2019

A Timely Right to Privacy

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

A Timely Right to Privacy

Stacey A. Tovino[*]

ABSTRACT: On December 28, 2017, the federal Department of Health and Human Services ("HHS") settled its fiftieth case involving potential violations of the privacy, security, and breach notification rules ("Rules") that implement the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"). This Article catalogues and examines currently available enforcement actions involving the HIPAA and HITECH Rules, including the cases in which HHS has entered into a settlement agreement with a HIPAA covered entity or business associate, the cases in which HHS has imposed a civil money penalty on a HIPAA covered entity, and the cases in which a state attorney general has entered into a settlement agreement or consent judgment with a HIPAA covered entity or business associate.

This Article finds that HHS and state attorneys general focus their settlement and penalty efforts on cases involving groups of patients and insureds, leaving individuals whose privacy and security rights have been violated out of the enforcement spotlight. This Article also shows that the execution of settlement agreements and the imposition of civil money penalties takes a considerable amount of time—more than seven years in some cases—resulting in a lack of timely attention to the privacy and security rights of both groups and individuals. Finally, this Article reveals that the corrective action required by HHS in cases that do not reach the settlement or penalty phase, when that information is made publicly available, tends to be prospective in nature. Although prospective action helps safeguard future rights, it does little to remedy past harms. Arguing that HITECH's improved enforcement provisions do little to support individual rights to privacy and security, this

[*] Judge Jack and Lulu Lehman Professor of Law and Founding Director, Health Law Program, William S. Boyd School of Law, University of Nevada, Las Vegas. I thank Daniel Hamilton, Dean, William S. Boyd School of Law, for his generous financial support of the research project on which this featured address is based. I also thank Nadia Sawicki, Georgia Reithal Professor of Law and Academic Director, Beazley Institute for Health Law and Policy, Loyola University Chicago School of Law, and the organizers and participants of the Eleventh Annual Beazley Symposium on Health Law and Policy ("Privacy, Big Data, and the Demands of Providing Quality Patient Care") for their comments and suggestions on the ideas presented at the symposium and in this Article.

Article proposes three new federal regulations. If adopted by HHS, these regulations will improve the ability of individuals to enforce their rights under the HIPAA Rules and reduce the time frame within which enforcement takes place.

I. INTRODUCTION

Consider a hypothetical involving a patient who is under the care of a local physician. The physician, who has not received any privacy or security training, downloads malicious software ("malware") that disseminates the

patient's electronic protected health information ("ePHI")[1] in violation of the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule.[2] When the patient learns that her sensitive ePHI has been disclosed without her authorization, she informs the physician that she is leaving his practice to seek care under a new provider. The patient requests a paper copy of her medical record, which she plans to give to her new provider. In violation of the HIPAA Privacy Rule, the physician refuses to give the patient a paper copy of her medical record.[3] The physician then discards the patient's paper medical record in a dumpster located behind the physician's clinic, violating the HIPAA Privacy Rule for a third time.[4]

Although hypothetical, the facts above are based on several cases in which the federal Department of Health and Human Services ("HHS") and state attorneys general have entered into settlement agreements or consent judgments with, or imposed civil money penalties on, covered entities and

---

1. Electronic protected health information ("ePHI") is "individually identifiable health information" that is "transmitted by electronic media" or "maintained in electronic media." 45 C.F.R. § 160.103 (2017).

> Individually identifiable health information is information that . . . :
>
> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) That identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Id. (emphasis omitted).

2. The HIPAA Privacy Rule is a set of federal regulations that governs covered entities and business associates with respect to their uses and disclosures of protected health information. *See id.* §§ 164.500–.534 (codifying the HIPAA Privacy Rule). The terms "covered entity" and "business associate" are defined *infra* notes 36 and 41, respectively. Protected health information ("PHI") is "individually identifiable health information . . . that is . . . [t]ransmitted by electronic media[,] . . . [m]aintained in electronic media[,] or . . . [t]ransmitted or maintained in any other form or medium." *Id.* § 160.103. Among other obligations, the HIPAA Privacy Rule requires covered entities and business associates to have in place appropriate technical "safeguards to protect the privacy of [PHI]" and to "reasonably safeguard [PHI] from . . . intentional [and] unintentional use[s] [and] disclosure[s] that . . . violat[e]" the HIPAA Privacy Rule. *Id.* § 164.530(c)(1)–(2).

3. *See id.* § 164.524(a)(1) (requiring (in most cases) covered entities to provide individuals with copies of their medical records, billing records, and other PHI that is maintained in a designated record set, if requested); *id.* § 164.501 (defining "designated record set" as "[a] group of records maintained by or for a covered entity," including within that definition medical records, billing records, enrollment records, payment records, claims adjudication records, and other records that are "[u]sed, in whole or in part, by or for [a] covered entity to make decisions about individuals").

4. *See id.* § 164.530(c)(1) (requiring covered entities to "have in place appropriate . . . physical safeguards to protect the privacy of [PHI]").

business associates for violations of the HIPAA Privacy Rule, the HIPAA Security Rule,[5] and the HIPAA Breach Notification Rule[6] (collectively, the "HIPAA Rules"). For example, HHS entered into a settlement agreement with the University of Washington ("UW") in December 2015 after a UW employee downloaded malware, resulting in the unauthorized disclosure of the ePHI of 90,000 UW patients.[7] The settlement agreement contained a $750,000 settlement amount, a detailed corrective action plan, and a requirement for annual reporting to HHS by UW on its compliance efforts.[8] By further example, HHS imposed a $4,351,600 civil money penalty on Cignet Health Center in February 2011 after finding that "Cignet violated 41 patients' rights by denying them access to their medical records."[9] By final example, the Indiana Attorney General entered into a $12,000 consent judgment in January 2015 with Joseph Beck, a dentist who discarded more than 60 boxes

5. The HIPAA Security Rule is a set of federal regulations that requires covered entities and business associates to: "(1) [e]nsure the confidentiality, integrity, and availability of all [ePHI] the covered entity or business associate creates, receives, maintains, or transmits," and "(2) [p]rotect against . . . reasonably anticipated threats or hazards to the security or integrity of such [ePHI]." *See id.* § 164.306(a)(1)–(2); *see also id* §§ 164.302–.318 (codifying the HIPAA Security Rule).

6. The HIPAA Breach Notification Rule requires covered entities to notify individuals, the media, and the Secretary of HHS in certain situations in which a breach of unsecured PHI has been discovered. *See id.* §§ 164.400–.414 (codifying the Breach Notification Rule).

7. Resolution Agreement between U.S. Dep't of Health & Human Servs. and the Board of Regents of the University of Washington on behalf of the University of Washington (U.S. Dep't Health & Human Servs. Dec. 2015), https://www.hhs.gov/sites/default/files/uw-ra-and-cap.pdf; Press Release, U.S. Dep't of Health & Human Servs., $750,000 HIPAA Settlement Underscores the Need for Organization-Wide Risk Analysis (Dec. 14, 2015) [hereinafter UW Press Release], *available at* http://wayback.archive-it.org/3926/20170127185458/https://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html.

8. *See* UW Press Release, *supra* note 7 ("The settlement includes a monetary payment of $750,000, a corrective action plan, and annual reports on the organization's compliance efforts.").

9. *See* Press Release, U.S. Dep't of Health & Human Servs., HHS Imposes a $4.3 Million Civil Money Penalty for Violations of the HIPAA Privacy Rule (Feb. 22, 2011), *available at* http://wayback.archive-it.org/3926/20140108162249/http://www.hhs.gov/news/press/2011pres/02/20110222a.html ("[The Office for Civil Rights] found that Cignet violated 41 patients' rights by denying them access to their medical records . . . . The HIPAA Privacy Rule requires that a covered entity provide a patient with a copy of their medical records within 30 . . . days of the patient's request."); *see also* Notice of Final Determination from Georgina Verdugo, Dir., Office for C.R., to Daniel E. Austin, Cignet Health Ctr. (Feb. 4, 2011) [hereinafter Notice of Final Determination, Cignet], https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/cignetpenaltyletter.pdf (imposing a $4,351,600 civil money penalty on Cignet Health); Notice of Proposed Determination from Georgina C. Verdugo, Dir., Office for C.R., U.S. Dep't of Health & Human Servs., to Daniel E. Austin, Cignet Health Ctr. [hereinafter Notice of Proposed Determination, Cignet], https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/cignetpenaltynotice.pdf ("Several of the individuals informed Cignet that they were requesting copies of their medical records so that they could obtain health care services from physicians other than those who were workforce members of Cignet.").

of dental records containing the paper protected health information ("PHI") of more than 5,600 patients in an Indianapolis dumpster.[10]

Between April 14, 2003, the compliance date for the HIPAA Privacy Rule,[11] and August 1, 2018, HHS has enforced the HIPAA Rules only 56 times through settlement agreements[12] and civil money penalty determinations.[13] The Author, who teaches the HIPAA Rules at law schools across the country[14] and represents a number of patients and insureds in pro bono privacy and security matters, has submitted several complaints to HHS following intentional and flagrant violations of the HIPAA Rules with little governmental response.[15] Inspired by the handful of enforcement actions to date as well as the frustration of the Author's own clients, who have unsuccessfully attempted to enforce their rights in a timely manner, this Article assesses the ability of an individual to enforce rights provided for in the HIPAA Rules, with a focus on the HIPAA Privacy Rule.

This Article proceeds as follows: Part II summarizes the HIPAA Privacy Rule, highlighting provisions frequently violated by covered entities as well as HHS's administrative enforcement process.[16] Part III makes a novel

---

10. *See* Consent Judgment at 3, ¶¶ 7–8, State v. Beck, No. 49D10 14 12 PL041613 (Ind. Cir./Super. Ct., Marion Cty. Jan. 5, 2015) ("The Defendant agrees to pay twelve thousand dollars ($12,000) at the execution of this judgment. . . . These funds shall be paid to the Office of the Indiana Attorney General."); *State Settles with Former Dentist Accused of Dumping Patient Files*, KOKOMO PERSPECTIVE (Jan. 9, 2015), http://kokomoperspective.com/kp/state-settles-with-former-dentist-accused-of-dumping-patient-files/article_3a5dbbfc-9831-11e4-b5ee-2fb4d5ff867a.html ("The state has reached a settlement with former Kokomo-area dentist, Dr. Joseph Beck, for mishandling medical records containing sensitive information of more than 5,600 patients.").

11. 45 C.F.R. § 164.534(a)–(b)(1), (c) (2017).

12. *See* Stacey A. Tovino, PowerPoint Presentation Keynote Address at 11th Annual Beazley Symposium on Health Law & Policy, Patient Privacy: Problems, Perspectives, and Opportunities, at slides 24–36 (Nov. 10, 2017) (on file with author) (collecting and summarizing HHS's settlement agreements as of November 10, 2017). *See infra* Appendix A (cataloguing the 52 cases in which HHS has entered into settlement agreements with covered entities).

13. *See infra* Appendix B (cataloguing the four cases in which HHS has imposed a civil money penalty on a covered entity). *See generally* Office for C.R., U.S. Dep't of Health & Human Servs., *Enforcement Highlights*, HHS.GOV (June 30, 2018) [hereinafter HHS, *Enforcement Highlights*], https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/2018-june/index.html (providing other enforcement data).

14. *See, e.g.*, Stacey Tovino, Health Information Privacy and Technology (Fall 2017) (Syllabus, Loyola University Chicago School of Law) (on file with author); Stacey Tovino, HIPAA Privacy Law (Jan. 2018) (Syllabus, Saint Louis University School of Law) (on file with author); Stacey Tovino, HIPAA Privacy Law (Spring 2017) (Syllabus, William S. Boyd School of Law) (on file with author).

15. *See, e.g.*, E-mail from the Office for C.R., U.S. Dep't of Health & Human Servs., to Stacey A. Tovino (Apr. 10, 2017, 10:52 AM) (on file with author) ("Thank you for filing a complaint via the website of the Office for Civil Rights . . . at [HHS]. This is an automated response to acknowledge receipt of your complaint. Your complaint will be assigned to an OCR staff member for review and appropriate action.").

16. *See infra* Part II.

contribution[17] to the patient privacy and security literatures by cataloguing and examining the 52 cases in which HHS has entered into a settlement agreement with a covered entity,[18] the four cases in which HHS has imposed a civil money penalty on a covered entity,[19] and the 15 cases in which a state attorney general has entered into a settlement agreement or consent judgment with a covered entity or business associate[20] for violations of the HIPAA Rules.

Part III shows how HHS and state attorneys generally focus their settlement and penalty efforts on cases involving groups of patients and insureds, leaving individuals whose privacy and security rights have been violated out of the enforcement spotlight.[21] Part III also shows how the execution of settlement agreements and the imposition of civil money penalties takes considerable time—over seven years in some cases—resulting in a lack of timely attention to the privacy and security rights of both groups and individuals.[22] Part III further reveals that the corrective action required by HHS in cases that do not reach the settlement or penalty phase tends to be prospective in nature.[23] Although prospective action protects future rights, it does little to remedy past harms.[24] Part III concludes by arguing that the Health Information Technology for Economic and Clinical Health Act's improved enforcement provisions fail to remedy past privacy and security violations.[25]

To correct these limitations, Part IV justifies and proposes a new federal regulation that would allow private parties who assist HHS in identifying violations of the HIPAA Rules to receive a percentage of any settlement amount or civil money penalty imposed by HHS.[26] Part V recommends a second federal regulation that would allow private parties harmed by violations of the HIPAA Rules to enforce their privacy and security rights

17. Prior scholarship in this area has described a few settlement agreements or civil money penalty cases but has neither catalogued nor identified trends among all available federal and state enforcement actions. *See generally, e.g.*, David Thomas et al., *HHS Issues First-Ever Civil Monetary Penalty for HIPAA Privacy Rule Violation*, 3 HEALTH IT L. & INDUSTRY 1 (2011) (discussing only HHS's first civil money penalty case against Cignet Health); Esther H. Yu, *HIPAA Privacy and Security: Analysis of Recent Enforcement Actions*, 15 J. HEALTH CARE COMPLIANCE 59 (2013) (summarizing only two enforcement actions involving Idaho State University and Shasta Regional Medical Center).

18. *See infra* Part III; *infra* Appendix A.

19. *See infra* Part III; *infra* Appendix B.

20. *See infra* Part III; *infra* Appendix C.

21. *See infra* Part III.

22. *See infra* Part III.

23. *See infra* Part III.

24. *See infra* Part III.

25. *See infra* Part III.

26. *See infra* Part IV.

through litigation.[27] Part VI suggests a third regulation that would exclude covered entities from Medicare and Medicaid participation if they grossly and flagrantly, or repeatedly, violate the HIPAA Rules.[28] If adopted by HHS, these regulations will improve the ability of individuals to enforce rights made available under the HIPAA Rules and shorten the time frame within which enforcement takes place.

This Article concludes by considering the role of federal regulations that are not enforced, or that are enforced infrequently, both in general and with respect to particular individuals.[29] HHS has an abundance of health, safety, and welfare regulations that are neither audited nor enforced on a timely basis, raising questions regarding agency discretion in terms of cases selected for enforcement, inconsistent agency enforcement of like violations, non-enforcement of federal regulations as a form of deregulation, and whistleblower incentives and private rights of action as solutions for agency inaction.

II. SUMMARY OF THE HIPAA PRIVACY RULE

As signed into law by President Clinton on August 21, 1996, the Health Insurance Portability and Accountability Act ("HIPAA") had several purposes: including "improve[ing] portability and continuity of health insurance coverage in the group and individual markets," combating health care fraud and abuse, "promot[ing] the use of medical savings accounts[,] . . . improv[ing] access to long-term care services and [insurance] coverage," and "simplify[ing] the administration of health insurance."[30]

---

27. *See infra* Part V.

28. *See infra* Part VI.

29. *See infra* Part VII.

30. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 1936 ("An Act [t]o amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."). In a number of prior articles, the Author has carefully reviewed the history, application, and general framework of the HIPAA Privacy Rule. *See, e.g.*, Stacey A. Tovino, *Complying with the HIPAA Privacy Rule: Problems and Perspectives*, 1 LOY. U. CHI. J. REG. COMPLIANCE 23, 25–28 (2016) (detailing the history of the HIPAA Privacy Rule, its application to covered entities and business associates, and its basic use and disclosure rules); Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973, 975–79 (2017) (stating the same); Stacey A. Tovino, *Silence Is Golden . . . Except in Health Care Philanthropy*, 48 U. RICH. L. REV. 1157, 1161–70 (2014) (stating the same); Stacey A. Tovino, *Teaching the HIPAA Privacy Rule*, 61 ST. LOUIS U. L.J. 469, 471–75 (2017) (stating the same). With updates and technical changes, the brief summary of the Privacy Rule set forth in Part II of this Article is taken with the permission of the Author from these prior publications.

HIPAA's Administrative Simplification Provisions, codified at Subtitle F of Title II of the statute,[31] directed HHS to issue regulations protecting the privacy of individually identifiable health information if Congress failed to enact comprehensive privacy legislation within three years of HIPAA's enactment.[32] When Congress failed to enact privacy legislation by its deadline, HHS incurred the duty to adopt privacy regulations.[33]

HHS responded. On November 3, 1999,[34] and December 28, 2000,[35] HHS issued a proposed and final privacy rule ("HIPAA Privacy Rule") regulating covered entities'[36] uses and disclosures of PHI. On March 27, 2002,[37] and August 14, 2002,[38] HHS issued proposed and final modifications to the HIPAA Privacy Rule. With the exception of technical corrections and conforming amendments,[39] these rules as reconciled remained largely unchanged between 2002 and 2009.

On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act ("ARRA") into law.[40] Division A, Title XIII of ARRA,

---

31. Health Insurance Portability and Accountability Act, §§ 261–264.

32. *Id.* § 264(c)(1) ("If legislation governing standards with respect to the privacy of individually identifiable health information . . . is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of [HHS] shall promulgate final regulations containing such standards . . . .").

33. *See id.*; Office for C.R., U.S. Dep't of Health & Human Servs., *Summary of the HIPAA Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last reviewed July 26, 2013) ("Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.").

34. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (proposed Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160–64).

35. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

36. Covered entities are defined to include health plans, health care clearinghouses, and those "health care provider[s] who transmit [any] health information in electronic form in connection with [standard] transaction[s]." 45 C.F.R. § 160.103 (2017).

37. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776 (proposed Mar. 27, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

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

39. *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, 66 Fed. Reg. 12,434, 12,434 (Feb. 26, 2001) (codified at 45 C.F.R. pts. 160, 164) ("This action corrects the effective date of the final rules adopting standards for privacy of individually identifiable health information published on December 28, 2000, in the Federal Register (65 FR 82462), resulting in a new effective date of April 14, 2001." (emphasis omitted)); Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information Published December 28, 2000, 65 Fed. Reg. 82,944, 82,944 (Dec. 29, 2000) (codified at 45 C.F.R. pts. 160, 164) ("These technical corrections address changes that inadvertently were excluded from the preamble of the Standards for Privacy of Individually Identifiable Health Information published December 28, 2000.").

40. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001–13424, 123 Stat. 115, 226–79.

better known as the Health Information Technology for Economic and Clinical Health Act ("HITECH"), contained certain provisions requiring HHS to expand the application of the HIPAA Privacy Rule to business associates,[41] modify some of the use and disclosure requirements,[42] adopt new breach notification rules,[43] provide education regarding the Privacy Rule[44] and, of importance to this Article, improve enforcement of the HIPAA Privacy Rule.[45] HHS responded with proposed and final rules on July 14, 2010,[46] and January 25, 2013,[47] respectively.

As amended over time during the Clinton, Bush, and Obama administrations, the HIPAA Privacy Rule strives to balance the interest of individuals in maintaining the confidentiality of their health information with the interests of society in obtaining, using, and disclosing health information to carry out a variety of public and private activities.[48] To this end, the HIPAA Privacy Rule now regulates covered entities' and business associates' uses of, disclosures of, and requests for individually identifiable health information ("IIHI")[49] to the extent such information does not constitute: (1) an education record protected under the Family Educational Rights and Privacy

41. See 42 U.S.C. § 17934 (2012) (providing the "[a]pplication of privacy provisions and penalties to business associates of covered entities"). Business associates ("Bas") are defined to include individual and institutions who: (1) on behalf of a covered entity, "but other than in the capacity of a member of the workforce of [a] covered entity . . . create[], receive[], maintain[], or transmit[] protected health information for a function or activity regulated by" the HIPAA Privacy Rule; and (2) "[p]rovide[], other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, . . . management, administrative, accreditation, or financial services to or for [the] covered entity." 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. pgs. 160, 164) [hereinafter Final HITECH Rules] (providing a new definition of business associate).

42. *See* 42 U.S.C. § 17935 (provoding "[r]estrictions on certain disclosures and sales of health information").

43. *See id.* § 17932 (requiring "[n]otification in the case of breach").

44. *See id.* § 17933 (titled "Education on health information privacy").

45. *See id.* § 17939 (titled "Improved enforcement").

46. *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868 (proposed July 14, 2010) (to be codified at 45 C.F.R. pts. 160, 164).

47. *See* Final HITECH Rules, *supra* note 41.

48. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164) ("The rule seeks to balance the needs of the individual with the needs of the society."); *id.* at 82,468 ("The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole."); *id.* at 82,472 ("The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule.").

49. *See* 45 C.F.R. § 160.103 (2017) (defining individually identifiable health information).

Act of 1974 ("FERPA"); (2) a student treatment record excepted from protection under FERPA; (3) an "employment record[] held by a covered entity in its role as [an] employer;" or (4) individually identifiable health information "regarding a person who has been deceased for more than 50 years."[50] The HIPAA Privacy Rule calls the subset of IIHI described in the previous sentence "protected health information" ("PHI").[51]

Before using or disclosing PHI, the HIPAA Privacy Rule requires covered entities and business associates to adhere to one of three different rules depending on the purpose of the information use or disclosure.[52] The first rule allows covered entities and business associates to use and disclose PHI with no prior permission from the individual who is the subject of the PHI —but only in certain situations.[53] That is, covered entities may freely use and disclose PHI without any form of prior permission in order to carry out certain treatment,[54] payment,[55] and health care operations[56] activities,[57] as well as certain public benefit activities.[58]

Under the second rule, a covered entity may use and disclose an individual's PHI for certain activities, but only if "the individual is informed in advance of the use or disclosure and has the opportunity to agree to[,]

---

50. *See id.* (defining "[p]rotected health information").

51. *See id.* (using the phrase "[p]rotected health information").

52. *See id.* §§ 164.502–.514 (setting forth the use and disclosure requirements regarding PHI applicable to covered entities and business associates).

53. *See id.* §§ 164.502–.504.

54. *See, e.g.*, §§ 164.502(a)(1)(ii), 164.506. Among other activities, treatment includes "the provision, coordination, or management of health care and related services by one or more health care providers." *Id.* § 164.501.

55. *See, e.g.*, §§ 164.502(a)(1)(ii), 164.506. Payment activities are "[t]he activities undertaken by . . . a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan" as well as the activities of "[a] health care provider or health plan to obtain or provide reimbursement for the provision of health care." *Id.* § 164.501.

56. The HIPAA Privacy Rule defines "health care operations" with respect to a list of activities that are related to a covered entity's covered functions. *See id.* (defining "health care operations"). These activities include, but are not limited to, "[c]onducting quality assessment and improvement activities[,] . . . conducting training programs in which" medical and other health care students learn to practice health care under supervision, and arranging for the provision of "legal services." *Id.*

57. *See id.* § 164.506(c)(1) (permitting "[a] covered entity [to] use or disclose [PHI] for its own treatment, payment, or health care operations"); *id.* § 164.506(c)(1)–(4) (permitting a covered entity to disclose PHI to certain recipients for the recipients' "treatment, payment, or health care operations" activities, respectively).

58. *See, e.g.*, § 164.512(k)(6). Covered entities may use and disclose PHI for 12 different public policy activities without the prior written authorization of the individual who is the subject of the information. *See id.* § 164.512(a)–(l). These public policy activities include, but are not limited to, "[u]ses and disclosures required by law," "[u]ses and disclosures for public health activities," disclosures for law enforcement activities, uses and disclosures for research, and disclosures for workers' compensation activities. *See id.* § 164.512(a), (b), (f), (i), (l).

prohibit[,] or restrict the use or disclosure."[59] The third rule—a default rule —requires covered entities and business associates to obtain the prior written authorization from the individual who is the subject of the PHI before using or disclosing the individual's PHI in any situation that does not fit under the first or second rule.[60] In the cases it investigates, HHS has identified these three rules (collectively, the "Use and Disclosure Requirements") as the most frequently violated requirements of the HIPAA Privacy Rule.[61] The third Use and Disclosure rule was violated by the physician in the hypothetical that opened this Article when the physician downloaded malware that resulted in the unauthorized disclosure of his patient's ePHI.

In addition to the Use and Disclosure Requirements, the HIPAA Privacy Rule also gives individuals five rights with respect to their PHI, including the right to receive a notice of privacy practices,[62] a right to request additional privacy protections,[63] a right to access PHI (including the right to receive a paper or electronic copy of PHI),[64] a right to request amendment of PHI,[65] and "a right to receive an accounting of disclosures of [PHI]"[66] (collectively, the "Individual Rights"). Covered entities frequently violate the third Individual Right, which requires individuals to be given access to their PHI.[67] This right was violated by the physician in the hypothetical that opened this Article when he refused to give his patient a copy of her medical record.

Finally, the Privacy Rule contains a set of administrative requirements, such as designating privacy personnel, training workforce members, safeguarding PHI, establishing a complaint process for individuals who believe their privacy rights have been violated, sanctioning workforce members who violate the HIPAA Privacy Rule, and developing privacy policies and procedures, among other requirements (collectively, the "Administrative Requirements").[68] Covered entities frequently violate the Administrative Requirements by failing to meet their obligation to safeguard individuals'

---

59. *See id.* § 164.510 (titled "Uses and disclosures requiring an opportunity for the individual to agree or to object")

60. *See id.* § 164.508(a)(1) (titled "Uses and disclosures for which an authorization is required")

61. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year*, HHS.GOV [hereinafter HHS, *Top Five Issues*], https://web.archive.org/web/20170630103320/https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html (last visited Nov. 18, 2018) (listing impermissible uses and disclosures as the top issue seen by HHS in investigated cases in years 2004 through 2015).

62. 45 C.F.R. § 164.520.

63. *Id.* § 164.522.

64. *Id.* § 164.524.

65. *Id.* § 164.526.

66. *Id.* § 164.528.

67. *See* HHS, *Top Five Issues*, *supra* note 61 (listing the failure to provide access to PHI as the third most frequent HIPAA issue seen by HHS in investigated cases in years 2003 through 2011 as well as 2013).

68. 45 C.F.R. § 164.530.

PHI.[69] For example, the physician in the hypothetical violated this requirement when he discarded the patient's medical records in a publicly accessible dumpster located outside his clinic.

The remedies available to patients who believe their privacy and security rights have been violated are limited. Under current law, no private right of action exists for patients and insureds whose rights under the HIPAA Rules have been violated.[70] Under the HIPAA Rules, an individual who is aggrieved by a privacy or security violation can complain to the covered entity itself,[71] the Secretary of HHS,[72] or a state attorney general who has the authority under HITECH to bring a civil action seeking damages or an injunction on behalf of a state resident for violations of the HIPAA Rules.[73] In response, HHS[74] (and, presumably, a state attorney general) may or will investigate the case,[75] may or will conduct a compliance review of the covered entity or business associate[76] and, if the investigation or review indicates

69. *See* HHS, *Top Five Issues*, *supra* note 61 (listing the failure to appropriately safeguard PHI as the second most frequent HIPAA issue seen by HHS in investigated cases in years 2004 through 2015).

70. *See, e.g.*, Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006) ("We hold there is no private cause of action under HIPAA . . . ."); Lee-Thomas v. LabCorp, No. 18-591 (RC), 2018 WL 3014824, at *3 (D.D.C. June 15, 2018) (granting the defendant's motion to dismiss based on failure to state a claim due to the lack of a private right of action); Johnson v. Quander, 370 F. Supp. 2d 79, 100 (D.D.C. 2005) ("[B]ecause no private right of action exists under the HIPAA, this Court does not have subject matter jurisdiction over this claim and it must be dismissed."), *aff'd*, 440 F.3d 489 (D.C. Cir. 2006), *cert. denied*, 549 U.S. 945 (2006); Univ. of Colo. Hosp. Auth. v. Denver Publ'g Co., 340 F. Supp. 2d 1142, 1144–46 (D. Colo. 2004) (citing a number of cases and secondary authorities supporting the rule that HIPAA contains no private right of action). *But see infra* Part V (proposing that HHS adopt a new regulation establishing a private right of action for HIPAA Rules violations).

71. *See* 45 C.F.R. § 164.530(d)(1) (requiring covered entities to provide a process for individuals to complain about suspected violations of the HIPAA Privacy Rule or the covered entity's privacy policies and procedures). Neither the HIPAA Privacy Rule nor any other law requires covered entities to make the complaints they receive, or any resolution of such complaints, publicly available. As such, the Author is unable to evaluate the ability of an individual to enforce his or her rights under the HIPAA Privacy Rule by complaining to the covered entity.

72. *See id.* § 160.306(a) (giving persons who believe that a covered entity or a business associate has violated the HIPAA Privacy Rule a right to file a complaint with the Secretary of HHS).

73. *See* 42 U.S.C. § 1320d–5(d) (2012) (authorizing a state attorney general to bring a civil action or an injunction on behalf of residents of that state for violations of the HIPAA Privacy Rule).

74. The procedures followed by state attorneys general depend on the state although they are guided by federal law. *See id.* (setting forth the process by which state attorneys general can enforce violations of the HIPAA Rules).

75. *See, e.g.*, 45 C.F.R. § 160.306(c)(1) (providing that "[t]he Secretary [of HHS] will investigate any complaint . . . when a preliminary review of the facts indicates a possible violation due to willful neglect"); *id.* § 160.306(c)(2) (providing that "[t]he Secretary may investigate any other complaint").

76. *See, e.g.*, *id.* § 160.308(a) (providing that "[t]he Secretary [of HHS] will conduct a compliance review to determine whether a covered entity or business associate is complying with the [HIPAA Rules] when a preliminary review of the facts indicates a possible violation due to willful neglect"); *id.* § 160.308(b) (providing that "[t]he Secretary [of HHS] may conduct a

noncompliance, may attempt to reach a resolution with the covered entity or business associate.[77]

HHS's resolution options include: (1) the provision of technical assistance by HHS to the covered entity or business associate and compliance therewith; (2) demonstrated compliance (also called voluntary compliance or voluntary cooperation) by the covered entity or business associate; (3) a settlement agreement that includes a settlement payment to HHS by the covered entity or business associate; (4) an agreement by the covered entity or business associate to take corrective action pursuant to a corrective action plan ("CAP"); (5) the imposition of a civil money penalty; and/or (6) the referral of the case to the federal Department of Justice ("DOJ") for criminal action.[78] HHS pursues a combination of the third and fourth options—a settlement plus a CAP—when HHS finds that the covered entity's or business associate's noncompliance was due to willful neglect or when "the nature and scope of the noncompliance warrants additional enforcement action."[79]

HHS pursues the fifth option—the imposition of civil money penalties —when HHS is unable to resolve the matter through technical assistance, demonstrated compliance, and/or corrective action (hereinafter, "agreement").[80] If HHS is unable to resolve the matter by agreement, then HHS will ask the "covered entity or business associate . . . to submit written evidence of any mitigating factors or affirmative defenses" relating to the entity's HIPAA Rules violations.[81] Following HHS's receipt of the requested information, HHS will send the covered entity or business associate a notice of proposed determination ("NPD"), which announces that a civil money penalty will be imposed on the covered entity or business associate and provides the opportunity for the covered entity or business associate to request a hearing.[82] Depending on the outcome of any hearing, the NPD is

---

compliance review to determine whether a covered entity or business associate is complying with the [HIPAA Rules] in any other circumstance").

77. *See, e.g., id.* § 160.312(a)(1).

78. *See, e.g., id.* (providing that if an investigation or a compliance review indicates noncompliance with the HIPAA Rules, then "the Secretary [of HHS] may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement").

79. *See* OFFICE FOR C.R., U.S. DEP'T OF HEALTH & HUMAN SERVS., ANNUAL REPORT TO CONGRESS ON HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION RULE COMPLIANCE FOR CALENDAR YEARS 2013 AND 2014, at 4–5, https://www.hhs.gov/sites/default/files/rtc-compliance-20132014.pdf.

80. *See id.* at 5.

81. 45 C.F.R. § 160.312(a)(3)(i).

82. *See id.* § 160.312(a)(3)(ii); *id.* § 160.420 (requiring a notice of proposed determination ("NPD") to be sent to a covered entity or business associate on whom HHS is proposing to impose a civil money penalty); Notice of Proposed Determination from Leon Rodriguez, Dir., Office for C.R., U.S. Dep't of Health & Human Servs., to Paul Tripp, Gen. Counsel, Lincare, Inc. (Jan. 28, 2014) [hereinafter Notice of Proposed Determination, Lincare], https://www.hhs.gov/sites/default/files/Lincare_NPD_remediated.pdf (providing an illustration of a NPD proposing to impose a

followed by a notice of final determination ("NFD"), which notifies the covered entity or business associate of HHS's final decision to impose a civil money penalty together with information stating when and how the covered entity or business associate shall pay the penalty.[83] Under the current HIPAA Rules, both settlement amounts and civil money penalties are paid directly by the covered entity or business associate to HHS, not to the individuals harmed by the HIPAA Rules violations.[84]

In addition to its civil enforcement of the HIPAA Rules, HHS also refers certain cases that are appropriate for criminal investigation, including those cases involving the knowing disclosure or obtaining of PHI in violation of the HIPAA Rules, to the federal Department of Justice.[85] As of this writing, HHS has referred 688 cases to the DOJ for criminal investigation.[86]

III. RESEARCH FINDINGS

A. *NUMBER OF AFFECTED INDIVIDUALS IN CASES SELECTED FOR SETTLEMENT OR PENALTY*

HHS makes public some information regarding its intake, investigation, and civil enforcement activities. This information includes the total number

---

$239,800 civil money penalty on covered entity Lincare); *infra* Appendix B (linking, in the far right column, to all of the NPDs sent by HHS to covered entities through the end of calendar year 2017).

83. *See* 45 C.F.R. § 160.424 (authorizing the Secretary of HHS to make final determinations regarding penalties through a notice of final determination ("NFD")); Notice of Final Determination from Jocelyn Samuels, Dir., Office for C.R., U.S. Dep't of Health & Human Servs., to Marshall S. Ney, Attorney, Friday, Eldredge & Clark, LLP (Mar. 1, 2016) [hereinafter Notice of Final Determination, Lincare], https://www.hhs.gov/sites/default/files/lincare-nfd-for-web.pdf (providing an illustration of an NFD stating a March 1, 2016, civil money penalty imposition date); *infra* Appendix B (linking, in the far right column, to all of the NFDs sent by HHS to covered entities through the end of calendar year 2017).

84. *See, e.g.*, Resolution Agreement between U.S. Dep't of Health & Human Servs. and St. Luke's-Roosevelt Hosp. Ctr. Inc. (U.S. Dep't Health & Human Servs. May 8, 2017) (requiring St. Luke's to pay a settlement amount (also called a resolution amount) of $387,200 to HHS); 45 C.F.R. § 160.424(a) (providing that civil money penalties for HIPAA Rules violations are paid to the Secretary of HHS). However, Part IV discusses long overdue federal regulations that would allow individuals harmed by HIPAA Rules violations to receive a percentage of such civil money penalties. *See infra* Part IV.

85. *See* 42 U.S.C. § 1320d–6(a) to (b) (2012) (providing that "[a] person who knowingly and in violation of" the HIPAA Rules uses, obtains, or discloses individually identifiable health information shall be punished in accordance with a three-tiered criminal penalty scheme that includes: (1) fines of not more than $50,000, imprisonment for not more than 1 year, or both; (2) for offenses committed under false pretenses, fines of not more than $100,000, imprisonment for not more than 5 years, or both; and (3) "if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm," fines of not more than $250,000, imprisonment for not more than 10 years, or both); HHS, *Enforcement Highlights*, *supra* note 13 (stating that OCR has made 688 referrals to the Department of Justice).

86. *See* HHS, *Enforcement Highlights*, *supra* note 13 (stating the number of cases referred to the DOJ).

of HIPAA complaints HHS receives,[87] the total number of notifications to HHS by covered entities and business associates of breaches affecting 500 or more individuals that have been resolved by HHS,[88] the total number of notifications to HHS of breaches affecting 500 or more individuals that are currently under investigation by HHS,[89] the number of complaints HHS has resolved,[90] illustrative examples of corrective action taken by some covered entities and business associates,[91] the content of all settlement agreements entered into by HHS,[92] the content of all proposed and final civil money penalty determinations made by HHS,[93] and other data, such as the number of complaints received by HHS (organized by year),[94] the number of cases enforced by HHS (organized by year),[95] and the number of cases enforced by HHS (organized by state of origin).[96]

---

87. *See id.* (stating that the OCR has, as of June 30, 2018, "received over 184,614 HIPAA complaints").

88. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information—Archive*, HHS.GOV, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 18, 2018) (listing 1,974 resolved breach notifications affecting 500 or more individuals as of August 1, 2018).

89. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information—Cases Currently Under Investigation*, HHS.GOV, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 18, 2018) (listing 419 breach notifications affecting 500 or more individuals that are currently under investigation by HHS as of August 1, 2018).

90. *See* HHS, *Enforcement Highlights*, *supra* note 13 ("We have resolved ninety-six percent of these cases (177,194).").

91. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *All Case Examples*, HHS.GOV [hereinafter HHS, *All Case Examples*], https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html (last reviewed June 7, 2017) (providing 32 illustrative examples of cases in which HHS obtained corrective action from a covered entity or business associate).

92. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *Resolution Agreements*, HHS.GOV [hereinafter HHS, *Resolution Agreements*], https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (last reviewed Oct. 15, 2018) (linking the public to press releases announcing the settlement agreements); *infra* Appendix A (referencing, summarizing, and linking to the settlement agreements).

93. *See* HHS, *Resolution Agreements*, *supra* note 92 (linking the public to press releases announcing the civil money penalty cases); *infra* Appendix B (referencing, summarizing, and linking to the civil money penalty cases).

94. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *Health Information Privacy Complaints Received by Calendar Year*, HHS.GOV, https://web.archive.org/web/20170629142436/https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html (last reviewed Oct. 13, 2016).

95. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *Enforcement Results by Year —Compliance Reviews*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/results-by-year-compliance-reviews/index.html (last reviewed June 7, 2017).

96. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *Enforcement Results by State*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-state/index.html (last reviewed Oct. 13, 2016).

Let us begin by focusing on the complaints filed by individuals with HHS to see the usefulness, from an individual's perspective, of filing a complaint with the federal government. As background, individual patients and insureds whose privacy and security rights have been violated frequently contact me at my law office to ask whether and how to file a complaint with HHS. These individuals may have heard that HHS imposes settlement amounts and civil money penalties on noncompliant covered entities and business associates and may wish to pursue that avenue of redress. These individuals frequently ask me what they should expect as a result of filing such a complaint.

Between April 14, 2003 (the compliance date for the HIPAA Privacy Rule) and June 30, 2018 (the most recent date as of the writing of this Article through which HHS has made complaint data available), HHS received 184,614 complaints alleging violations of the HIPAA Rules.[97] Of these 184,614 complaints, HHS states that it has resolved 177,194 complaints through: (1) a finding of a lack of jurisdiction by HHS, an untimely complaint, or a description of an activity that, even if true, does not violate the HIPAA Rules (111,179);[98] (2) an investigation that led to a change in privacy practices, the imposition of corrective action, and/or the provision of technical assistance to the offending covered entity or business associate (26,071, including the 52 settlement agreements and four civil money penalties cases);[99] (3) an investigation that led to a finding of no violation of the HIPAA Rules (11,494);[100] or (4) an "early intervention" by HHS—not an investigation—that led to the provision by HHS of technical assistance to the covered entity or business associate (28,450).[101] HHS does not provide any information regarding the complaints that it has received but not yet processed or resolved (7,420).[102]

Because my clients frequently ask me about the possibility that HHS will investigate and impose a settlement amount or civil money penalty on the entity that violated their rights, let us focus for a moment on the 26,071 cases in which HHS conducted an investigation that led to a change in privacy practices, the imposition of corrective action (including a settlement plus CAP or a civil money penalty), and/or the provision of technical assistance to the covered entity or business associate.[103] How many of the settlement and

---

97. *See* HHS, *Enforcement Highlights*, *supra* note 13.

98. *See id.*

99. *See id.* (providing these numbers; stating that, "[c]orrective actions obtained by OCR from these entities have resulted in change that is systemic and that affects all the individuals they serve").

100. *See id.* (providing these numbers).

101. *See id.* (presenting this information).

102. *See id.* (providing no information regarding the 7,420 [184,614 minus 177,194] complaints HHS received between April 14, 2003, and June 30, 2018, but that HHS has yet to resolve).

103. *See id.* ("OCR has investigated and resolved over 26,071 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates.").

penalty cases involved just one individual, like each of my clients, who has been harmed by a privacy or security violation?

1. HHS Settlement Agreements

Appendix A to this Article catalogues the 52 settlement agreements and CAPS entered into by HHS with covered entities for violations of the HIPAA Rules through August 1, 2018.[104] Forty-eight (92.3%) of the 52 cases selected for settlement by HHS involved a group—and many times a very large group—of patients and insureds whose privacy or security rights were potentially violated in the same incident or series of incidents.[105] For example, HHS settled with 21st Century Oncology, Inc. ("21st Century") for $2.3 million in December 2017 after 21st Century likely violated the HIPAA Privacy Rule. 21st Century had "disclos[ed] the names, social security numbers, physicians' names, diagnoses, and treatment and insurance information of 2,213,597" patients without their prior written authorization, as required by the third rule within the Use and Disclosure Requirements.[106] The 21st Century case clearly involved the PHI of a large group of patients; that is, a group numbering over 2,000,000.

Likewise, HHS settled with Advocate Health Care Network for $5.5 million in July 2016, following a series of incidents in which Advocate had the

---

104. *See infra* Appendix A.

105. *See infra* Appendix A (listing 41 cases involving a group of individuals as identified by the exact number of individuals affected (e.g., "192" or "1,023,209") or by a number range of individuals affected (e.g., ">386,000," "[o]ver 1,000," or "[m]illions"); listing three cases in which HHS used a phrase, such as "[n]umerous individuals" or "[m]any patients" that indicated that a group of individuals had been affected; and listing four cases, indicated by the symbol † in the third column, with respect to which HHS does not identify the exact number or range of individuals who were affected and does not use a phrase such as "[n]umerous individuals" or "[m]any patients"; however, by HHS's description of the nature of the incident, it is reasonable to assume that the incident affected many individuals). A case in which it is reasonable to assume that the incident affected many individuals is described by HHS as follows:

> OCR . . . opened its investigation of Rite Aid after television media videotaped incidents in which pharmacies were shown to have disposed of prescriptions and labeled pill bottles containing individuals' identifiable information in industrial trash containers that were accessible to the public. These incidents were reported as occurring in a variety of cities across the United States. Rite Aid pharmacy stores in several of the cities were highlighted in media reports.

See Office for C.R., U.S. Dep't of Health & Human Servs., *Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/rite-aid/index.html (last reviewed June 7, 2017).

106. *See infra* Appendix A, at row 50, col. 5 (summarizing the reasons for the settlement agreement with 21st Century); *see also* Press Release, U.S. Dep't of Health & Human Servs., Failure to Protect the Health Records of Millions of Persons Costs Entity Millions of Dollars (Dec. 28, 2017) [hereinafter 21st Century Press Release], *available at* https://www.hhs.gov/about/news/2017/12/28/failure-to-protect-the-health-records-of-millions-of-persons-costs-entity-millions-of-dollars.html ("[21st Century] determined that 2,213,597 individuals were affected by the impermissible access to their names, social security numbers, physicians' names, diagnoses, treatment, and insurance information.").

ePHI of nearly 4,000,000 patients stolen or accessed without the patients' prior written authorization.[107] By final illustrative example, HHS settled with Blue Cross and Blue Shield of Tennessee for $1.5 million in March 2012 after the insurer failed to secure and had stolen 57 unencrypted hard drives containing the PHI of 1,023,209 insureds.[108]

Only four (7.69%) of the 52 cases selected by HHS for settlement involved one or two individuals. HHS may have selected these cases because they involved intentional and egregious violations of the HIPAA Rules by senior leadership or because they involved the unauthorized disclosure of extremely sensitive PHI, such as HIV diagnoses.

In the first case involving the unauthorized disclosure of PHI of only one or two individuals,[109] HHS settled with Shasta Regional Medical Center for $275,000 in June 2013.[110] The settlement occurred after senior leadership at Shasta met with various media outlets and sent an email to the entire Shasta workforce discussing the health care provided to one identifiable patient without the patient's prior written authorization.[111] In the second case, HHS settled with New York and Presbyterian Hospital ("Hospital") for $2.2 million in April 2016, after the Hospital allowed a television film crew to film one identifiable patient who was dying and a second identifiable patient who was in significant distress, even after a medical professional urged the crew to stop filming.[112] The Hospital failed to obtain the prior written authorization of the

---

107. Press Release, U.S. Dep't of Health & Human Servs., Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million (Aug. 4, 2016), *available at* https://wayback.archive-it.org/3926/20170127192127/https://www.hhs.gov/about/news/2016/08/04/advocate-health-care-settles-potential-hipaa-penalties-555-million.html ("The combined breaches affected the ePHI of approximately 4 million individuals."); *see infra* Appendix A, at row 38, col. 5 (summarizing the reasons for the settlement agreement with Advocate Health Care Network).

108. *See* Press Release, U.S. Dep't of Health & Human Serv., HHS Settles HIPAA Case with BCBST for $1.5 Million (Mar. 13, 2012), *available at* https://wayback.archive-it.org/3926/20150121155524/http://www.hhs.gov/news/press/2012pres/03/20120313a.html ("The [stolen hard] drives contained the [PHI] of over 1 million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers."); *infra* Appendix A, at row 7, col. 5 (summarizing the reasons for the settlement agreement with the insurer).

109. *See infra* Appendix A (listing two cases involving one individual and two cases involving two individuals).

110. Press Release, U.S. Dep't of Health & Human Servs., HHS Requires California Medical Center to Protect Patients' Right to Privacy (June 13, 2013), *available at* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/srmc/press-release/index.html.

111. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and Shasta Reg'l Med. Ctr. 1–2 (U.S. Dep't Health & Human Servs. June 6, 2013) [hereinafter Resolution Agreement, Shasta Reg'l], https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/shasta-agreement.pdf (discussing the facts that gave rise to the settlement with Shasta Regional Medical Center).

112. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and N.Y. & Presbyterian Hosp., at 1 (U.S. Dep't Health & Human Servs. Apr. 19, 2016), https://www.hhs.gov/sites/default/files/nyp-nymed-racap-april-2016.pdf (describing the case's factual background); Press Release, U.S. Dep't of Health & Human Servs., Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital (Apr. 21, 2016) [hereinafter NY

two patients, as required by the third rule of the Use and Disclosure Requirements.[113]

In the third case involving the PHI of only one or two individuals, HHS settled with Houston-based Memorial Hermann Health System ("Memorial Hermann") for $2.4 million in April 2017 after senior leadership at Memorial Hermann impermissibly disclosed one identifiable patient's PHI to several media outlets and placed that same patient's PHI on Memorial Hermann's website, all without the patient's prior written authorization.[114] In the fourth and final case involving the PHI of only one or two individuals, HHS settled with St. Luke's-Roosevelt Hospital Center Inc. for $387,200 in May 2017 after a St. Luke's employee faxed, without prior written authorization, the sensitive PHI of one patient to the patient's employer and the PHI of a second patient to the second patient's place of volunteer work.[115] The sensitive PHI included information about the two patients' HIV status as well as their sexually transmitted diseases, sexual orientation, mental health, and physical abuse.[116]

2. HHS Civil Money Penalties

The cases discussed in the section above were settled by HHS and the named covered entity through a settlement agreement plus a corrective action plan, or CAP. According to the former Acting Deputy Director of HHS's Office for Civil Rights, HHS "is prepared to take all of its cases to an [administrative law judge ("ALJ")] for [the imposition of] a civil money

---

Med Press Release], *available at* http://wayback.archive-it.org/3926/20170128230744/https://www.hhs.gov/about/news/2016/04/21/unauthorized-filming-ny-med-results-22-million-settlement-new-york-presbyterian-hospital.html ("[OCR] announced that it has reached a $2.2 million settlement with [NYP] for the egregious disclosure of two patients' [PHI] to film crews and staff during the filming of 'NY Med,' an ABC television series, without first obtaining authorization from the patients. In particular, OCR found that NYP allowed the ABC crew to film someone who was dying and another person in significant distress, even after a medical professional urged the crew to stop."); *infra* Appendix A, at row 34, col. 5 (summarizing the reasons for the settlement agreement with New York and Presbyterian Hospital).

113. *See supra* note 112 (explaining that the two patients had not authorized filming).

114. *See* Press Release, U.S. Dep't of Health & Human Servs., Texas Health System Settles Potential HIPAA Disclosure Violations (May 10, 2017) [hereinafter Texas Health Press Release], *available at* https://www.hhs.gov/about/news/2017/05/10/texas-health-system-settles-potential-hipaa-disclosure-violations.html (quoting OCR Director Roger Severino stating "Senior management should have known that disclosing a patient's name on the title of a press release was a clear HIPAA Privacy violation that would induce a swift OCR response"); *infra* Appendix A, at row 48, col. 5 (summarizing the reasons for the settlement agreement with Memorial Hermann).

115. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and St. Luke's-Roosevelt Hosp. Ctr. Inc., at 1 (U.S. Dep't Health & Human Servs. May 8, 2017) [hereinafter Resolution Agreement, St. Luke's-Roosevelt], https://www.hhs.gov/sites/default/files/st-lukes-signed-ra-cap.pdf (describing the facts that gave rise to the settlement); Press Release, U.S. Dep't of Health & Human Serv., Careless Handling of HIV Information Jeopardizes Patient's Privacy, Costs Entity $387k (May 23, 2017), *available at* https://www.hhs.gov/about/news/2017/05/23/careless-handling-hiv-information-costs-entity.html; *infra* Appendix A, at row 49, col. 5 (summarizing the reasons for the settlement agreement with St. Luke's).

116. *See supra* note 115.

penalty."[117] However, HHS prefers settlements, which allow HHS to require the covered entity or business associate to enter into a CAP, mandating corrections and prospective HIPAA compliance.[118] On the other hand, in civil money penalty cases, HHS does not have authority to obtain injunctive relief or to impose corrective action.[119] Settlements also offer non-compliant covered entities and business associates significant savings compared to civil money penalties.[120] Settlement amounts typically range from ten to 70% of the dollar amount HHS could impose if the case went to an ALJ for a civil money penalty.[121]

Despite HHS's preference for settlements in this context, Appendix B to this Article catalogues the four cases in which HHS imposed a civil money penalty for violations of the HIPAA Rules through August 1, 2018.[122] In these four cases, HHS was unable to obtain voluntary compliance or agreement regarding past non-compliant behavior and/or future compliance. The third column of Appendix B shows the number of individuals affected by each privacy or security violation that led to the civil money penalty.[123] All four, or 100%, of the civil money penalty cases involved groups of patients, rather than individuals.[124]

In the first civil money penalty case, HHS imposed a $4,351,600 penalty on Cignet Health Care in February 2011 after Cignet failed to give a group of 41 patients copies of their requested medical records.[125] In the second case, HHS imposed a $239,800 penalty on Lincare, Inc. in March 2016 after a Lincare employee left the PHI of a group of 278 patients under a bed and in a kitchen drawer after the employee moved out of the home she shared with another person.[126] In the third case, HHS imposed a $3,217,000 fine on

---

117. *The Intersection of OCR Enforcement and Health Care Data Privacy & Security* (Polsinelli Health Care Webinar Series Mar. 8, 2018) [hereinafter Polsinelli Webinar], https://www.polsinelli.com/intelligence/webinar-the-intersection-of-ocr-enforcement (featuring recorded statements made by Iliana Peters, the former Acting Deputy Director of HHS's Office for Civil Rights, regarding settlements versus civil money penalties).

118. *Id.*

119. *Id.*

120. *Id.*

121. *Id.*

122. *See infra* Appendix B.

123. *See infra* Appendix B, at col. 3.

124. *See infra* Appendix B (listing groups consisting of 41, 278, "at least" 2,484, and approximately 33,500 individuals).

125. *See* Notice of Proposed Determination, Cignet, *supra* note 9, at 1 (summarizing the case); *id.* at Attachment A (noting that Cignet failed to provide 41 patients access to their medical records starting in November 2008 and proceeding throughout 2009); *infra* Appendix B, at row 1 (cataloguing the Cignet civil money penalty case).

126. *See* Notice of Final Determination, Lincare, *supra* note 83, at 1 (summarizing the case); Notice of Proposed Determination, Lincare, *supra* note 82, at 2, ¶ 5 (noting that the complainant stated that he found PHI of 278 patients "under a bed and in a kitchen drawer in approximately November 2008"); *infra* Appendix B, at row 2 (cataloguing the Lincare civil money penalty case).

Children's Medical Center of Dallas in January 2017 following several incidents involving the loss or theft of unencrypted devices containing the ePHI of at least 2,484 individuals.[127] In the fourth case, HHS imposed a $4,348,000 fine on the University of Texas MD Anderson Cancer Center in June 2018 following an investigation into three data breaches involving one stolen laptop and two lost flash drives (all unencrypted) that compromised the identifiable health information of more than 33,500 individuals.[128] Again, all four cases selected by HHS for the imposition of civil money penalties involved the PHI of groups of patients, not individuals.

3. State Attorney General Enforcement

In addition to civil enforcement by HHS, a state attorney general also has the authority under HITECH to bring a civil action seeking damages or an injunction on behalf of a state resident for violations of the HIPAA Rules.[129] Appendix C to this Article catalogues the 15 HIPAA Rules cases brought by seven attorneys general out of Connecticut, Indiana, Massachusetts, Minnesota, New Jersey, New York, and Vermont through August 1, 2018.[130] The fourth column of Appendix C shows the number of individuals affected by each privacy or security incident that led to the state enforcement action. All 15 (100%) of the cases brought by state attorneys general involved groups of patients and insureds, rather than individuals, who were affected by violations of the HIPAA Rules.[131]

The Connecticut Attorney General brought the first state action enforcing the HIPAA Rules in July 2010.[132] In that action, Health Net, Inc.

---

127. *See* Notice of Final Determination from Jocelyn Samuels, Dir., Office for C.R., U.S. Dep't of Health & Human Servs., to David Berry, President, Sys. Clinical Operations, Children's Med. Ctr. 1 (Jan. 18, 2017) [hereinafter Notice of Final Determination, Children's Med. Ctr.], https://www.hhs.gov/sites/default/files/childrens-notice-of-final-determination.pdf (imposing the penalty on Children's Medical Center of Dallas); Notice of Proposed Determination from Marisa M. Smith, Reg'l Manager, Office for C.R., U.S. Dep't of Health & Human Servs., to David Berry, President, Sys. Clinical Operations, Children's Med. Ctr. 6 (Sept. 30, 2016) [hereinafter Notice of Proposed Determination, Children's Med. Ctr.], https://www.hhs.gov/sites/default/files/childrens-notice-of-proposed-determination.pdf (describing the HIPAA Rules violations that led to the penalty; stating in relevant part that "Children's impermissibly disclosed the PHI of at least 2,484 individuals"); *infra* Appendix B, at row 3 (cataloguing the Children's Medical Center of Dallas civil money penalty case).

