Prior scholars writing in the area of health data privacy and security have impliedly assumed, without testing, that new or expanded legislation or

319. *See* ICO Letter, *supra* note 4.

320. *See, e.g.*, Protecting Personal Health Data Act, S.1842, 116th Cong. (2019) (directing the Secretary of the federal Department of Health and Human Services to promulgate regulations to help strengthen privacy and security protections for consumers' personal health data that are collected, processed, analyzed, or used by consumer devices, services, applications, and software).

321. Data Care Act § 3.

322. Protecting Personal Health Data Act § 4.

323. Mind Your Own Business Act §7.

324. Stop Marketing and Revealing the Wearables and Trackers Consumer Health § 3 (defining CHI).

325. *Id.*

regulation will automatically result in compliance by regulated entities which, in turn, will produce greater data privacy and security protections.[326] Given the research findings presented in Part II of this Article, we know this assumption is not always true. The study referenced in Part II.A showed, for example, that notwithstanding the Privacy Rule requirement for plain-language authorizations, the average reading level of HIPAA authorizations is much higher than the average reading capacity of U.S. adults.[327] The research presented in Part II.B showed, by further example, that notwithstanding Privacy Rule and state law provisions that require covered entities to provide access to PHI in certain forms and formats and that prohibit certain access fees, covered entities still refuse to provide access in certain forms and formats and still overcharge patients for such access.[328] Moreover, the studies highlighted in Parts II.C and II.E suggest that HIPAA-covered PHRs do not adhere to the Privacy Rule's accounting of disclosures requirement[329] and that the majority of (likely self-interested) covered entities self-report not being fully or even mostly compliant with the HIPAA Rules both in the first year following the compliance date as well as in the third year.[330] The AHIMA studies mentioned in Part II.E explore reasons for non-compliance, including a lack of resources and competing priorities.[331] Despite the imperfect relationship between regulation and compliance, the work highlighted in Part II.F of this Article does suggest, however, that health data privacy and security laws, including HIPAA and HITECH, can have a "strong and immediate effect"[332] on reducing the number of privacy and security breaches and that federal laws sometimes do achieve their intended goals of enhancing patient privacy and data security.[333]

The relationship between regulation and compliance in the context of health data privacy and security is, thus, extraordinarily complex and requires further investigation. That said, the research presented in Part II of this Article can be used to support concrete legislative proposals. To this end, let us turn to Senator Brian Schatz's DCA, which would establish very general duties of care, loyalty, and confidentiality for online service providers that handle personal data.[334] In particular, the DCA requires online service providers to "reasonably" secure individual identifying data; to not use identifying data in a way that will result in "reasonably" foreseeable harm to an end user; and to take "reasonable steps" to ensure that the practices of any person to whom the online service

326. *See* Cohen & Mello, *supra* note 28.
327. *See supra* Part II.A.
328. *See supra* Part II.B.
329. *See supra* Part II.C, II.E.
330. *See supra* Part II.E.
331. *See* supra Part II.E.
332. *See* Yaraghi & Gopal, *supra* note 137, at 153.
333. *See supra* Part II.F.
334. Data Care Act § 3.

provider discloses or sells, or with whom the online service provider shares, individual identifying data fulfils the duties of care, loyalty, and confidentiality.[335]

This Article argues that the duties set forth in the DCA, or in future legislation that is similar to the DCA, are simply too vague to drive compliance and should not be pursued further. If the compliance data presented in Part II show that covered entities and business associates struggle to comply with specific HIPAA Rules provisions such as the access to PHI provision[336] and the accounting of disclosures provision[337]—provisions that specifically identify the information to be provided, the information that does not have to be provided, the date by which information shall be provided, and the process by which information shall be provided—this Article predicts that newly regulated entities would struggle to understand what is required of them by statutory duties based on a "reasonable" standard of care. In the context of health data and privacy, tort-like duties of reasonableness are simply insufficient. If tort-like duties based on a "reasonable" standard of care were sufficient, then health data holders would not breach privacy and security for fear of violating existing common law tort duties. Given the number of recent health data privacy and security breaches reported to or discovered by HHS, we know this to be untrue.[338]

Let us now turn to Senator Klobuchar's PPHDA, which would direct the Secretary of HHS to promulgate regulations that would strengthen privacy and security protections for personal health data that are collected, processed, analyzed, or used by consumer devices, services, applications, or software.[339] The PPHDA does not establish substantive data privacy or security protections. Instead, the PPHDA directs HHS, through a protracted process, to develop future regulations designed to protect the privacy and security of personal health data.[340]

However, the history of the HIPAA Rules summarized in Part I of this Article shows that a lengthy rulemaking process is not desirable. Recall that President Clinton signed HIPAA into law on August 21, 1996, but that final modified privacy regulations were not published until August 14, 2002, almost

335. *Id.*

336. 45 C.F.R. § 164.524.

