Hofstra Law Review

12-1-2019

Your Personal Health Information May Have Been Compromised: Using Encryption to Prevent Data Breaches on End-User Devices

Nina Patel
Maurice A. Deane School of Law at Hofstra University

Follow this and additional works at: https://scholarlycommons.law.hofstra.edu/hlr

Part of the Law Commons

NOTE

YOUR PERSONAL HEALTH INFORMATION MAY HAVE BEEN COMPROMISED: USING ENCRYPTION TO PREVENT DATA BREACHES ON END-USER DEVICES

I. INTRODUCTION

Envision a large company that provides health insurance services to roughly 3.7 million members.[1] Each and every one of those members provide their personal information, including names, social security numbers, and addresses.[2] The company also gathers and retains protected health information, including medical histories, test and lab results, claims for coverage, and demographic information.[3] The company collects this information and takes a few physical and technical steps to be in compliance with the company's policy to safeguard the information.[4] Most notably, the company provides password protected laptops to the employees and uses cables to lock them to the employees' workstation.[5] But upon arriving to work one day, it was discovered that an unauthorized individual had cut the cables and stolen two employee laptops.[6] To the company's dismay, they had never encrypted those laptops and now the company is subject to a lawsuit.[7] The company's subpar technical safeguards have now put nearly 840,000 members' personal health information at risk.[8] It turns out that the company could have most likely avoided this disclosure of information and a $1.1

---

1. *See In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 629 (3d Cir. 2017) (alleging that Horizon Healthcare Services potentially exposed the personal information of more than 839,000 people after two unencrypted laptops were stolen).
2. *See id.*
3. *See id.*
4. *See id.* at 629-30.
5. *See id.* at 641.
6. *See id.* at 630-31; Plaintiffs'-Appellants' Brief and Volume I of the Appendix at 31, *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d at 629 (No. 15-2309).
7. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d at 630-31.
8. *See id.* at 629-30.

million settlement if the company had just encrypted those laptops.[9] This
was the outcome of a recent such case in New Jersey.[10]

The recent shift of medical records from paper to electronic formats
has led to increased efficiency and access because we are better able to
keep track of important medical information.[11] For instance, currently
there are web portals to ease payment and reimbursement transactions
among healthcare providers and insurance plans.[12] Medical claim
submissions can be completed online by uploading medical
documentation, including x-rays, and the claims can also be
conveniently managed on mobile devices.[13]

However, the shift also leads to personal information becoming
vulnerable to data breaches through third-party hacking as people are
increasingly accessing such information in their own homes through
personal laptops and mobile devices.[14] Hackers have recently shifted
their focus from stealing financial data to stealing electronic healthcare
records because electronic healthcare records are increasingly more
valuable.[15] When a credit card is stolen by a hacker, banks ordinarily
have a series of protective mechanisms in place to flag the account and
instantly cancel the credit card.[16] In contrast, the reaction after a hacker
steals a partial healthcare record may not be as instantaneous and the
information can then be used to make fraudulent insurance claims.[17] One

---

9. *See Horizon Blue Cross/Blue Shield of New Jersey Agrees to Pay $1.1 Million, Tighten Data Security to Settle Allegations of Privacy Lapses Concerning Personal Information of Policyholders*, N.J. DIVISION CONSUMER AFF. (Feb. 17, 2017), https://www.njconsumeraffairs.gov/News/Pages/02172017.aspx.

10. *Id.* (agreeing to pay a "$926,803.22 civil penalty, a $93,196.78 reimbursement of the state's attorney fees and $80,000 to be used at the sole discretion of the attorney general for the promotion of consumer privacy programs").

11. Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1440, 1444, 1450 (2002) ("Polling data have consistently shown that Americans are concerned about the privacy of their medical data. Over 80% of respondents in one survey suggested they had 'lost all control over their personal information.' In another national survey, 78% of respondents felt it is very important that medical records be kept confidential.").

12. *Id.* at 1440, 1450. (stating that sharing health data can help improve health research, public health, and the administration of justice and law enforcement).

13. *How to Make a Claim*, AETNA, https://www.aetnainternational.com/en/individuals/make-most-of-plan/how-to-make-claim.html (last visited Jan. 25, 2020).

14. *See* Andrew Freedman, Note, *Managing Personal Device Use in the Workplace: How to Avoid Data Security Issues and to Dig Yourself Out of Your Failed BYOD Policy*, 20 SUFFOLK J. TRIAL & APP. ADVOC. 284, 286-88 (2015).