128. *See* Dir. of the Office for C.R. v. Univ. of Tex. MD Anderson Cancer Ctr., Docket No. C-17-854, Decision No. CR5111, at 1–2, 4–5 (U.S. Dep't Health & Human Servs. June 1, 2018); *infra* Appendix B, at row 4 (cataloguing MD Anderson's civil money penalty case).

129. *See* 42 U.S.C. § 1320d–5(d) (2012) (authorizing a state attorney general to bring a civil action or an injunction on behalf of residents of that state for violations of the HIPAA Privacy Rule).

130. *See infra* Appendix C.

131. *See infra* Appendix C, at col. 4 (listing groups consisting of 500,000, 525, 800,000, >23,000, 67,000, 12,127, 3,796, >5,600, 2,159, 3,403, "Multiple 'patients' and 'consumers,'" 690,000, 2,460, 81,122, and >1,650 persons).

132. *See* Press Release, Conn. Attorney Gen.'s Office, Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial

("Health Net") entered into a $250,000 settlement agreement with the Connecticut Attorney General following Health Net's loss of a hard drive containing the PHI of 1.5 million insureds total, including 500,000 Connecticut residents.[133] The Vermont Attorney General brought the second state action enforcing the HIPAA Rules in January 2011, also against Health Net.[134] In the Vermont action, Health Net agreed to pay the Vermont Attorney General an additional $55,000 because the lost hard drive contained the PHI of 525 Vermont residents.[135] In a third illustrative example of a state enforcement action involving the PHI of a group of patients, rather than the PHI of just one individual, South Shore Hospital paid the Massachusetts Attorney General $750,000 in May 2012 after the "[h]ospital shipped three boxes [holding] 473 unencrypted back-up computer tapes" that contained the PHI of 800,000 patients.[136] Only one box made it to its final destination in Texas.[137]

In summary, HHS and state attorneys general focus their settlement and penalty efforts on cases involving groups—many times large groups—of patients and insureds, leaving individuals whose privacy and security rights have been violated out of the enforcement spotlight. In particular, 48 (92.3%) of the 52 HIPAA Rules cases selected by HHS for settlement involved the PHI of groups, rather than individuals.[138] All four (100%) of the four civil money penalty cases involved the PHI of groups, rather than individuals.[139]

Info (July 6, 2010), *available at* https://portal.ct.gov/AG/Press-Releases-Archived/2010-Press-Releases/Attorney-General-Announces-Health-Net-Settlement-Involving-Massive-Security-Breach-Compromising-Priv ("Attorney General Richard Blumenthal today announced a settlement—the first of its kind in the nation—with Health Net and its affiliates for failing to secure private patient medical records and financial information on nearly a half million Connecticut enrollees and promptly notify consumers endangered by the breach.").

133. *See id.* ("The settlement provides powerful protections for consumers and a $250,000 payment to the state—and marks the first action by a state attorney general for violations of . . . (HIPAA) since . . . (HITECH) authorized state attorneys general to enforce HIPAA.").

134. *See* Press Release, Vt. Office of the Attorney Gen., Attorney General Settles Security Breach Allegations Against Health Insurer (Jan. 18, 2011) (on file with author).

135. *See id.* ("The case arises from a portable hard drive that contained protected health information, social security numbers, and financial information of approximately 1.5 million people, including 525 Vermonters.").

136. *See* Press Release, Attorney Gen. of Mass., South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations (May 24, 2012), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html ("In February 2010, South Shore Hospital shipped three boxes containing 473 unencrypted back-up computer tapes with 800,000 individuals' personal information and protected health information off-site to be erased. . . . In June 2010 South Shore Hospital learned that only one of the boxes arrived at its destination in Texas.").

137. *See id.*

138. *See infra* Appendix A (assuming that the cases in which "[n]either the Resolution agreement nor the press release released by HHS state the exact number of individuals affected" involved many individuals, rather than one or two people).

139. *See infra* Appendix B.

And, all 15 (100%) of the 15 HIPAA Rules cases selected by state attorneys general for enforcement involved the PHI of groups, rather than individuals.[140] These trends were apparent in my own law practice. Using the HHS complaint portal,[141] I have assisted dozens of individual patients and insureds with the filing of timely, valid complaints against covered entities. These complaints contained direct, written, photographic, and sometimes even video evidence of intentional, flagrant, and repeated violations of the HIPAA Rules. Not one of my individual clients' complaints resulted in a settlement or penalty.

4. HHS Corrective Action in Non-Settlement and Non-Penalty Cases

In addition to the full text of its settlement agreements and proposed and final civil money penalty determinations, HHS also provides the public with 32 examples of investigated cases not selected for settlement or penalty that involve HIPAA Rules violations.[142] Twenty-five (78%) of these examples involve the PHI of one patient (or one patient plus one family member of that patient), whereas only six (18.75%) of the examples involve the PHI of groups of patients or insureds.[143] It appears, then, from the 32 examples of corrective action publicized by HHS on its website, that privacy and security violations involving one person's PHI are steered towards corrective action without settlement or penalty whereas violations involving the PHI of groups of patients and insureds may be steered towards settlement or penalty.

HHS's selection of cases involving the PHI of groups for settlement or penalty makes sense considering the agency's own regulations, which list factors to be considered by HHS in determining the amount of a civil money penalty.[144] "The number of individuals affected" by the violation is the first factor, among more than a dozen factors, to be considered by HHS in determining the amount of the penalty.[145] Mathematically, privacy and security violations involving the PHI of large numbers of patients and insureds

---

140. *See infra* Appendix C.

141. *See* Office for C.R., U.S. Dep't of Health and Human Servs., *Complaint Portal—File a Health Information Privacy Complaint*, HHS.GOV, https://ocrportal.hhs.gov/ocr/cp/wizard_cp.jsf (last visited Nov. 18, 2018).

142. *See* HHS, *All Case Examples*, *supra* note 91 (providing 32 illustrative examples of cases in which HHS obtained corrective action from a covered entity or business associate).

143. *See id.* (indicating that the first through eighth, 13th, 14th through 22nd, 24th through 28th, 30th, and 31st examples involve the PHI of only one patient or a patient and one family member; whereas the ninth, 11th, 12th, 23rd, 29th, and 32nd examples involve the PHI of groups of patients or insureds. The tenth example is unclear in terms of whether it involves the PHI of an individual or a group of persons).

144. *See* 45 C.F.R. § 160.408 (2017) (titled "Factors considered in determining the amount of a civil money penalty.").

145. *See id.* § 160.408(a)(1) ("In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate: . . . [t]he number of individuals affected . . . .").

will yield higher penalties, as well as higher settlement amounts, for HHS compared to violations involving the PHI of a single person. The catch is that individuals whose privacy and security rights have been intentionally, and many times flagrantly and repeatedly, violated by covered entities and business associates are unlikely to see their offenders penalized in the same way that groups are. That is, they are unlikely to experience the same sense of civil justice associated with the imposition of a settlement payment or monetary penalty. Perhaps HHS believes that the corrective action required by HHS in the cases not selected for settlement or penalty serves the same purpose. As discussed in Section III.B.3 below, however, the majority of examples of corrective action provided by HHS are prospective in nature. Prospective action does safeguard future rights, but it does little to remedy past harms.

B. TIMELINESS AND NATURE OF ENFORCEMENT

1. HHS Settlement Agreements

With respect to the 26,071 investigated cases in which HHS required a covered entity to change its privacy practices or take other corrective action, HHS provides no information stating how long it took each of the covered entities or business associates to change its practices or take the required action. However, in 52 of those 26,071 cases (i.e., the 52 cases in which HHS imposed a settlement amount and corrective action plan ("CAP") on the covered entity for potential violations of the HIPAA Rules), the length of time can be estimated from the full text of the publicly available settlement agreement and CAP.

To illustrate the length of time it can take HHS to enter into a settlement agreement, which can include settlement amounts as low as $25,000[146] and as high as $5.55 million,[147] and to illustrate the length of time it can take for the covered entity's corrective action obligations to begin, this Article will analyze the first, tenth, 20th, 30th, 40th, and 50th settlements agreements set forth at Appendix A to this Article. As described in detail below, these time frames range from more than two years to more than five years.

HHS entered into its first-ever resolution agreement and CAP with Seattle-based Providence Health & Services ("Providence") on July 15, 2008, approximately two and one-third years after the first privacy incident, dated September 29, 2005, that gave rise to HHS's investigation of Providence in

146. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and Complete P.T., Pool & Land Physical Therapy, Inc., at 2, ¶ 6 (U.S. Dep't Health & Human Servs. Feb. 2, 2016), [hereinafter Resolution Agreement, Complete PT], https://www.hhs.gov/sites/default/files/cpt-res-agreement.pdf (setting forth a resolution amount of $25,000).

147. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and Advocate Health Care Network, at 3, ¶ 6 (U.S. Dep't Health & Human Servs. July 8, 2016), https://www.hhs.gov/sites/default/files/Advocate_racap.pdf (setting forth a resolution amount of $5.55 million).

the first place.[148] Providence's CAP required Providence to revise its privacy policies and procedures, re-train its workforce members on those revised policies and procedures, and monitor its workforce's familiarity and compliance with the revised policies and procedures.[149] The CAP did not become effective until, at the earliest, 90 days after the CAP's execution date of July 15, 2008.[150] Approximately two and two-third years elapsed between the date of the first privacy incident that gave rise to HHS's investigation of Providence and the date of Providence's actual corrective action.[151]

HHS entered into its tenth resolution agreement and CAP with Massachusetts Eye and Ear Infirmary ("MEEI") on September 13, 2012, approximately two and one-third years after MEEI notified HHS of the breach that gave rise to HHS's investigation of MEEI.[152] The CAP, which required MEEI to revise its privacy and policies and procedures, train its workforce members on the revised policies and procedures, and monitor its workforce's familiarity and compliance with the revised policies and procedures, did not become effective until, at the earliest, 90 days after the CAP's execution date of September 13, 2012.[153] Approximately two and two thirds of a year elapsed between the date of the first privacy incident that gave rise to HHS's investigation of MEEI to the date of MEEI's actual corrective action.

HHS entered into its 20th resolution agreement and CAP with New York and Presbyterian Hospital ("NYP") on May 7, 2014, approximately three years and six months after NYP notified HHS of the breach that gave rise to HHS's

148. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and Providence Health & Servs., at 10 (U.S. Dep't Health & Human Servs. July 9, 2015) [hereinafter Resolution Agreement, Providence], https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/agreement.pdf (setting forth a full execution date of July 15, 2008); *id.* at 1 (noting that "laptops containing ePHI were left unattended and were stolen from [workforce] members of [Providence Health & Services]" on September 29, 2005); *infra* Appendix A, at row 1 (cataloguing HHS's settlement agreement with Providence).

149. *See* Resolution Agreement, Providence, *supra* note 148, app. A, at 3–8 (listing Providence's corrective action obligations); *id.* app. A, at 4 (requiring Providence, for example, to provide HHS with HIPAA-compliant policies and procedures within ninety days of the CAP's execution date).

150. *See id.* at 3–4.

151. *See id.* at 3–4; *id.* app. A, at 4.

152. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and Mass. Eye & Ear Infirmary, at 1 (U.S. Dep't Health & Human Servs. Sept. 13, 2012) [hereinafter Resolution Agreement, MEEI], https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf (noting that HHS received MEEI's breach notification on April 20, 2010); Press Release, U.S. Dep't of Health & Human Servs., Massachusetts Provider Settles HIPAA Case for $1.5 Million (Sept. 17, 2012), *available at* https://wayback.archive-it.org/3926/20150121155313/http://www.hhs.gov/news/press/2012pres/09/20120917a.html (noting a September 27, 2012, press release date); *infra* Appendix A, at row 10 (cataloguing HHS's settlement agreement with MEEI).

153. *See* Resolution Agreement, MEEI, *supra* note 152, app. A, at A-3 to A-8 (listing MEEI's corrective action obligations); *id.* app. A, at A-6 (requiring, for example, MEEI to designate a monitor within 90 days of the effective date of the CAP).

investigation of NYP.[154] The CAP required NYP to "[d]evelop and [i]mplement a [r]isk [m]anagement [p]lan," "[r]eview and [r]evise [its] [p]olicies and [p]rocedures on [i]nformation [a]ccess [m]anagement," "[i]mplement [new] [p]rocess[es] for [e]valuating [e]nvironmental and [o]perational [c]hanges," and "[d]evelop an [e]nhanced [p]rivacy and [s]ecurity [a]wareness [t]raining [p]rogram," among other requirements.[155] The corrective action obligations set forth in the CAP did not become effective until, at the earliest, 90 days after the CAP's execution date of May 7, 2014.[156] Approximately four years elapsed between the date of NYP's notification to HHS of NYP's breach and the date of NYP's actual corrective action.

HHS entered into its 30th resolution agreement and CAP with Complete P.T., Pool and Land Physical Therapy, Inc. ("Complete PT") on February 2, 2016, approximately three years and five months after HHS received the complaint that gave rise to HHS's investigation of Complete PT.[157] The CAP required Complete PT to remove patients' PHI from its public website, develop HIPAA-compliant privacy policies and procedures and distribute those policies and procedures to its workforce members, and train workforce members on such policies and procedures.[158] These corrective action obligations, including the obligation to remove patient PHI from Complete PT's website, did not become effective until, at the earliest, ten days after the CAP's execution date of February 2, 2016, or three and one-half years after HHS received the complaint giving rise to its investigation of Complete PT.[159]

---

154. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and the New York & Presbyterian Hosp., at 1 (U.S. Dep't Health & Human Servs. May 2014) [hereinafter Resolution Agreement, NYP 2014], https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/ny-and-presbyterian-hospital-settlement-agreement.pdf (noting that NYP notified HHS of a breach on September 27, 2010); Press Release, U.S. Dep't of Health & Human Servs., Data Breach Results in $4.8 Million HIPAA Settlements (May 7, 2014) [hereinafter NYP Press Release], *available at* http://wayback.archive-it.org/3926/20150618190123/http://www.hhs.gov/news/press/2014pres/05/20140507b.html ("[HHS] . . . initiated its investigation of [NYP] and Columbia University . . . following their submission of a joint breach report, dated September 27, 2010 . . . ."); *infra* Appendix A, at row 20 (cataloguing HHS's settlement agreement with NYP).

155. *See* Resolution Agreement, NYP 2014, *supra* note 154, app. A, at *2–7 (listing NYP's corrective action obligations).

156. *See id.* at 2–3; *id.* app. A, at *3 (requiring, for example, NYP to review its information access management policies and procedures within ninety days of the CAP's effective date).

157. *See* Resolution Agreement, Complete PT, *supra* note 146, at 11 (showing an execution date of February 2, 2016); *id.* at 1 (noting that HHS received a complaint regarding Complete PT on August 8, 2012); *infra* Appendix A, at row 30 (cataloguing HHS's settlement agreement with Complete PT).

158. *See* Resolution Agreement, Complete PT, *supra* note 146, at 6–9 (listing Complete PT's corrective action obligations and requiring Complete PT to remove PHI from its website within ten days of the effective date of the CAP).

159. *Id.* at 9 (noting that the "[r]emoval of PHI from [Complete PT's] [w]ebsite" must occur "[w]ithin 10 days of the [e]ffective [d]ate of [the Resolution] Agreement").

HHS entered into its 40th resolution agreement and CAP with St. Joseph Health ("SJH") on October 13, 2016, approximately four years and seven months after SJH notified HHS of the breach that gave rise to HHS's investigation of SJH.[160] The CAP required SJH to "[c]onduct an [e]nterprise-wide [r]isk [a]nalysis," "[d]evelop and [i]mplement a [r]isk [m]anagement [p]lan," revise its privacy policies and procedures, and train its workforce on the revised policies and procedures.[161] The compliance date for these corrective action obligations was, at the earliest, 240 days after the CAP's effective date of October 13, 2016.[162] Almost five and one-half years elapsed between the date SJH notified HHS of its breach and SJH's actual corrective action.

HHS entered into its 50th settlement agreement and CAP with 21st Century Oncology, Inc. ("21st Century") on December 28, 2017, approximately two years and two months after the first date (October 3, 2015) an unauthorized hacker likely obtained PHI from 21st Century in violation of the HIPAA Rules.[163] Among other obligations, the CAP requires 21st Century to "[c]omplet[e] [a] [r]isk [a]nalysis and [r]isk [m]anagement [p]lan," revise its policies and procedures, and implement an internal monitoring plan.[164] These corrective action obligations do not become effective until, at the earliest, 60 days after the CAP's execution date of December 28, 2017; that is, the last day of February 2018.[165] Approximately two years and four months will have elapsed between the date of the security incident and the date of 21st Century's actual corrective action.

In summary, the first, tenth, 20th, 30th, 40th, and 50th settlement agreements entered into by HHS with covered entities for potential violations of the HIPAA Rules show that covered entities are not required to correct

160. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and St. Joseph Health, at 11 (U.S. Dep't Health & Human Servs. Oct. 13, 2016) [hereinafter Resolution Agreement, SJH], https://www.hhs.gov/sites/default/files/signed-sjh-ra-and-cap.pdf (showing an execution date of October 13, 2016); *id.* at 1 (noting that SJH reported the relevant breach on February 14, 2012); *infra* Appendix A, at row 40 (cataloguing HHS's settlement agreement with SJH).

161. Resolution Agreement, SJH, *supra* note 160, at 6–8 (summarizing SJH's corrective action obligations).

162. *Id.* at 6 (requiring SJH's "[e]nterprise-wide [r]isk [a]nalysis" to be performed and submitted to HHS within 240 days of the effective date of the Resolution Agreement).

163. *See* Resolution Agreement between U.S. Dep't of Health & Human Servs. and 21st Century Oncology, Inc., at 1 (U.S. Dep't Health & Human Servs. Dec. 2017) [hereinafter Resolution Agreement, 21st Century Oncology], https://www.hhs.gov/sites/default/files/21co-ra_cap.pdf (referencing the October 3, 2015, unauthorized access date); 21st Century Press Release, *supra* note 106 (showing a December 28, 2017, press release date); *infra* Appendix A, at row 50 (cataloguing HHS's settlement agreement with 21st Century).

164. *See* Resolution Agreement, 21st Century Oncology, *supra* note 163, at 6–15 (listing the corrective action obligations of 21st Century Oncology).