337. *Id.* § 164.528.

338. *See Cases Currently Under Investigation*, OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Sept. 20, 2020) (listing more than 600 recent breaches involving the unsecured protected health information (uPHI) of 500 or more individuals per breach; referring readers to a different web page that lists breaches involving the uPHI of fewer than 500 individuals).

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

340. *Id.* at § 4.

six years after HIPAA's date of enactment.[341] Moreover, final regulations promulgating HITECH's changes to the Privacy Rule did not appear until January 25, 2013,[342] *sixteen-plus years* after HIPAA's date of enactment. As of this writing, HHS is still *more than eight years* overdue on HITECH-required regulations that would give individuals harmed by privacy and security violations the right to share in settlements or penalties associated with those violations.[343] Given this history of privacy and security regulatory delay, the Author does not trust to a federal agency the timely promulgation of health data privacy and security regulations. In particular, this Article does not support statutory provisions that would simply delegate the promulgation of new health data privacy regulations to HHS or another federal agency, such as the FTC.[344] Given the pace with which Google and other for-profit companies are acquiring identifiable health data, relevant laws are needed sooner rather than later. Senator Klobuchar's PPHDA and Senator Wyden's MYOBA provisions requiring lengthy rulemaking processes are not ideal.[345]

That said, this Article strongly agrees with many of the directives identified by Senator Klobuchar in the PPHDA, including appropriate minimum security requirements for personal health data; limitations on the collection, use, and disclosure of personal health data; data subject consent prior to the collection, use, and disclosure of personal health data; requirements relating to the clarity, conciseness, and organization of such consent; appropriate standards for the de-identification of health data;[346] and perhaps most importantly, initial and ongoing outreach to industries, businesses, and individuals with respect to their new data privacy and security obligations and rights, as appropriate.[347] This Article simply recommends that the PPHDA be re-written such that these substantive provisions are set forth in final form in the statute itself, rather than delegating the responsibility to a federal agency to promulgate regulations addressing these issues.

Although federal health laws are notoriously vague and typically delegate to federal agencies the responsibility of promulgating specific, substantive

341. *See supra* text accompanying notes 44–53 (detailing the legislative history of the HIPAA statute and the regulatory history of the Privacy Rule).

342. 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 (Jan. 25, 2013) (codified at 45 C.F.R. pt. 160, 164).

343. *See supra* note 53 (referencing HHS's eight-plus year delay in promulgating relevant regulations).

344. *See* Protecting Personal Health Data Act § 4(a) (delegating to HHS the duty to promulgate new privacy regulations within six months).

345. *See id.*; Mind Your Own Business Act §§ 5(a)(2), 6(a) (requiring the FTC to promulgate regulations consistent with MYOBA within two years).

346. *See, e.g.*, Stacey A. Tovino, *The Myth of Health Data De-Identification* (forthcoming 2020) (arguing that current federal and state standards for health data de-identification are inadequate).

347. *See* Protecting Personal Health Data Act § 4(b)(2), (3)(B) (listing these requirements).

regulations,[348] there is precedent in federal and state health law for specific, substantive statutory requirements.[349] The California Consumer Privacy Act (CCPA), for example, is a state statute, not a regulation, that contains specific and detailed data privacy and security requirements applicable to certain California businesses.[350] The CCPA, now understood as a powerful state initiative for protecting the privacy and security of the personal data of California residents, came into being relatively quickly. The CCPA shows that lengthy rulemaking processes are not always necessary, especially in the context of data privacy and security.[351]

Moving from substance to implementation, many of the studies referenced in Part II suggest that a lack of resources is a significant factor driving non-compliance with the HIPAA Rules.[352] Covered entities and business associates spend significant resources trying to comply with the HIPAA Rules, including by hiring attorneys and otherwise devoting human and other resources to drafting notices of privacy practices, authorization forms, and business associate agreements. When resources are low, covered entities struggle with the lack of expertise needed to develop this documentation. Indeed, the studies referenced in Parts II.A, II.B, and II.E of this Article specifically suggest that covered entities are having particular difficulty producing HIPAA-compliant written authorization forms, medical release forms, and notices of privacy practices due to a lack of financial resources.