15. Ken Lynch, *Why Healthcare Hacking Is Profitable and How You Can Prevent It*, INTELLIGENTHQ (Sept. 24, 2018), https://www.intelligenthq.com/resources/healthcare-hacking-profitable-can-prevent.

16. *Id.* (finding that theft of financial data will continue to remain a concern, but hackers have shifted their attention away from it because it is less profitable).

17. *Id.*; *see Healthcare Fraud*, HEALTHCARE BUS. & TECH., http://www.healthcarebusinesstec

such claim may be for a sham medical procedure at a nonexistent hospital.[18] Studies estimate that one credit card number can yield $1 for a hacker, whereas each partial electronic healthcare record can yield $50.[19] Meanwhile, the data breach can cost the company $408 per lost or stolen record.[20] Since 2009, hackers have stolen healthcare records of more than 120 million individuals by means of 1100 distinct security breaches.[21]

Encryption of protected health information ("PHI") uses an algorithm to convert regular text into encoded text, thereby preventing unauthorized users, such as hackers, from accessing the PHI.[22] Currently, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which sets the mandatory national standards for PHI, does not mandate encryption.[23] States are permitted to develop laws that are more stringent than HIPAA's minimum standards.[24]

This Note argues that as technology advances and more people use end-user devices to access PHI, HIPAA needs to be amended to respond to technological advancements and mandate encryption to protect PHI.[25] Part II provides a background of current regulation under HIPAA and the Health Information Technology for Economic and Clinical Health ("HITECH") Act.[26] It then explores different methods of encryption and HIPAA's Audit Program.[27] Part III focuses on the legal issues that result from encryption not being mandated under HIPAA.[28] Part IV proposes an amendment to HIPAA that mandates encryption and independent audits.[29] The amendment will create a well-defined safeguard for

---

h.com/healthcare-fraud (last visited Jan. 25, 2020) (finding that healthcare fraud and abuse remains a major "threat to individuals as well as to the economic condition of the nation").

18. Lynch, *supra* note 15; *see Healthcare Fraud, supra* note 17 (according to the National Health Care Anti-Fraud Association, billing for services that were not rendered is one of the most recurrent types of healthcare fraud, wherein information obtained through identity theft is used "to fabricate entire claims or by padding claims with charges for procedures or services that did not take place").

19. Lynch, *supra* note 15.

20. Meg Bryant, *Healthcare Sector Leads in Costs for Data Breaches, Study Finds*, HEALTHCARE DIVE (July 13, 2018), https://www.healthcaredive.com/news/healthcare-sector-leads-in-costs-for-data-breaches-study-finds/527716.

21. Lynch, *supra* note 15.

22. Zoe Milak, Comment, *The Copyrightability of Encryption Methods and Encryption Algorithms on Computers*, 1996 U. CHI. LEGAL F. 589, 593-95 (1996).

23. 45 C.F.R. § 164.312(a)(2)(iv) (2013) (stating that encryption and decryption are both addressable).

24. 45 C.F.R. § 160.203(b) (2002).

25. *See infra* Part IV.

26. *See infra* Part II.

27. *See infra* Part II.B.1–2.

28. *See infra* Part III.

29. *See infra* Part IV.

electronic PHI that all covered entities and business associates must implement.[30] Patients will be confident in knowing that their health information is being secured,[31] and covered entities will lower their risk of a compliance action.[32]

II.   THE HISTORY OF HIPAA AND ITS AMENDMENTS

The Health Insurance Portability and Accountability Act of 1996 was enacted by Congress to provide standardized security and privacy safeguards to protect health information.[33] Several courts have held that Congress has the power to create health care fraud provisions, as in HIPAA, under the Commerce Clause.[34] Prior to HIPAA's enactment, health plans could freely disclose a patient's personal information to a lender, who could subsequently reject the patient's request for a credit card.[35] HIPAA also aimed to reduce scams and abuse in health insurance and healthcare delivery.[36] This Part discusses the history of HIPAA, including its amendments and the role of encryption to protect data security.[37] Subpart A provides an overview of HIPAA's regulations.[38] It

---

30. *See infra* Part IV.

31. *See* Milak, *supra* note 22, at 593-94.