165. *See id.* at 9 (requiring 21st Century to select an independent assessor within 60 days of the effective date of the CAP).

their problematic practices, policies, and procedures until, at the earliest, approximately two and one-half years after the date of the first incident or the breach notification that gave rise to HHS's investigation of the covered entity in the first place. One covered entity (St. Joseph Health) had much longer —approximately five and one-half years—to take corrective action. Clinical issues raised by these time periods are discussed in the sub-section immediately below.[166]

2. HHS Civil Money Penalties

In addition to its 52 settlement agreements, which resolve potential violations of the HIPAA Rules, HHS also has imposed civil money penalties on four covered entities following formal findings of non-compliance with the HIPAA Rules and after attempts to obtain corrective action and/or settlement failed.[167] Although the first civil money penalty case involving Cignet Health Center took approximately two years and two months from the date of the first HIPAA Rules violation to the date of penalty imposition,[168] the second, third, and fourth civil money penalty cases took significantly longer to resolve. In particular, HHS's imposition of a civil money penalty against Lincare, Inc. took approximately seven years and four months from the date of the very first privacy incident that gave rise to Lincare's investigation.[169] Similarly, HHS's imposition of a civil money penalty against Children's Medical Center of Dallas ("Children's") took approximately seven years and two months from the date of the very first privacy incident that gave rise to HHS's investigation of Children's.[170] HHS's recent imposition of a civil money penalty against the University of Texas MD Anderson Cancer Center ("MD Anderson") took

166. *See infra* Section III.B.2.

167. *See infra* notes 168–71 (referencing the four civil money penalty cases, documented by HHS in notices of final penalty determinations); *infra* Appendix B (cataloguing the four cases in which HHS imposed a civil money penalty on a covered entity).

168. Notice of Final Determination, Cignet, *supra* note 9, at 1 (noting a February 4, 2011, civil money penalty imposition date); Notice of Proposed Determination, Cignet, *supra* note 9, at Attachment A (noting that Cignet failed to provide patients with access to their medical records starting in November 2008 and proceeding throughout 2009).

169. *Compare* Notice of Final Determination, Lincare, *supra* note 83, at *2 (stating the civil money penalty due date as "due upon Lincare's receipt of [the] Notice of Final Determination," which is dated March 1, 2016), *with* Notice of Proposed Determination, Lincare, *supra* note 82, at 2 (noting that "the [c]omplainant stat[ed] that he found . . . PHI under a bed and in a kitchen drawer in approximately November 2008").

170. *Compare* Notice of Final Determination, Children's Med. Ctr., *supra* note 127, at 2 (stating that payment of funds is due "upon Children's receipt of [the] Notice of Final Determination," which is dated January 18, 2017), *with* Notice of Proposed Determination, Children's Med. Ctr., *supra* note 127, at 2 (noting that a workforce member of Children's Medical Center's lost "an unencrypted, non-password protected BlackBerry device at the Dallas/Fort Worth International Airport on November 19, 2009").

approximately six years and one month from the date of the very first privacy incident that gave rise to the government's investigation of MD Anderson.[171]

Interestingly, HHS did not appear to obtain corrective action from any of the four covered entities that paid civil money penalties to HHS for violations of the HIPAA Rules. News reports state that Cignet, the first penalty payor, actually refused to take corrective action and refused to cooperate with HHS during the federal investigation.[172] It is not clear whether the 41 patients who needed copies of their medical records from Cignet ever obtained them, even after Cignet paid its multi-million-dollar penalty. Similarly, Lincare, the second penalty payor, reportedly took "only minimal action to correct its policies and strengthen safeguards to ensure compliance with the HIPAA Rules," thus leading to its high penalty.[173] Children's Medical Center, the third penalty payor, also does not appear to have taken any corrective action. Indeed, HHS's press release announcing the Children's penalty states, "[a]lthough OCR prefers to settle cases and assist entities in implementing corrective action plans, a lack of risk management . . . can also cost covered entities a sizable fine."[174] The penalty payors' refusal or failure to completely correct their problematic privacy practices is consistent with statements made by former government regulators, who have explained that HHS does not have injunction or corrective action authority in cases that result in a civil money penalty.[175]

---

171. *Compare* Dir. of the Office for Civil Rights v. Univ. of Tex. MD Anderson Cancer Ctr., Docket No. C-17-854, Decision No. CR5111 (U.S. Dep't Health & Human Servs. June 1, 2018) (sustaining on June 1, 2018, the imposition of a civil money penalty on MD Anderson), *with* Notice of Proposed Determination from Marisa M. Smith, Reg'l Manager, Office for C.R., U.S. Dep't of Health & Human Servs., to Scott McBride, Baker & Hostetler 3 (Mar. 24, 2017), https://www.hhs.gov/sites/default/files/md-anderson-npd-signed.pdf (noting the theft of an unencrypted laptop of a workforce member of MD Anderson on April 30, 2012).

172. *See* John Commins, *Cignet Health Fined $4.3M for HIPAA Violations*, HEALTHLEADERS (Feb. 23, 2011), https://www.healthleadersmedia.com/innovation/cignet-health-fined-43m-hipaa-violations ("The civil money penalty for the violations was $1.3 million. During the investigations, however, Cignet allegedly ignored OCR's demands to produce the records. A federal court issued a default judgment against Cignet on March 30, 2010. On April 7, 2010, Cignet gave the medical records to OCR, allegedly with no efforts to resolve the complaints through 'informal means.' OCR alleged that Cignet also failed to cooperate with the investigation from March 17, 2009, to April 7, 2010, indicating 'Cignet's willful neglect to comply with the Privacy Rule.' The failure to cooperate with OCR added $3 million to the civil money payment, HHS said.").

173. Press Release, U.S. Dep't of Health & Human Servs., Administrative Law Judge Rules in Favor of OCR Enforcement, Requiring Lincare, Inc. to Pay $239,800 (Feb. 3, 2016), *available at* http://wayback.archive-it.org/3926/20170127185543/https://www.hhs.gov/about/news/2016/02/03/administrative-law-judge-rules-favor-ocr-enforcement-requiring-lincare-inc-pay-penalties.html.

174. Press Release, U.S. Dep't of Health & Human Servs., Lack of Timely Action Risks Security and Costs Money (Feb. 1, 2017), *available at* https://www.hhs.gov/about/news/2017/02/01/lack-timely-action-risks-security-and-costs-money.html (quoting Robinsue Frohboese, OCR Acting Director).

175. *See supra* notes 117–21 and accompanying text (discussing how in civil money penalty cases HHS lacks authority to grant injunctions or impose corrective actions).

A covered entity's violation of the HIPAA Rules, or refusal to take prompt corrective action, can be clinically problematic. Consider a patient who needs to see a specialist, such as an oncologist, because the cancer care the patient needs is outside the expertise of the general practitioner ("GP") who has been treating the patient. A delay by the GP in transferring or a refusal to transfer the patient's medical record to the oncologist could lead to a delay in surgery, chemotherapy, or radiation, which could result in the spread of the patient's cancer and a reduced chance of survival for the patient.

Consider, by further example, a patient for whom a risky surgery is recommended by one surgeon. The patient would be wise to obtain an opinion from a second surgeon and, indeed, many public and private health insurers will pay for that second opinion.[176] A delay by the first surgeon in transferring or a refusal by the first surgeon to transfer the patient's medical record to the surgeon who will provide the second opinion could result in the patient not receiving the second opinion and possibly undergoing a risky and medically unnecessary surgery, potentially leading to complications or death.

In summary, a covered entity's violation of an Individual Right or another provision within the HIPAA Privacy Rule is not just a legal and ethical problem, as is commonly thought.[177] The violation can also negatively impact patient health, safety, and welfare. In addition, a covered entity that ultimately takes corrective action imposed by HHS, even after a two-to-seven-year delay, may be helping to ensure that future patients have exercisable rights.[178] However, this Article argues that settlement agreements and CAPs that result in delayed corrective action, or the imposition of a civil money penalty without any corrective action, do nothing to remedy the past harm suffered by individuals whose rights have already been violated.

3. HHS Corrective Action in Non-Settlement and Non-Penalty Cases

Remember that HHS has required changes in privacy practices or other corrective action in 26,071 investigated cases in total, and that Appendices A

176. *See, e.g.*, AETNA INC., NOW INCLUDED IN YOUR HEALTH PLAN: A FIRST-RATE SECOND OPINION 1 (2014), https://www.aetna.com/content/dam/aetna/pdfs/aetna-international/memberkit/Flyer-Mem-Second-Opinion.pdf ("Your Aetna International health plan now enables you to get a second opinion for some conditions and treatments at no additional cost."); *Your Medicare Coverage: Second Surgical Opinions*, MEDICARE.GOV, https://www.medicare.gov/coverage/second-surgical-opinions (last visited Nov. 18, 2018) ("Medicare Part B . . . covers a second opinion in some cases for surgery that isn't an emergency. Medicare also will help pay for a third opinion if the first and second opinions are different.").

177. *See, e.g.*, TEX. HEALTH & SAFETY CODE ANN. § 181.102 (West 2017) (providing patients with a legal right to access their electronic health records); CODE OF MEDICAL ETHICS: PRIVACY, CONFIDENTIALITY & MEDICAL RECORDS Op. 3.3.1 (AM. MED. ASS'N 2016) ("[P]hysicians have an ethical obligation to manage medical records appropriately. This obligation encompasses . . . providing copies or transferring records to a third party as requested by the patient . . . .").

178. *But see* HHS, *Enforcement Highlights*, *supra* note 13 (stating that change resulting from corrective action imposed by HHS "is systemic and . . . affects all the individuals [the covered entity] serve[s]").

and B to this Article reference only 56 of these cases.[179] What happened in the other 26,015 investigated cases? Did HHS make the covered entity take corrective action within a day, or a week, or a month, of receiving a patient complaint or a breach notification from the covered entity? Did this corrective action actually remedy the harm suffered by the individual whose privacy or security rights were violated?

HHS provides only brief summaries of 32 of these other 26,015 cases on its website.[180] Although each case summary provides two or three examples of the prospective corrective action required by HHS of the covered entity, not one of the summaries states how long it took the covered entity to take the required action. In addition, most of the summaries do not mention any remedy for the harmed individual other than an acknowledgement that the individual's rights had been violated and/or an apology to the patient.[181]

For example, one of the case examples involved a hospital employee who failed to adhere to an agreed-upon privacy restriction requested by a patient in violation of the HIPAA Privacy Rule.[182] In particular, the employee left considerable PHI on the patient's home voicemail that was accessed by other family members, in contravention of the patient's agreed-upon request to be

---

179. *See infra* Appendices A, B.

180. *See* HHS, *All Case Examples*, *supra* note 91 (providing 32 illustrative examples of cases in which HHS obtained corrective action from a covered entity or business associate).

181. *See, e.g.*, *id.* (referring to the compliance enforcement case titled "Mental Health Center Corrects Process for Providing Notice of Privacy Practices," a case in which a covered entity failed to provide a patient with the entity's notice of privacy practices; stating that "the mental health center acknowledged that it had not provided the . . . notice" of privacy practices as required; making the covered entity "revise[] its intake . . . polic[ies] and procedures to specify that" future patients will be provided notices of privacy practices and retrain its staff regarding those policies); *id.* (referring to the compliance enforcement case titled "Private Practice Implements Safeguards for Waiting Rooms," a case in which "[a] staff member of a [private clinic] discussed HIV testing procedures with a patient in the waiting room, thereby disclosing" the patient's diagnosis to other individuals in the waiting room; identifying several corrective action measures that would prevent the unauthorized disclosure from occurring again, such as new policies and procedures designed to safeguard PHI and the training of staff on those policies); *id.* (referring to the compliance enforcement case titled "Radiologist Revises Process for Workers Compensation Disclosures," a case in which an employee of a radiology practice sent a patient's test result to the patient's employer without the patient's prior written authorization; requiring the radiology practice to apologize to the patient and to sanction the employee who made the unauthorized disclosure; also requiring the radiology practice to revise its policies and procedures); *id.* (referring to the compliance enforcement case titled "Dentist Revises Process to Safeguard Medical Alert PHI," a case in which a dental clinic placed a red HIV sticker on the outside of a medical record belonging to a patient with HIV and noting that the sticker could be seen by staff and other patients; requiring the dental clinic to adopt a new policy requiring the movement of all HIV stickers from the outside to the inside of patients' medical records; requiring the dental clinic to apologize to the patient in person and in writing).

182. *Id.* (referring to the compliance enforcement case titled "Hospital Implements New Minimum Necessary Policies for Telephone Messages"); *see* 45 C.F.R. § 164.522(a)(1)(iii) (2017) (requiring covered entities to adhere to agreed-upon restrictions).

contacted only at work.[183] In response, HHS required the covered entity to develop new voicemail policies and procedures and to train staff members on those new policies and procedures.[184] The summary provided by HHS does not indicate that the patient received any remedy for the violation of her privacy rights.

A second illustrative corrective action case involved a "hospital [that] released to the local media, without the patient's [prior written] authorization, copies of the patient's skull x-ray as well as a description of the [patient's] medical condition."[185] Following the information release, "[t]he local newspaper then featured on its front page the individual's x-ray and an article that included the date of the accident, the location of the accident, the patient's gender, a description of the patient's medical condition, and numerous quotes from the hospital about such unusual sporting accidents."[186] HHS required the hospital to develop a new policy and procedure and to train its staff members on that new policy and procedure.[187] The summary provided by HHS does not indicate that the patient received any remedy for the violation of his privacy rights.[188]

Only a handful of the 32 case summaries mention any type of remedy for the individual who suffered the privacy or security harm.[189] All but one of these cases involved a patient who was initially refused access to the patient's PHI but, after HHS's intervention, was subsequently given access.[190] In these access-to-PHI cases, it is unclear from HHS's summary how long the individual had to wait for a copy of his or her PHI and whether the PHI the individual

---

183. HHS, *All Case Examples*, *supra* note 91.

184. *Id.*

185. *Id.* (referring to the compliance enforcement case titled "Hospital Issues Guidelines Regarding Disclosures to Avert Threats to Health or Safety").

186. *Id.*

187. *Id.*

188. *Id.*

189. *See generally id.* (providing a list of HHS enforcement actions with a description of covered entities' improper actions and the remedy).

190. *See id.* (referring to the compliance enforcement case titled "Entity Rescinds Improper Charges for Medical Record Copies to Reflect Reasonable, Cost-Based Fees," a case in which a patient complained to HHS that "a covered entity failed to provide [the patient] access to his medical records"; noting that OCR told the covered entity to give the patient access to his medical records; further noting that the covered entity subsequently released the records to the patient but then charged the patient an illegal non-cost-based fee for such records; finally noting that the illegal fee also had to be corrected by HHS); *id.* (referring to the compliance enforcement case titled "Private Practice Revises Process to Provide Access to Records," involving a similar fact pattern in which "[a] private practice failed to honor an individual's request for a complete copy of her minor son's medical record"); *id.* (referring to the compliance enforcement case titled "Private Practice Revises Access Procedure to Provide Access Despite an Outstanding Balance," a case in which a physician believed he could refuse to give a patient a copy of the patient's medical record if the patient had an outstanding balance; noting that when HHS informed the physician that the existence of a balance did not affect the patient's legal right to access her medical records under the HIPAA Privacy Rule, the physician provided the requested medical records to the patient).

ultimately received was timely given the purpose for which the individual needed it, such as care by a subsequent treating physician or a second surgical opinion. In the one non-access-to-PHI case summary that mentions a remedy, the summary does not specify the remedy other than stating that the covered entity "mitigat[ed] . . . harm to the complainant."[191]

IV. A QUI TAM PROCESS

Section III.A of this Article found that HHS and state attorneys general focus their settlement and penalty efforts on cases involving groups of patients and insureds, leaving individuals whose privacy and security rights have been violated out of the government enforcement spotlight. Sections III.B.1 and III.B.2 of this Article found that the execution of settlement agreements and the imposition of civil money penalties takes a considerable amount of time —more than seven years in some cases—resulting in a lack of timely attention to the privacy and security rights of both groups and individuals. Section III.B.3 of this Article revealed that the corrective action required by HHS in cases that do not reach the settlement or penalty phase, when that information is made publicly available and is summarized by HHS for the public, tends to be prospective in nature. Although prospective action, such as the revision of policies and procedures and the re-training of workforce members, helps safeguard future rights, it does little to remedy past harms. Part III thus showed that HHS's current enforcement mechanisms do little to support individual rights to privacy and remedies for violations thereof.[192] The remainder of this Article responds to these limitations. That is, Parts IV, V, and VI propose new federal regulations, the first of which, set forth in this Part, would establish a process for qui tam plaintiffs who assist HHS in identifying and investigating HIPAA Rules violations to receive a percentage of any HHS settlement or penalty. Some background is necessary before proceeding to this point.

On February 17, 2009, President Obama signed HITECH into law.[193] HITECH directed the Government Accountability Office ("GAO") to submit to the Secretary of HHS within 18 months a report recommending methodologies pursuant to which an individual who is harmed by a violation of the HIPAA Rules may receive a percentage of any settlement with or penalty

191. *See id.* (referring to the compliance enforcement case titled "Health Sciences Center Revises Process to Prevent Unauthorized Disclosures to Employers Covered Entity").

192. *Cf.* Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 LOY. U. CHI. L.J. 175, 191–209 (2014) (arguing that HIPAA has failed to protect patient privacy against increasing technological threats, and that federal laws allowing state attorneys general to sue under HIPAA are also ineffective).

193. *See supra* text accompanying notes 40–45 (providing background information regarding the passage of ARRA, including HITECH).

imposed by HHS for such violation.[194] On August 9, 2010, the GAO timely issued its report.[195] The report identified and discussed three recovery models, including an individualized determination model, a fixed recovery model, and a hybrid model.[196]

The Secretary of HHS was supposed to consider these models and, within three years of the date of HITECH (i.e., by February 17, 2012), issue regulations selecting a model under which individuals harmed by violations of the HIPAA Rules could receive a percentage of any HHS settlement or penalty.[197] To date, HHS has yet to issue these regulations, due six years ago. In a PowerPoint presented by HHS on March 7, 2017, HHS apparently stated that these regulations were still on its "[l]ong-term [r]egulatory [a]genda."[198] And, in Spring 2018, the Office of Management and Budget posted a public notice on its regulatory agenda website stating that an advance notice of proposed rulemaking ("ANPRM") would be published in November 2018 and would request public input regarding how HHS should share HIPAA settlements and civil penalties with harmed individuals.[199] Academics, attorneys, consultants, and other professionals who work with the HIPAA Rules have been waiting a long time for these regulations. Many are frustrated by HHS's extreme regulatory delay in this area.[200] The title of this Article ("A Timely Right to Privacy") is drawn in part from this notable pause in agency rulemaking.