In response, this Article formally proposes that these forms, releases, and notices be set forth in the statute itself—that is, in the PPHDA, in a future bill like the PPHDA, or in an amended version of the HIPAA Privacy Rule. Because the HIPAA compliance literature discussed in Part II shows that covered entities continue to struggle writing authorization forms in sufficiently

348. *See, e.g.*, Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (Mar. 23, 2010), *as amended and reconciled by* Health Care and Education Reconciliation Act, Pub. L. No. 111-152, 124 Stat. 1029 (Mar. 30, 2010) (as reconciled, the Affordable Care Act (ACA)). Section 1302(b)(1) of the ACA contains a vague requirement for certain health plans to include essential health benefits (EHBs), which were implemented through more specific federal regulations that required states to select reference or benchmark health plans. *See generally* Stacey A. Tovino, *State Benchmark Plan Coverage of Opioid Use Disorder Treatments and Services: Trends and Limitations*, 70 S.C. L. REV. 763 (2019) (explaining this process).

349. *See, e.g.*, 42 U.S.C. § 1395dd (2019) (setting forth specific statutory requirements that apply to Medicare-participating hospitals with respect to the examination and treatment of individuals who present to the hospital's emergency department); 42 U.S.C. § 11101–52 (2019) (setting forth specific statutory peer-review processes that must be followed to ensure good-faith immunity protection).

350. *See* CAL. CIV. CODE § 1798.100–99. (2019).

351. *See, e.g.*, Mark A. Rothstein & Stacey A. Tovino, *California Takes the Lead on Data Privacy Law*, HASTINGS CTR. REP., Sept.–Oct. 2019 4 (explaining the history of the CCPA, including the leading role played by wealthy Californian Alastair Mactaggart, who spent millions of dollars gathering signatures to place an initiative on California's November 2018 ballot and subsequently negotiated a deal with lawmakers to enact a scaled-back version of his desired legislation; further noting that California Governor Jerry Brown signed the California Consumer Privacy Act into law in mid-summer 2018 and that most of the legislation went into effect on January 1, 2020).

352. *See supra* Parts II.E, II.G, and II.H.

plain language,[353] that medical release forms continue to be confusing and/or otherwise non-compliant,[354] and that a lack of institutional support and/or resources may be to blame for these violations,[355] then the federal government should bear the burden of assisting newly regulated entities by pre-drafting the bulk of these documents in plain language and inserting them into the government's new legislation.

There is precedent for including templates and forms in the statute requiring such documentation. State health statutes frequently contain state-law compliant authorization templates and forms,[356] state-law-compliant advance directive templates and forms,[357] and other forms designed to ensure the privacy, security, health, safety, and welfare of patients and insureds. The Texas Health and Safety Code, for example, contains an authorization form written in plain language for the use and disclosure of protected health information during medical malpractice litigation.[358] The statutory provision including the form provides that authorizations for the release of patient information "shall be in the following form" and, moreover, "shall be construed in accordance with the [HIPAA Privacy Rule.]"[359] There is no reason the PPHDA, or future similar legislation, cannot do the same.

These forms, releases, and notices will necessarily vary by regulated entity and by data subject. For example, the intention of one particular regulated entity to disclose a data subject's information for research or marketing purposes might be indicated in that regulated entity's authorization form, but not in a different regulated entity's authorization form. By further example, the specific information that the regulated entity will collect, use, and disclose will vary as well. However, Congress certainly can and should develop a template prompting the regulated entity to include particular information or to specify other information. State legislatures have been doing this for quite some time with great success. There is no reason Congress cannot follow suit. HHS has already developed model (and HIPAA-compliant) notices of privacy practices[360] and model business associate agreements.[361] These notices and

353. *See supra* Part II.A.

354. *See supra* Part II.B.

355. *See supra* Part II.E.

356. *See, e.g.*, TEX. CIV. PRAC. & REM. CODE ANN. § 74.052 (West 2019) (including within a Texas statute a template for an authorization for the use and disclosure of patient medical records).

357. *See, e.g.*, TEX. HEALTH & SAFETY CODE ANN. § 166.033 (including within a Texas statute a template for an advanced health care directive).

358. *See* TEX. CIV. PRAC. & REM. CODE ANN. § 74.052.

359. *Id.* § 74.052(c)(1).

360. *See Model Notice of Privacy Practices*, HHS (last updated Apr. 8, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html.

361. *See Business Associate Contracts: Sample Business Associate Agreement Provisions*, HHS (last updated Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

forms could be updated with new requirements, to the extent desired by Congress, and inserted directly into the PPHDA or similar future legislation.