---

194. *See* 42 U.S.C. § 17939(c)(2) (2012) ("Not later than 18 months after [the date of the enactment of the law], the Comptroller General shall submit to the Secretary a report including recommendations for a methodology under which an individual who is harmed by an act . . . may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.").

195. *See* Letter from Lynn H. Gibson, Acting Gen. Counsel, U.S. Gov't Accountability Office, to the Honorable Kathleen Sebelius, Sec'y of Health and Human Servs. (Aug. 9, 2010) (on file with author) (providing the report on "Models for the Distribution of Civil Monetary Penalties" in letter form).

196. *See id.* at 3–10 (identifying and discussing these three models).

197. *See* 42 U.S.C. § 17939(c)(3) ("Not later than 3 years after [the date of enactment of the law], 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.").

198. Office for C.R., U.S. Dep't of Health & Human Servs., PowerPoint Presentation, HCCA 2017 Compliance Institute, at slide 3 (Mar. 7, 2017) (on file with author).

199. *See* Office of Mgmt. & Budget, Office of Info. & Regulatory Aff., *HIPAA Enforcement: Distribution of a Percentage of Civil Money Penalties or Monetary Settlements to Harmed Individuals*, REGINFO.GOV (Spring 2018), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201804&RIN=0945-AA04.

200. *See, e.g.*, Jeff Hardee, *How Will Proposed Additions to HIPAA Provisions Affect MSPs?*, SOLARWINDS MSP (Apr. 27, 2017), https://www.solarwindsmsp.com/blog/how-will-proposed-additions-hipaa-provisions-affect-msps (discussing the forthcoming regulations; noting that "[o]nly time will tell what effect this change will have in regard[] to HIPAA").

Much of Part III focused on the relative inability of individuals, versus groups, to see their HIPAA complaints trigger settlements or penalties.[201] Indeed, only four (7.69%) of the 52 cases selected by HHS for settlement involved an individual versus a group.[202] These settlements were entered into with Shasta Regional Medical Center (after senior leadership at Shasta spoke with numerous media outlets about an identifiable patient's condition without the patient's authorization),[203] New York and Presbyterian Hospital (after senior leadership at the hospital allowed a television film crew to film one dying and one distressed patient without the patients' authorization),[204] Memorial Hermann Health System (after senior leadership at the health system approved using a patient's name in a press release without the patient's authorization),[205] and St. Luke's-Roosevelt Hospital Center Inc. (after a St. Luke's employee faxed extremely sensitive HIV and mental health information to two patients' places of work).[206] Even though HHS collected a combined $5.26 million in settlement payments from these four covered entities,[207] the individuals whose privacy rights were violated in these cases received nothing. The groups of patients and insureds affected by the violations that led to the other 48 settlement agreements as well as the four civil money penalties also received nothing, even though complaints from some members of those groups spurred HHS to take its settlement or penalty action.

In response, this Article recommends that HHS publish a proposed rule responding to President Obama's call in HITECH, now nine years old, to allow private parties who bring HIPAA Rules violations to HHS to receive a percentage of any settlement amount or penalty recovered by HHS. This recommendation begs the question: What recovery model shall be set forth in this proposed rule? One option is a fixed recovery model, such as the model set forth in the federal False Claims Act ("FCA") with which many health care attorneys and whistleblowers are familiar.

The FCA creates civil liability for any person who "knowingly presents" a false claim for payment to the federal government, such as a false Medicare claim; knowingly uses a false record, such as a false medical record or false billing record, to induce the government to pay such false claim; conspires

---

201. *See, e.g.*, *supra* Sections III.A.1–.3.

202. *See supra* Section III.A.

203. *See* Resolution Agreement, Shasta Reg'l, *supra* note 111, at 1–2 (summarizing the case); *infra* Appendix A, at row 13 (cataloguing the case).

204. *See* NY Med Press Release, *supra* note 112 (summarizing the case); *infra* Appendix A, at row 34 (cataloguing the case).

205. *See* Texas Health Press Release, *supra* note 114 (summarizing the case); *infra* Appendix A, at row 48, col. 5.

206. *See* Resolution Agreement, St. Luke's-Roosevelt, *supra* note 115, at 1; *infra* Appendix A, at row 49, col. 5 (cataloguing the case).

207. *See infra* Appendix A, at rows 13, 34, 48, & 49, col. 4 (listing the settlement amounts in each of these four cases).

with respect to the preceding conduct; or knowingly uses a false statement to decrease an obligation to pay money to the government, among other conduct.[208] Knowing conduct includes conduct involving "actual knowledge" of a falsehood, as well as conduct involving "deliberate ignorance" or "reckless disregard of the truth."[209] Individuals who violate the FCA are "liable to the [federal] [g]overnment for a civil penalty of not less than $5,000 and not more than $10,000, as adjusted by the Federal Civil Penalties Inflation Adjustment Act of 1990 [("FCPIA")], . . . plus [three] times the amount of damages . . . sustain[ed] [by the government] because of the act of that person."[210]

The FCA permits a private individual (called a whistleblower, qui tam plaintiff,[211] or qui tam relator) who has knowledge of past or present fraud committed against the federal government to bring a suit in the government's name and on the government's behalf.[212] "If the [g]overnment proceeds with [the] action brought by a [private] person," the private person can "receive at least 15[%] but not more than 25[%] of the proceeds of the action or settlement of the claim, depending upon the extent to which the person substantially contributed to the prosecution of the action," as well as "reasonable attorneys' fees," costs, and expenses.[213] "If the [g]overnment does not proceed with [the] action," the private person can receive an amount "not less than 25[%] and not more than 30[%] of the proceeds of the action or settlement," as well as "reasonable attorneys' fees," costs, and expenses.[214] Thus, the FCA not only allows, but actually encourages, individuals with knowledge of government fraud to quickly complete a significant portion of the investigatory legwork necessary to prove a violation of the FCA which, in turn, can result in a remedy, or bounty, for the individual.[215]

---

208. 31 U.S.C. § 3729(a)(1)(A), (B), (C), (G) (2012).

209. *Id.* § 3729(b)(1)(A).

210. *See id.* § 3729(a)(1) (setting forth these statutory amounts); 28 C.F.R. § 85.5 (2017) (setting forth, in table form, the higher, inflated amounts that currently apply to violations of the FCA and other statutes under the FCPIA).

211. The term "qui tam" is derived "from the Latin phrase '*qui tam pro domino rege quam pro se ipso in hac parte sequitur*,' which means he 'who pursues this action on our Lord the King's behalf as well as his own.'" Pamela H. Bucy, *Federalism and False Claims*, 28 CARDOZO L. REV. 1599, 1600 (2007) (translating and discussing the term); *see, e.g.*, J. Randy Beck, *The False Claims Act and the English Eradication of* Qui Tam *Legislation*, 78 N.C. L. REV. 539, 550 (2000) (discussing the meaning of the phrase).

212. *See* 31 U.S.C. § 3730(b) (allowing a private person to bring a civil action for violations of 31 U.S.C. § 3729).

213. *Id.* § 3730(d)(1).

214. *Id.* § 3730(d)(2).

215. *See, e.g.*, William E. Kovacic, *Whistleblower Bounty Lawsuits as Monitoring Devices in Government Contracting*, 29 LOY. L.A. L. REV. 1799, 1821–25 (1996) (providing an excellent discussion of the advantages and disadvantages of the FCA's qui tam provisions; on the advantage side, focusing on the costs associated with government audits and inspections, the strength of the inside knowledge possessed by employees compared to the superficial observations of external auditors and

I recommend that HHS adopt a similar approach for HIPAA Rules violations in a proposed rule that shall be codified as new 45 C.F.R. § 160.428. This new proposed rule shall include sub-sections that: (1) give private individuals the authority to bring an action in the name of HHS for violations of subparts C, D, or E of part 164 of Title 45 of the Code of Federal Regulations (i.e., the HIPAA Rules); (2) establish the process by which such individuals shall bring an action in the name of HHS; (3) set forth the time frames within which HHS shall review such actions and decide whether to proceed with such actions; (4) state that HHS has the right not to proceed with any particular action; and (5) establish the amounts, or amount ranges, in percentage terms, that the private individual may recover if HHS proceeds with the action and collects a settlement or penalty for a violation of the HIPAA Rules.

In the preamble to the proposed rule, HHS shall request comments from the general public as well as academics, attorneys, whistleblowers, and other individuals who are familiar with the benefits and limitations of the FCA's qui tam provisions[216] upon which this proposed rule is based. HHS shall edit the proposed regulation in its final rule after considering the comments it receives during the notice-and-comment rulemaking process. When the rule becomes effective, it will provide a much-needed remedy to individuals who assist HHS in identifying and investigating HIPAA Rules violations that lead to settlements and penalties.[217]

V. A PRIVATE RIGHT OF ACTION

"*Ubi jus, ibi remedium.* Where there is a right, there must be a remedy."[218] The qui tam process proposed above would provide a remedy to those who assist HHS in identifying and investigating HIPAA Rules violations that lead to settlements and penalties. Through August 1, 2018, however, HHS only imposed settlements or penalties in 56 cases.[219] The qui tam process identified above could help individuals in these 56 cases, but only in these 56 cases. Individuals and groups whose cases were not selected for settlement or penalty would have no federal remedy due to the lack of a private right of

---

inspectors, and the ability of an employee with inside knowledge to quickly and correctly identify and assess relevant information at a lower cost than an external government observer).

216. 31 U.S.C. § 3730(b)–(g) (codifying the FCA's qui tam provisions).

217. *Cf.* Press Release, U.S. Dep't of Justice, 21st Century Oncology to Pay $26 Million to Settle False Claims Act Allegations (Dec. 12, 2017), *available at* https://www.justice.gov/opa/pr/21st-century-oncology-pay-26-million-settle-false-claims-act-allegations (noting that a whistleblower "will receive $2,000,000 as his share of the recovery associated with the" $26 million FCA case the relator brought to, and in the name of, the U.S. Government).

218. *See, e.g.*, Tracy A. Thomas, Ubi Jus, Ibi Remedium: *The Fundamental Right to a Remedy Under Due Process*, 41 SAN DIEGO L. REV. 1633, 1636 (2004) ("Stated simply: *Ubi jus, ibi remedium.* Where there's a right, there must be a remedy.").

219. *See infra* Appendices A, B (cataloguing the 52 settlements and the four civil money penalty cases, respectively).

action in the HIPAA Rules.[220] This Part responds by recommending a second new federal regulation that would establish a private right of action for violations of the HIPAA Rules. Some background is necessary before proceeding to this point.

When a statute lacks a private right of action, an individual who is harmed by a violation of that statute cannot file a lawsuit in federal or state court seeking damages or an injunction designed to remedy the harms caused by the statute violation. The case of *Beaulieu v. Frisbie Memorial Hospital*[221] illustrates this legal point. In *Beaulieu*, pro se plaintiff Christopher Beaulieu sued Frisbie Memorial Hospital, alleging that the hospital violated the HIPAA Privacy Rule when it disclosed Beaulieu's brother's medical records to Beaulieu without his brother's prior written authorization, causing Beaulieu "a lot of stress and emotional problems."[222]

In a very brief judicial opinion, the U.S. District Court for the District of New Hampshire stated:

> Beaulieu brings this action under HIPAA and the HIPAA Privacy Rule, neither of which creates a private right of action. "Rather, a patient must file a written complaint with the Secretary of Health and Human Services through the Office of Civil Rights. It is then within the Secretary's administrative discretion whether to investigate complaints and conduct compliance reviews to determine whether covered entities are in compliance." Accordingly, Beaulieu has failed to state a viable cause of action for the improper release of his brother's medical records, and the complaint should be dismissed.[223]

Although an individual cannot currently sue in federal or state court for a violation of the HIPAA Rules, an individual can find an analogous common law cause of action and file a lawsuit stating that cause of action instead. For example, in *R.K. v. St. Mary's Medical Center*, a patient sued a hospital alleging numerous state law tort claims following the hospital's unauthorized disclosure of the patient's confidential health information.[224] Although the

---

220. *See supra* note 70 (citing case law rulings that no private right of action exists for HIPAA Rules violations).

221. Beaulieu v. Frisbie Mem'l Hosp., No. 12-cv-191-JD, 2012 WL 4857036 (D.N.H. Sept. 18, 2012).

222. *Id.* at *1.

223. *Id.* (footnote omitted) (citations omitted) (quoting Spencer v. Roche, 755 F. Supp. 2d. 250, 271 (D. Mass. 2010)).

224. *See, e.g.*, R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 717-18 (W. Va. 2012) (stating common law "negligence, outrageous conduct, intentional infliction of emotional distress, negligent infliction of emotional distress, negligent entrustment, breach of confidentiality, [and] invasion of privacy" claims following the patient's discovery that his confidential health information had been accessed by the defendant's employees and disclosed by such employees to the plaintiff's estranged wife and the wife's attorney).

hospital filed a motion to dismiss, alleging that the patient's state law tort claims were preempted by the HIPAA Rules and arguing that HIPAA contains no private right of action, the court disagreed, ruling that the patient's common law claims could proceed since they were not preempted by HIPAA.[225]

Although many states support common law causes of action for the unauthorized disclosure of identifiable patient information,[226] the catch is that the HIPAA Rules contain a number of other rights and protections, including those set forth in the Individual Rights and the Administrative Requirements, for which there is no analogous common law duty or cause of action. For example, most states do not require covered entities to provide their patients with notices of privacy practices.[227] Most states also do not require covered entities to give patients the right to request additional privacy restrictions,[228] or to amend their PHI,[229] or to receive an accounting of disclosures of their PHI.[230] Many states also do not require covered entities to adopt physical, technical, and administrative safeguards designed to protect the privacy of PHI.[231] Two out of three of the violations committed by the physician in the hypothetical that opened this Article are codified in the Individual Rights and Administrative Requirements, not the Use and Disclosure Requirements. Violations of the Individual Rights and Administrative Requirements have caused my clients tremendous harm over the past 15 years, yet most states do not address these issues.

---

225. *Id.* at 721 ("[W]e have located sufficient authority to clearly demonstrate that HIPAA does not preempt state-law causes of action for the wrongful disclosure of health care information.").

226. *See, e.g.*, Fairfax Hosp. *ex rel.* INOVA Health Sys. Hosps. v. Curtis, 492 S.E.2d 642, 643–45 (Va. 1997) (holding that a health care provider does owe a patient a duty not to disclose patient information without the patient's authorization; upholding a $100,000 jury verdict for the patient); MacDonald v. Clinger, 466 N.Y.S.2d 801, 802, 805 (N.Y. App. Div. 1982) (holding that a patient may bring an action sounding in tort law against a psychiatrist who "disclos[es] personal information learned during the course of treatment" to the patient's wife for "breach of . . . fiduciary duty of confidentiality").

227. *Cf.* 45 C.F.R. § 164.520(c)(2) (2017) (memorializing the HIPAA Privacy Rule provision requiring direct health care providers to give patients a notice of privacy practices at the date of first service delivery).

228. *Cf. id.* § 164.522(a)(1)(i), (iii) (memorializing the HIPAA Privacy Rule provision giving individuals the right to request additional privacy restrictions and obligating covered entities to adhere to agreed-upon restrictions).

229. *Cf. id.* § 164.526(a)(1) (memorializing the HIPAA Privacy Rule provision giving individuals the right to request amendment of their PHI).

230. *Cf. id.* § 164.528(a)(1) (memorializing the HIPAA Privacy Rule provision giving individuals the "right to receive an accounting of disclosures of [PHI]").

231. *Cf. id.* § 164.530(c)(1) (memorializing the HIPAA Privacy Rule provision requiring covered entities to establish safeguards to protect PHI). *See generally* Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy* (forthcoming) (cataloguing and assessing generally applicable state privacy, security, and breach notification laws; reporting that less than half of states have generally applicable data security laws).

In addition, although some states allow plaintiffs to use federal regulations, such as the HIPAA Privacy Rule, to establish a duty, and then a violation of the regulation to establish a breach of duty sufficient to state the negligence per se ("NPS") cause of action, not all states do. In *I.S. v. Washington University*, for example, the Eastern District of Missouri held that a provision in the HIPAA Privacy Rule could be used to establish a duty for purposes of NPS under Missouri Law.[232] On the other hand, in *Sheldon v. Kettering Health Network*, the Court of Appeals of Ohio held that the HIPAA Rules could not be used to establish a duty for purposes of NPS under Ohio law.[233] The Court in *Sheldon* reasoned that "utilization of HIPAA as an ordinary negligence 'standard of care' [for purposes of NPS was] tantamount to authorizing a prohibited private right of action for violation of HIPAA itself."[234]

Given that patients and insureds who are injured by violations of the Individual Rights and the Administrative Requirements have few remedies, especially in states such as Ohio, this Article recommends that HHS publish a proposed rule authorizing private rights of action for violations of the HIPAA Rules. The proposed rule, to be codified at new 45 C.F.R. § 160.430, shall be modeled after the private right of action set forth in the federal Emergency Medical Treatment and Active Labor Act ("EMTALA"), with which many health care attorneys are familiar.[235]

As background, EMTALA requires Medicare-participating hospitals with emergency departments to provide individuals who request examination and treatment an appropriate medical screening examination.[236] If, through the screening examination, the patient is determined to have an emergency medical condition, the hospital must provide the patient with necessary stabilizing treatment[237] or appropriately transfer the patient to another medical facility that can stabilize the patient,[238] all without regard to the patient's ability to pay.

Like HIPAA, HHS can impose civil money penalties on hospitals that violate EMTALA.[239] Unlike HIPAA, however, EMTALA also contains a private

---

232. I.S. v. Wash. Univ., No. 4:11CV235SNLJ, 2011 WL 2433585, at *2 (E.D. Mo. June 14, 2011) ("[T]he Court finds that Count III may stand as a state claim for [NPS] despite its exclusive reliance upon HIPAA.").

233. Sheldon v. Kettering Health Network, 40 N.E.3d 661, 672 (Ohio Ct. App. 2015) ("[W]e further conclude that federal regulations—as opposed to an Ohio statute that sets forth a positive and definite standard of care—cannot be used as a basis for [NPS] under Ohio law.").

234. *Id.*

235. *See* 42 U.S.C. § 1395dd (2012) (codifying EMTALA); *id.* § 1395dd(d)(2)(A) (establishing a private right of action for patients injured by EMTALA violations).

236. *Id.* § 1395dd(a).

237. *Id.* § 1395dd(b)(1)(A).

238. *Id.* § 1395dd(b)(1)(B).

239. *See id.* § 1395dd(d)(1)(A) (authorizing HHS to impose "civil money penalt[ies] of not more than $50,000" on hospitals with 100 or more beds, or not more than $25,000 on hospitals

cause of action allowing individuals harmed by violations of EMTALA to sue a hospital for damages in court under state law.[240] This private cause of action recognizes that HHS cannot possibly audit every Medicare-participating hospital across the United States for violations of EMTALA and cannot timely enforce all of the violations it identifies through audits, compliance reviews, or complaints.

This Article therefore recommends that HHS propose a similar right of action for incorporation into the HIPAA Rules. The proposed regulation shall provide:

> 45 C.F.R. § 160.430. Civil Enforcement—Personal Harm.
>
> Any individual who suffers personal or financial harm as a direct result of a covered entity or business associate's violation of subpart C, D, or E of part 164 of title 45 of the Code of Federal Regulations may, in a civil action against the covered entity or business associate, obtain those damages available for such injuries under the law of the State in which the covered entity or business associate is located, and such equitable relief as is appropriate.

In the preamble to the proposed rule, HHS shall request comments from the general public, including academics, attorneys, and other individuals who are familiar with the benefits and limitations of EMTALA's private right of action. HHS shall edit its proposed rule after considering the valuable comments it will receive during the notice-and-comment rulemaking process. When the rule becomes effective, it will provide a much-needed remedy to individuals who are unable to enforce their privacy and security rights through the administrative complaint process established by HHS.[241]

VI. EXCLUSION AUTHORITY

Finally, this Article also recommends that HHS adopt a regulation authorizing the Office of Inspector General ("OIG") to exclude any covered

---

with fewer than 100 beds, for violations of EMTALA); *id.* § 1395dd(d)(1)(B) (authorizing HHS to impose "civil money penalt[ies] of not more than $50,000" on physicians who negligently violate their on-call and other duties under EMTALA).

240. *See id.* § 1395dd(d)(2)(A) (labeling the section "Civil Enforcement—Personal Harm").

241. *Cf.* Jackson v. East Bay Hosp., 980 F. Supp. 1341, 1343, 1348 (N.D. Cal. 1997) (allowing plaintiff Barbara Jackson to bring a private action under EMTALA for damages arising from the wrongful death of and personal injury to Robert Jackson, her husband). *Compare* Jack Brill, Note, *Giving HIPAA Enforcement Room to Grow: Why There Should Not (Yet) Be a Private Cause of Action*, 83 NOTRE DAME L. REV. 2105, 2107 (2008) (concluding in 2008—a decade ago—that "the costs of a [HIPAA] private [right] of action . . . outweigh[ed] the benefits" and predicting, "with time, [that] HIPAA compliance . . . [would] increase" without a private cause of action), *with* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 354–59 (2007) (justifying and recommending a HIPAA private right of action).

entity from participating in the Medicare and Medicaid Programs if the entity grossly and flagrantly, or repeatedly, violates the HIPAA Rules. Some background is necessary before proceeding to this final point.

Even in health law contexts in which there is a process for qui tam relators and/or a private right of action, it may be economically efficient for an actor to engage in proscribed behavior because the benefits of the behavior outweigh the risks of the behavior. Consider, for example, a covered entity that is offered $200,000 for the sale of PHI relating to a famous patient. The civil money penalty for the one-time sale of the PHI, if a penalty is imposed by HHS, may be in the range of $50,000.[242] In addition, in cases in which patients have sued covered entities under state common law for the one-time wrongful disclosure of patient information, the damages tend to be in the very rough range of approximately $100,000 per wrongful disclosure.[243] Thus, a rational covered entity may decide to violate the HIPAA Rules by selling the famous patient's PHI because the payment for the sale of the PHI ($200,000) exceeds the sum of the expected civil money penalty by HHS and the expected damages in the private lawsuit ($150,000).

Because rational health industry participants may decide to engage in proscribed behavior in situations in which the benefits of the behavior outweigh the risks, this Article recommends that HHS adopt a third regulation authorizing the OIG to exclude a covered entity from the Medicare and Medicaid Programs. This regulation would serve as a final deterrent to behavior proscribed by the HIPAA Rules.

The government successfully uses exclusion as a compliance tool in other health law contexts. For example, Medicare-participating facilities that pose an immediate jeopardy to a Medicare beneficiary's physical health or safety can lose their Medicare-participating status within 23 days if the unsafe conditions are not immediately corrected.[244] In my practice, I frequently helped my Medicare-participating clients respond to these 23-day termination threats from the federal government. I assisted my clients in quickly putting an end to the dangerous conduct, removing the dangerous conditions, or adopting prospective plans of correction so that they would not lose their ability to participate in the Medicare Program. The potential loss of federal health care program dollars was a tremendous compliance incentive for my clients. Many health care providers and health care facilities rely heavily on

---

242. *See* 45 C.F.R. § 160.404(b)(2)(iii)(A) (2017) (stating that the appropriate civil money penalty range for violations of the HIPAA Rules that are due to willful neglect but that are corrected within 30 days is $10,000 to $50,000).

243. *See, e.g.*, Fairfax Hosp. *ex rel.* INOVA Health Sys. Hosps., Inc. v. Curtis, 492 S.E.2d 642, 643–44, 648 (Va. 1997) (upholding a $100,000 jury verdict for a patient in a case in which the patient's provider disclosed the patient's information without the patient's authorization).

244. *See* 42 C.F.R. § 488.410(a) ("If there is immediate jeopardy to resident health or safety, the State must (and [the Centers for Medicare and Medicaid Services] does) either terminate the provider agreement within 23 calendar days of the last date of the survey or appoint a temporary manager to remove the immediate jeopardy.").

Medicare and Medicaid reimbursement and the loss of such reimbursement is considered a financial death sentence in the health industry.[245]

This Article therefore recommends that HHS propose a third and final new regulation for incorporation into the HIPAA Rules. This proposed regulation shall provide:

> 45 C.F.R. § 160.432. Exclusion from Government Programs.
>
> A covered entity that grossly and flagrantly, or repeatedly, violates a provision in subpart C, D, or E of part 164 of title 45 of the Code of Federal Regulations shall be subject to exclusion from participation in subchapter XVIII of title 42 of the United States Code as well as State health care programs.

HHS shall request comments on this proposed rule not only from the general public, but also from academics, attorneys, and other individuals who are familiar with EMTALA's exclusion provision, on which this proposed rule is based. HHS shall edit its proposed rule after considering the comments it receives during the notice-and-comment rulemaking process. When this rule becomes effective, it should provide a sufficient, and final, deterrent for covered entities considering whether to violate the HIPAA Rules.[246]

---

245. *See, e.g.*, Thomas Sullivan, *HHS OIG: Medicare and State Healthcare Programs: Fraud and Abuse–OIG Proposes Revisions to Exclusion Authorities and "Early Reinstatement" for Certain Healthcare Providers*, POL'Y & MED., https://www.policymed.com/2014/05/hhs-oig-medicare-and-state-health-care-programs-fraud-and-abuse-revisions-to-the-office-of-inspector-generals-exclusion.html (last updated May 6, 2018) ("[E]xclusion . . . is referred to by many as a 'kiss of death' or 'death sentence' due to the fact that Medicare and Medicaid are often vital revenue sources for providers."). As an illustration, consider Dr. George E. Sloan, a randomly selected hematologist/oncologist who practices medicine in Indiana. *See* Community Healthcare System, *Find a Doctor: George Sloan, M.D. Oncology-Hematology*, COMMUNITY HEALTHCARE SYS. https://www.comhs.org/find-a-doctor/s/sloan-george (last visited Nov. 18, 2018) (summarizing Dr. Sloan's areas of practice). In 2015, Dr. Sloan received $2,164,385 in reimbursement from the Medicare Program. *See Medicare Unmasked*, WALL ST. J., graphics.wsj.com/medicare-billing/#/name=sloan&special=&city=&state (last visited Nov. 18, 2018) (providing Dr. Sloan's total Medicare reimbursement in 2015). The threat of that reimbursement loss, even for one year, likely would deter Dr. Sloan from violating the HIPAA Rules. Further consider Tenet Desert Health System Inc., a randomly selected ambulatory surgery center ("ASC") located in Palm Springs, California. Alex Kacik, *Tenet Ups Stake in Ambulatory Surgery Center Chain*, MOD. HEALTHCARE (Apr. 26, 2018), http://www.modernhealthcare.com/article/20180426/NEWS/180429918; *Tenet Healthsystem Desert Inc.*, MANTA, https://www.manta.com/c/mm463jx/tenet-healthsystem-desert-inc (last visited Nov. 18, 2018). The ASC received $2,109,261 in Medicare reimbursement in the year 2015. *See Medicare Unmasked*, *supra*. Again, the threat of that reimbursement loss, even for just one year, should deter the ASC from violating the HIPAA Rules.

246. *Cf.* Oulton v. Bowen, 674 F. Supp. 429, 430, 438 (W.D.N.Y. 1987) (denying a psychiatric hospital's motion for a preliminary injunction to prevent HHS from excluding it from the Medicare Program for violating staffing and other Medicare conditions of participation); Kahn v. Inspector Gen. of the U.S. Dep't of Health & Human Servs., 848 F. Supp. 432, 434, 437 (S.D.N.Y. 1994) (upholding the mandatory exclusion of a New York podiatrist from the Medicare Program for five years following his conviction for grand larceny); Greene v. Sullivan,

VII. CONCLUSION

This Article has carefully examined currently available federal and state enforcement actions involving the HIPAA and HITECH Rules. Showing how HHS and state attorneys general focus their settlement and penalty efforts on cases involving groups of patients and insureds, this Article has argued that individuals who suffer privacy- and security-related harms have received relatively little enforcement attention. This Article has also revealed that the execution of settlement agreements and the imposition of civil money penalties take a considerable amount of time—more than seven years in some cases—resulting in a lack of timely attention to the privacy and security rights of both groups and individuals. Finally, this Article has explained that the corrective action required by HHS in cases that do not reach the settlement or penalty phase, when that information is made publicly available, tends to be prospective but not remedial in nature. Although prospective action helps safeguard future rights, it does little to remedy past harms.

Arguing that HITECH's improved enforcement provisions have done little to support timely, individual rights to privacy and security, this Article has proposed structure and content for three new federal regulations that should be codified at 45 C.F.R. §§ 160.428, 160.430, and 160.432. If adopted by HHS, these regulations will: (1) establish a process pursuant to which qui tam plaintiffs can receive a percentage of any settlement or penalty imposed by HHS for HIPAA Rules violations; (2) create a private right of action for individuals harmed by HIPAA Rules violations; and (3) authorize the OIG to exclude any covered entity that grossly and flagrantly, or repeatedly, violates the HIPAA Rules from federal and state health care programs, including Medicare and Medicaid.

More broadly, this Article has also gently inquired as to the proper role of federal regulations that are not enforced, or that are enforced infrequently, both in general and with respect to particular individuals.[247] HHS has an abundance of health, safety, and welfare regulations[248] that can neither be audited nor enforced on a timely basis. As an illustration, HHS started in 2011, auditing covered entities for compliance with the HIPAA Rules.[249] Since

---

731 F. Supp. 835, 836, 838 (E.D. Tenn. 1990) (upholding the mandatory exclusion of a Tennessee pharmacist from the Medicare Program for five years for fraud).

247. *Cf.* Ryan Meade, *Call for Papers: Center for Compliance Studies 2018 Symposium "What is the Role of a Regulation if It Is Not Enforced?"*, LOY. U. CHI. (Sept. 4, 2017), http://blogs.luc.edu/compliance/2017/09/04/call-for-papers-center-for-compliance-studies-2018-symposium-what-is-the-role-of-a-regulation-if-it-is-not-enforced (asking this question of symposium participants).

248. *See, e.g.*, 42 C.F.R. pt. 482 (codifying regulations governing Medicare-participating hospitals); *id.* pt. 483 (codifying regulations applicable to Medicare and Medicaid-participating long-term care facilities); *id.* pt. 484 (codifying regulations governing the provision of home health services); *id.* pt. 493 (codifying regulations governing the provision of laboratory services); *id.* pt. 494 (codifying regulations governing "end-stage renal disease facilities").

249. *See* Office for C.R., U.S. Dep't of Health & Human Servs., *HIPAA Privacy, Security, and Breach Notification Audit Program*, HHS.GOV., https://www.hhs.gov/hipaa/for-professionals/

2011, HHS has audited 115 and 166 covered entities through its first and second rounds of HIPAA audits, respectively.[250] The United States is home, however, to more than 1.9 million Medicare-participating health care professionals, and that number does not include the hundreds of thousands of other individual and institutional providers, health plans, and health care clearinghouses that also meet the definition of a HIPAA covered entity.[251] Although HHS's audit results are helpful to academics and practitioners who wish to understand enforcement trends, the audits cannot be understood as a meaningful deterrent of HIPAA Rules violations.

The research findings set forth in Part III of this Article also raise questions regarding agency discretion in terms of cases selected for enforcement and, more broadly, the theory and purpose of health information privacy and security regulation. Will privacy and security cases involving groups always be preferred by HHS due to the HHS regulation that allows higher penalties for cases involving the PHI of more individuals?[252] Do privacy and security cases involving impermissible PHI uses and disclosures by senior leadership[253] garner significant enforcement attention simply because HHS hopes to use those actions to send strong messages to senior leadership to take HIPAA compliance seriously? If so, what about the individuals whose rights are violated by rank-and-file employees? Are their privacy and security rights any less important?[254]

---

compliance-enforcement/audit/index.html (last reviewed Dec. 1, 2016) (summarizing HHS's HIPAA compliance audits).

250. *See id.* (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).

251. *See* 45 C.F.R. § 160.103 (defining covered entity to include health plans, health care clearinghouses, and "health care provider[s] who transmit[] . . . health information in electronic form in connection with [standard] transaction[s]"); *Medicare Individual Provider List*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://data.cms.gov/Medicare-Claims/Medicare-Individual-Provider-List/u8ug-2upx/data (last visited Nov. 18, 2018) (showing 1,923,127 current and former individual providers in a search run on November 17, 2018).

252. *See* 45 C.F.R. § 160.408(a)(1) (listing "[t]he number of individuals affected" as the first factor to be considered by HHS in determining the amount of a civil money penalty).

253. *See supra* text accompanying notes 203–06 (referencing three cases involving impermissible PHI disclosures by senior leadership that led to HHS enforcement).

254. *See, e.g.*, Tobi M. Murphy, *Enforcement of the HIPAA Privacy Rule: Moving from Illusory Voluntary Compliance to Continuous Compliance Through Private Accreditation*, 54 LOY. L. REV. 155, 157–58 (2008) ("[C]onsider the additional number of smaller breaches that also likely occurred in the same time period, but were not newsworthy enough for an entire nation or region to read about. Despite the smaller scope of such incidents, it is doubtful these additional victims consider their individual privacy breach any less significant." (footnote omitted)); *id.* at 158 ("[R]egardless of the manner, scope, or location of a privacy breach, one thing remains the same: an individual's trust in the privacy of his or her personal health information was damaged.").

In addition, what is the exact theory behind HHS's regulation of health information privacy and security? According to public statements made by a former HIPAA regulator, HHS appears to be using its enforcement authority to simply: (1) identify cases involving various privacy, security, and breach notification issues; and (2) provide instruction (either through the publicly available corrective action plan or through the publicly available notice of proposed civil money penalty) regarding how covered entities and business associates should comply with various provisions within the HIPAA Rules.[255] HHS does not appear to be using its enforcement authority to actually try to enforce all HIPAA rules violations; indeed, HHS enters into a settlement or imposes a civil money penalty in only one-tenth of one percent (0.1%) of cases involving a valid and timely-filed complaint over which HHS has jurisdiction.[256] Whether the federal government lacks the desire or the capacity to penalize a greater number of non-compliant entities is unclear, although it is likely that one or both factors is at play.

Finally, is HHS consistently enforcing like violations? Do the cases that go to settlement or penalty involve worse covered entity behavior[257] or, perhaps, is HHS's selective enforcement of the HIPAA Rules a form of deregulation?[258] Going forward, it is my hope that both the data and recommendations set forth in this Article will assist experts in administrative law in considering these important questions in both health law and non-health law contexts.

---

255. *See* Polsinelli Webinar, *supra* note 117 (containing recorded statements by a former government regulator regarding HIPAA enforcement; explaining that HHS "identifi[es] . . . cases . . . they feel will send a message to the industry . . . . [w]here they can highlight different issues, . . . [including issues involving paper PHI under the HIPAA Privacy Rule and ePHI under the HIPAA] [S]ecurity [R]ule that will be instructive for other covered entities and business associates to understand . . . the different concerns that OCR continues to see over and over again . . . .").

256. As shown in Appendices A and B, HHS has entered into 52 settlement agreements and has imposed civil money penalties in four cases for a total of 56 settlement or penalty civil enforcement actions. *See infra* Appendices A, B. In comparison, HHS has received 54,521 valid, timely filed, HIPAA complaints over which HHS has jurisdiction. *See* HHS, *Enforcement Highlights*, *supra* note 13 (explaining that, in response to 26,071 of these complaints, HHS "require[ed] changes in privacy practices" or provided technical assistance; further explaining that, in 28,450 of these complaints, HHS "intervened early and provided technical assistance"). Dividing 56 settlements and penalties by 54,521 (26,071 + 28,450) yields a 0.1027% (slightly more than one-tenth of one percent) chance of a valid complaint resulting in a settlement or penalty, with the remainder receiving only technical assistance or minor changes in privacy practices.

257. Compare cases discussed in Sections III.A.4 and III.B.3 (involving corrective action that did not lead to settlement or penalty), with cases discussed in Sections III.A.1–.2 and III.B.1–.2 (leading to settlement or penalty). Both sets of cases involve like-natured violations.

258. *See* Danielle Ivory & Robert Faturechi, *The Deep Industry Ties of Trump's Deregulation Teams*, N.Y. TIMES (July 11, 2017), https://www.nytimes.com/2017/07/11/business/the-deep-industry-ties-of-trumps-deregulation-teams.html ("President Trump entered office pledging to cut red tape, and within weeks, he ordered his administration to assemble teams to aggressively scale back government regulations."); Eric Lipton & Danielle Ivory, *Trump Says His Regulatory Rollback Already Is the 'Most Far-Reaching,'* N.Y. TIMES (Dec. 14, 2017), https://www.nytimes.com/2017/12/14/us/politics/trump-federal-regulations.html ("President Trump said . . . that his administration was answering 'a call to action' by rolling back regulations on . . . health care . . . and other industries . . . .").