Moving from substance to statutory clarity and simplicity, the PHR study presented in Part II.C shows that study authors continue to misunderstand and/or confuse the audit logs and access report requirements set forth in the Security Rule with the right of an individual to receive an accounting of disclosures under the Privacy Rule. In addition, the text-messaging studies presented in Part II.D show that covered entities continue to misunderstand the Privacy Rule's use and disclosure requirements in general and the TPO rules in particular. For example, some of the medical resident and teaching physician respondents to the text-messaging studies reviewed in Part II.D indicated that they believe that sharing PHI for treatment and education purposes necessarily violates the Privacy Rule and/or the Security Rule.

These studies strongly suggest the need for statutory clarity and simplicity. If a privacy or security provision is so complex that a researcher affiliated with an Ivy League institution cannot understand it, a problem exists with respect to that provision. Senator Klobuchar's PPHDA would require both initial and ongoing outreach to industries, businesses, and individuals with respect to their new data privacy and security obligations and rights, as appropriate. This Article strongly supports this requirement while also calling for simple and straightforward statutory language.

Given that several of the study authors referenced in this Article confused bifurcated compliance dates (i.e., earlier compliance dates for some covered entities and later compliance dates for other entities),[362] this Article formally proposes that new or expanded privacy and security legislation establish one "catchall" compliance deadline. Although additional compliance time for smaller or less resourceful entities may have been needed two decades ago, when data privacy and security expertise was less common and privacy and security policies and procedures were not publicly available, the case is different today. Today, draft privacy and security policies and procedures, as well as templates and forms, are readily available from federal and state agencies, trade associations, attorneys, consultants, and individuals certified in privacy compliance, and these policies, procedures, templates, and forms can easily be updated or amended to reflect the priorities of new or expanded legislation.

This Article has focused on undesirable and desirable features of the DCA and the PPHDA, respectively. What about Senator Wyden's MYOBA[363] and Senator Cassidy's Smartwatch Data Act?[364] MYOBA, similar to a portion of the

362. *See supra* Part II.G.

363. Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019).

364. Stop Marketing and Revealing the Wearables and Trackers Consumer Health (Smartwatch) Data Act, S. 2885, 116th Cong. (2019).

PPHDA,[365] emphasizes the rights of data subjects with respect to controlling the collection, use, and disclosure of their information. MYOBA, in particular, gives data subjects the right to opt out of data sharing.[366] The catch with basing privacy and security regulation in large or whole part on the ability of data subjects to opt out of data collection, use, disclosure, and sale activities is that we assume that data subjects know enough about privacy and security in general, and what particular regulated entities are doing with their data in particular, to make informed decisions and to correctly exercise those decisions. Recent, thoughtful scholarship challenges this assumption.[367]

Unlike MYOBA, however, Senator Cassidy's Smartwatch Data Act prioritizes provisions prohibiting entities from transferring, selling, sharing, or allowing access to consumer health information.[368] Given the findings presented in Part II of this Article suggesting the difficulty many individuals experience in terms of understanding and exercising their privacy rights, the Smartwatch Data Act's "top-down" prohibitions may be valuable going forward. This Article also prefers the Smartwatch Data Act's legislative approach. That is, the Smartwatch Data Act includes substantive privacy and security protections in the Act itself.[369] The Act does not delegate to an administrative agency the (likely lengthy) task of promulgating privacy and security regulations.

CONCLUSION

Prior scholars writing in the area of health data privacy and security have impliedly assumed, without testing, that new or expanded legislation or regulation will automatically result in compliance, followed by greater privacy and security protections for data subjects. This Article has challenged this assumption. By carefully reviewing academic, industry, and government studies investigating compliance with the HIPAA Rules, this Article reveals a complex and nuanced relationship between regulation and compliance. This Article concludes by suggesting methods for further developing the privacy and security compliance literature and by identifying ways that pending privacy and security bills can be strengthened and improved.

365. Protecting Personal Health Data Act § 4 (giving data subjects the right to amend and delete their personal health data as well as the right to withdraw their consent to the processing of their data).

366. Mind Your Own Business Act § 6.

367. *See, e.g.*, Solove, *supra* note 28, at *Abstract* (explaining that consumers sometimes "fail to make good assessments of privacy risks and to fail to manage their privacy effectively. Managing one's privacy is a vast, complex, and never-ending project that does not scale; it becomes virtually impossible to do comprehensively"; further arguing that "giving individuals more tasks for managing their privacy will not provide effective privacy protection. Instead, regulation should employ a different strategy – focus on regulating the architecture that structures the way information is used, maintained, and transferred.").

368. Smartwatch Data Act § 3.

369. *Id.*