APPENDIX A:
HHS SETTLEMENT AGREEMENTS AND CORRECTIVE ACTION PLANS

	Name of Covered Entity or Business Associate	Number of Affected Individuals	Settlement Amount	Illustrative Covered Incidents	Date of Settlement Agreement
1.	Providence Health & Services et al.	>386,000	$100,000	Failure to safeguard the unencrypted ePHI of over 386,000 patients	July 2008
2.	CVS Pharmacy, Inc. et al.	"Millions of health care consumers"	$2,250,000	Disposal of paper PHI in open dumpsters; failure to train employees on proper safeguards	Jan. 2009
3.	Rite Aid Corporation et al.	†	$1,000,000	Disposal of paper PHI in open dumpsters; failure to train employees on proper safeguards	June 2010
4.	Management Services Organization Washington, Inc.	"Numerous individuals"	$35,000	Disclosure of ePHI for marketing purposes; insufficient safeguards	Dec. 2010

Legend:
BA Business Associate
BAA Business Associate Agreement
ePHI Electronic Protected Health Information
PHI Protected Health Information
PR Press Release by HHS
RA Resolution Agreement (i.e., settlement agreement plus corrective action plan)with HHS

* First HIPAA breach settlement by HHS involving fewer than 500 patients.

† Neither the Resolution agreement nor the press release released by HHS state the exact number of individuals affected. However, by the nature of the incident, it is reasonable to assume that the incident affected many individuals. In the press release announcing its settlement with Rite Aid, for example, HHS does not state how many patients' PHI had been discarded in dumpsters without their authorization in violation of the HIPAA Rules. However, HHS does state that it opened its investigation of Rite Aid "after television media videotaped incidents in which pharmacies were shown to have disposed of prescriptions and labeled pill bottles containing individuals' identifiable information in industrial trash containers that were accessible to the public. These incidents were reported as occurring in a variety of cities across the United States. Rite Aid pharmacy stores in several of the cities were highlighted in media reports."HHS's use of the plural words "incidents," "pharmacies" and individuals'," as well as the phrase "pill bottles" and "variety of cities," suggests that the PHI of many individuals was involved.

5.	The General Hospital Corporation and Massachusetts General Physicians Organization, Inc.	192	$1,000,000	Removal of unencrypted PHI in billing encounter forms and loss of daily office schedules containing PHI of 192 patients	Feb. 2011
6.	University of California at Los Angeles Health System	"Many Patients"	$865,000	Employee examination of the ePHI of many patients without reason	July 2011
7.	BlueCross BlueShield of Tennessee	1,023,209	$1,500,000	Theft of 57 unencrypted hard drives containing the PHI of 1,023,209 people	Mar. 2012
8.	Phoenix Cardiac Surgery, P.C.	"Over 1,000"	$100,000	Posting of ePHI on a public, Internet-based calendar; failure to document workforce training; failure to establish safeguards; failure to enter into BAAs when necessary	Apr. 2012
9.	Alaska Department of Health and Social Services	†	$1,700,000	Theft of portable hard drive containing ePHI from employee's vehicle; failure to conduct risk analysis and have proper policies and procedures	June 2012
10.	Massachusetts Ear and Eye Infirmary and Massachusetts Ear and Eye Associates, Inc.	†	$1,500,000	Theft of unencrypted personal laptop containing patient prescriptions and clinical information; failure to conduct risk analysis; failure to implement proper policies and procedures	Sept. 2012
11.	Hospice of North Idaho*	441	$50,000	Theft of laptop containing the ePHI of 441 patients; failure to conduct risk analysis; failure to adopt security measures	Dec. 2012

12.	Idaho State University	17,500	$400,000	Failure to secure the ePHI of 17,500 patients for ten months; failure to conduct risk analysis; failure to implement security measures	May 2013
13.	Shasta Regional Medical Center	1	$275,000	Disclosure of PHI about a patient to multiple media outlets and the entity's workforce without the patient's authorization; failure to safeguard PHI; failure to train workforce members; failure to sanction workforce members	June 2013
14.	Wellpoint, Inc.	612,402	$1,700,000	Impermissible disclosure of the ePHI of 612,402 individuals; failure to implement required policies and procedures; failure to have in place technical safeguards that verify the identities of individuals seeking access to ePHI	July 2013
15.	Affinity Health Plan, Inc.	≤ 344,579	$1,250,000	Disclosure of the ePHI of up to 344,579 individuals following failure to erase hard drives of leased photocopy machine	Aug. 2013
16.	Adult and Pediatric Dermatology, P.C.	≤ 2,200	$150,000	Disclosure of the ePHI of up to 2,200 individuals as a result of a stolen, unencrypted thumb drive; failure to conduct timely risk assessment; failure to timely comply with other administrative requirements	Dec. 2013
17.	Skagit County, Washington	1,581	$215,000	Disclosure of the ePHI of 1,581 individuals via public web server; failure to provide proper breach notification; failed to implement appropriate policies and procedures	Mar. 2014

18.	Concentra Health Services	†	$1,725,220	Theft of an unencrypted laptop containing ePHI; failure to follow up on prior risk assessments noting the risk of unencrypted ePHI; failure to implement policies and procedures	Apr. 2014
19.	QCA Health Plan, Inc.	148	$250,000	Theft of unencrypted laptop containing the ePHI of 148 individuals; failure to implement policies and procedures	Apr. 2014
20.	The New York Presbyterian Hospital	6,800	$3,300,000	Disclosure of the ePHI of 6,800 patients to Google and other search engines; failure to conduct risk analysis; failure to implement appropriate policies and procedures	May 2014
21.	Trustees of Columbia University in the City of New York	6,800	$1,500,000	Disclosure of the ePHI of 6,800 patients to Google and other search engines (network shared with The New York and Presbyterian Hospital, above); failure to conduct risk analysis	May 2014
22.	Parkview Health System, Inc. d/b/a Parkview Physicians Group f/k/a Parkview Medical Group	5,000 to 8,000	$800,000	Failure to safeguard the PHI of 5,000 to 8,000 individuals (by delivering and leaving 71 unsecured, cardboard boxes containing the medical records of those 5,000 to 8,000 individuals) on the driveway of a physician's home located within twenty feet of a public road	June 2014
23.	Anchorage Community Health Services, Inc.	2,743	$150,000	Malware breach of the unsecured ePHI of 2,743 individuals; failure to conduct risk assessment; failure to implement technical security measures	Dec. 2014

24.	Cornell Prescription Pharmacy	1,610	$125,000	Disposal of the unsecured PHI of 1,610 patients in an unlocked, open container; failure to implement required policies and procedures; failure to train workforce members	Apr. 2015
25.	St. Elizabeth's Medical Center	1,093	$218,400	Use of an internet-based document sharing application to store documents containing the ePHI of at least 498 individuals without conducting a risk assessment; breach of unsecured ePHI on a laptop and flash drive of an additional 595 individuals	July 2015
26.	Cancer Care Group, P.C.	55,000	$750,000	Theft of unencrypted computer server backup tapes containing the ePHI of 55,000 individuals from employee's car; failure to conduct risk assessment; failure to implement required policies and procedures	Aug. 2015
27.	Lahey Clinic Hospital, Inc.	599	$850,000	Theft of an unencrypted radiology/CT laptop from an unlocked treatment room; laptop contained the ePHI of 599 individuals	Aug. 2015
28.	Triple-S Management Corporation	At least 2,500 due to five breaches affecting more than 500 individuals per breach plus two breaches affecting fewer than 500 individuals	$3,500,000	Former employees accessed ePHI due to lack of termination of access rights; separately, and twice, vendors without BAAs disclosed PHI of beneficiaries on Medicare mailings; separately, a former employee copied member ePHI onto a CD and then took the CD home, later downloading that ePHI at his new place of work; and separately, enrollment staff placed incorrect member identification cards in mailing envelopes	Dec. 2015

29.	The Board of Regents of The University of Washington, on behalf of the University of Washington	90,000	$750,000	Breach of the unsecured ePHI of 90,000 individuals after an employee downloaded malware; failure to conduct risk assessment; failure to establish policies and procedures	Dec. 2015
30.	Complete P.T., Pool & Land Physical Therapy, Inc.	"Numerous Individuals"	$25,000	Impermissible disclosure of "numerous individuals'" PHI through the posting of patient testimonials, including names and photographs, on the Internet without prior written authorization; failure to safeguard PHI; failure to establish policies and procedures	Feb. 2016
31.	North Memorial Health Care	289,904 plus 9,497	$1,550,000	Failure to enter into a BAA with a BA; inappropriate disclosure of the ePHI of 289,904 individuals to that BA with whom there was no BAA; theft of an unencrypted laptop containing the ePHI of 9,497 individuals from a workforce member of the BA; failure to conduct risk assessment	Mar. 2016
32.	Feinstein Institute for Medical Research	13,000	$3,900,000	Theft of an unsecured, unencrypted laptop containing the ePHI of 13,000 individuals from employee's car; failure to conduct risk analysis; failure to implement required policies and procedures	Mar. 2016
33.	Raleigh Orthopaedic Clinic, P.A.	17,300	$750,000	Failure to enter into a BAA with a BA (x-ray vendor) before disclosing PHI (x-ray films) of 17,300 individuals to that BA	Apr. 2016

34.	The New York and Presbyterian Hospital	2	$2,200,000	Unauthorized disclosure of the PHI of two patients to the film crew and staff of a reality television show (NY Med); failure to safeguard PHI; failure to implement required policies and procedures	Apr. 2016
35.	Catholic Health Care Services of the Archdiocese of Philadelphia	412	$650,000	Theft of a BA's unencrypted, non-password-protected iPhone containing the ePHI of 412 nursing home residents; failure of BA to conduct risk assessment; failure of BA to implement security measures	June 2016
36.	Oregon Health & Science University	≥ 3,044	$2,700,000	Theft of an unencrypted, unsecured laptop; failure to enter into a BAA with internet service provider BA who stored the ePHI of more than 3,044 individuals; failure to implement required policies and procedures	July 2016
37.	The University of Mississippi on behalf of the University of Mississippi Medical Center	10,000	$2,750,000	Impermissible use of generic logins by users of the ePHI of 10,000 individuals; failure to assign unique user name to users of the same ePHI; failure to notify individuals (versus just media outlets) of breach; failure to implement safeguards	July 2016
38.	Advocate Health Care Network	3,998,529	$5,550,000	Theft of a desktop computer containing the ePHI of 3,994,175 patients; separately, the unauthorized access of the ePHI of 2,027 patients when an unauthorized party accessed the network of BA; separately, the theft of an unencrypted laptop containing the ePHI of 2,237 individuals from a BA; failure to enter into a BAA with the BA; failure to conduct risk assessment; failure to implement policies and procedures; failure to safeguard PHI	July 2016

39.	Care New England Health System	14,004	$400,000	Missing, unencrypted back-up tapes containing ePHI; failure to enter into a BAA with a BA; impermissible disclosure of the ePHI of 14,004 individuals to the BA	Sept. 2016
40.	St. Joseph Health	31,800	$2,140,500	Impermissible availability of the ePHI of 31,800 individuals on Internet; failure to conduct risk assessment	Oct. 2016
41.	University of Massachusetts Amherst	1,670	$650,000	Malware breach of the unsecured ePHI of 1,670 individuals; failure to document health care components per hybrid entity rules; failure to conduct risk analysis; failure to implement firewalls	Nov. 2016
42.	Presence Health Network	836	$475,000	Untimely reporting of breach of unsecured, paper-based PHI (operating room schedules) of 836 individuals; untimely reporting to affected individuals, HHS, and the media of past breaches involving additional individuals	Jan. 2017
43.	MAPFRE Life Insurance Company of Puerto Rico	2,209	$2,204,182	Theft of an unsecured thumb drive containing the ePHI of 2,209 individuals; failure to conduct risk analysis; failure to encrypt ePHI; failure to implement required policies and procedures	Jan. 2017
44.	South Broward Hospital District d/b/a/ Memorial Healthcare System	80,000	$5,500,000	Impermissible disclosure of the ePHI of 80,000 individuals; failure to implement audit controls; failure to implement required policies and procedures	Feb. 2017

45.	Metro Community Provider Network	3,200	$400,000	Hacker accessed employee email accounts and obtained the ePHI of 3,200 individuals; failure to implement required policies and procedures; failure to conduct risk analysis	Apr. 2017
46.	Center for Children's Digestive Health, S.C.	≥ 10,728	$31,000	Impermissible disclosure of the PHI of at least 10,728 individuals to a BA with whom there was no BAA	Apr. 2017
47.	CardioNet, Inc.	3,610	$2,500,000	Theft of a laptop from an employee's car containing the ePHI of 1,391 individuals; separately, another breach of the unsecured ePHI of 2,219 individuals; failure to conduct risk analysis; failure to implement required policies and procedures; failure to safeguard ePHI	Apr. 2017
48.	Memorial Hermann Health System	1	$2,400,000	Disclosure of one patient's PHI to multiple media outlets without the patient's prior written authorization; further disclosure by senior leaders of the same patient's PHI during multiple meetings without authorization; still further disclosure of the same patient's PHI on the covered entity's website without authorization; failure to document timely sanctions against workforce members	Apr. 2017

49.	St. Luke's—Roosevelt Hospital Center, Inc.	2	$387,200	Employee impermissibly faxed sensitive PHI of one patient to the patient's employer; employee impermissibly faxed sensitive PHI of a second patient to the second patient's place of volunteer work; the sensitive PHI included information about the patients' HIV, sexually transmitted diseases, sexual orientation, and mental health; failure to safeguard PHI	May 2017
50.	21st Century Oncology, Inc.	2,213,597	$2,300,000	Impermissible disclosure of the names, social security numbers, physicians' names, diagnoses, and treatment and insurance information of 2,213,597 individuals; failure to conduct risk analysis; failure to implement security measures; failure to enter into BAA with BA	Dec. 2017
51.	Fresenius Medical Care North America ("FMCNA")	521	$3,500,000	Failure to conduct an accurate and thorough risk analysis; impermissible disclosure of ePHI of approximately 521 individuals; failure to implement policies and procedures to safeguard facilities and equipment, to govern the receipt and removal of hardware and electronic media, and to address security incidents; failure to implement a mechanism to encrypt and decrypt ePHI	Feb. 2018
52.	Filefax, Inc.	2,150	$100,000	Impermissible disclosure of the PHI of 2,150 individuals; failure to safeguard the PHI of the same individuals	Feb. 2018

APPENDIX B:
HHS CIVIL MONEY PENALTY CASES

	Name of Covered Entity or Business Associate	Number of Affected Individuals	Amount of Penalty	HIPAA Rules Violations	Date Penalty Imposed
1.	Cignet Health dba Uplift Medical, P.C., Cignet Health Center, Cignet Health Plan, and Cignet Healthcare	41	$4,351,600	45 C.F.R. § 164.524 45 C.F.R. § 160.310(b)	Feb. 2011
2.	Lincare, Inc. dba United Medical	278	$239,800	45 C.F.R. § 164.502(a) 45 C.F.R. § 164.530(c) 45 C.F.R. § 164.530(i)(1)	Mar. 2016
3.	Children's Medical Center of Dallas	"at least" 2,484	$3,217,000	45 C.F.R. § 164.312(a)(2)(iv) 45 C.F.R. § 164.310(d)(1) 45 C.F.R. § 164.502(a)	Jan. 2017
4.	University of Texas MD Anderson Cancer Center	~ 33,500	$4,348,000	45 C.F.R. § 164.312(a) 45 C.F.R. § 164.502(a)	June 2018

Legend:

NFD Notice of Final Determination by HHS

NPD Notice of Proposed Determination by HHS

PR Press Release by HHS

APPENDIX C:
STATE ATTORNEY GENERAL ENFORCEMENT ACTIONS

	Name of Covered Entity or Business Associate	Jurisdiction of State Attorney General	Number of Affected Individuals	Amount of Consent Judgment or Settlement Agreement	Description of Incident Leading to State Attorney General Enforcement	Date of Judgment or Agreement
1.	Health Net, Inc.	Connecticut	500,000	$250,000	Loss of hard drive containing the PHI of 1.5 million individuals total, including 500,000 Connecticut residents	July 2010
2.	Health Net, Inc.	Vermont	525	$55,000	Loss of hard drive containing the PHI of 1.5 million individuals total, including 525 Vermont residents	Jan. 2011
3.	South Shore Hospital	Massachusetts	800,000	$750,000	Shipping of three boxes containing 473 unencrypted back-up computer tapes containing the ePHI of 800,000 individuals; only one box made it to its destination	May 2012
4.	Accretive Health	Minnesota	> 23,000	$2,500,000	Theft of an unencrypted laptop from the car of a BA employee; the laptop contained the PHI of more than 23,000 individuals	July 2012

Legend:
BA Business Associate
CJ Consent Judgment
ePHI Electronic Protected Health Information
PHI Protected Health Information
PR Press Release by the Relevant State Attorney General
SA Settlement Agreement

5.	Four pathology groups and one billing company	Massachusetts	67,000	$140,000	Disposal of the PHI of 67,000 Massachusetts residents in a public dump	Jan. 2014
6.	Woman & Infant's Hospital	Massachusetts	12,127	$150,000	Loss of 19 unencrypted back-up tapes containing the PHI of 12,127 Massachusetts residents	July 2014
7.	Beth Israel Deaconess	Massachusetts	3,796	$100,000	Theft of an unsecured, unencrypted personal laptop containing the PHI of 3,796 patients and employees	Nov. 2014
8.	Joseph Beck, DDS	Indiana	> 5,600	$12,000	Disposal in church dumpster of 63 boxes of patient records containing the PHI of more than 5,600 patients	Dec. 2014
9.	Boston Children's Hospital ("BCH")	Massachusetts	2,159	$40,000	Theft of BCH-issued laptop from a BCH physician while he presented at a conference in Buenos Aires; the laptop contained the PHI of 2,159 patients	Dec. 2014
10.	University of Rochester Medical Center	New York	3,403	$15,000	Provision to departing nurse of a spreadsheet containing the PHI of 3,403 patients; nurse gave PHI to new employer	Nov. 2015

11.	All American Home Care	New York	Multiple "patients" and "consumers"	$25,000	Impermissible use of the PHI of former home health agency patients for marketing purposes without patient authorization	Dec. 2016
12.	Horizon Healthcare	New Jersey	690,000	$1,100,000	Theft of two laptops containing the PHI of 690,000 New Jersey policyholders	Feb. 2017
13.	Aetna Inc.	New York	2,460	$1,150,000	Unauthorized disclosure of HIV diagnoses of 2,460 individuals through postal mailer with oversized transparent window	Jan. 2018
14.	EmblemHealth	New York	81,122	$575,000	Unauthorized disclosure of the Social Security numbers of 81,122 individuals through a mailing	Mar. 2018
15.	Virtua Medical Group	New Jersey	> 1,650	$417,816	Failure to protect the privacy of more than 1,650 patients whose medical records were accessible on the Internet	Mar. 2018