32. *See Encryption: A Critical Safeguard Against HIPAA Liability*, KAUFMAN & CANOLES (July 26, 2016), https://www.kaufcan.com/blog/health-care-law/encryption-a-critical-safeguard-against-hipaa-liability; *see also Openness and Transparency*, U.S. DEP'T HEALTH & HUM. SERVS. 1 (Apr. 19, 2019), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/heal thit/opennesstransparency.pdf.

33. *When Was HIPAA Enacted?*, HIPAA J. (Mar. 9, 2018), https://www.hipaajournal.com/wh en-was-hipaa-enacted.

34. Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. Fed. 133 § 3 (2004). In *United States. v. Lauersen*, No. 98 CR. 1134(WHP), 1999 WL 637237 (S.D.N.Y. Aug. 20, 1999), a trial court sitting in the Southern District of New York held that the two healthcare statutes relating to fraud were constitutional exercises of Congress' Commerce Clause authority. *Id.* at *7. The court reasoned that "the administration of private health care programs is an economic activity substantially affecting interstate commerce." *Id.* at *6. This decision was affirmed by the Second Circuit Court of Appeals. United States v. Lauersen, 348 F.3d 329, 344 (2d Cir. 2003). In *United States v. Whited*, 311 F.3d 259 (3d Cir. 2002), the Third Circuit Court of Appeals held that "regulating theft or embezzlement from medical service providers," as under HIPAA, "constitutes a proper exercise of Congress' Commerce Clause authority." *Id.* at 267. In *Peebler v. Reno*, 965 F. Supp. 28 (D. Or. 1997), the Oregon District Court held that there is no private cause of action to challenge the constitutionality of HIPAA's health care fraud provisions when it comes to breach of PHI. *Id.* at 31.

35. *Why Is the HIPAA Privacy Rule Needed?*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.h tml.

36. *When Was HIPAA Enacted?*, *supra* note 33.

37. *See infra* Part II.A–C.

38. *See infra* Part II.A.

discusses the Privacy Rule,[39] the Security Rule,[40] and the HITECH Act.[41] Subpart B discusses the enforcement of the HIPAA Rules.[42] This includes both Phase I of HIPAA's Audit Program[43] and Phase II.[44] Subpart C provides an overview of encryption.[45] It discusses symmetric encryption,[46] asymmetric encryption,[47] and key management for both types of encryption.[48] The three core provisions of the Act are the portability provisions, tax provisions, and administrative simplification provisions.[49] This Note focuses on the administrative simplification provisions.[50] There have been three major legislative expansions to HIPAA: (1) the Privacy Rule, (2) the Security Rule, and (3) the HITECH Act.[51]

Prior to the enactment of HIPAA, the House Committee on Government Reform and Oversight indicated that fraud and abuse in the health care industry were of grave concern due to the vast amount of money being lost.[52] Under HIPAA in 1996, Congress did not specify

---

39. *See infra* Part II.A.1.
40. *See infra* Part II.A.2.
41. *See infra* Part II.A.3.
42. *See infra* Part II.B.
43. *See infra* Part II.B.1.
44. *See infra* Part II.B.2.
45. *See infra* Part II.C.
46. *See infra* Part II.C.1.
47. *See infra* Part II.C.2.
48. *See infra* Part II.C.3.
49. BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 153 (Sharyl J. Nass et al. eds., 2009); *see* Buckman, *supra* note 34, § 2 (noting that the administrative simplification provision of HIPAA focuses mainly on electronic information, but paper records are also covered as "if coverage were limited to electronic data, there would be perverse incentives for entities covered by the rule to avoid the computerization and portability of any medical records").
50. *See infra* Part II.A–B; *see also* BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH, *supra* note 49, at 153-54 (stating that the portability provisions of HIPAA focus on preventing "individuals from losing health care coverage due to a preexisting condition when changing to a new employer's health plan" and HIPPA's tax provisions also aim to "make it easier for individuals to maintain health insurance. . . . HIPAA does not regulate the price of health insurance, but rather, it relies on tax breaks and other tax incentives to reduce health care costs.").
51. *When Was HIPAA Enacted?*, *supra* note 33.
52. Buckman, *supra* note 34, at § 2 (stating that based on "approximately one trillion dollars spent on health care, divided among Medicare, Medicaid, and various state and private programs," it is estimated "that as much as 10% or $100 billion—$274 million a day—was lost to fraud and abuse"); *see* H.R. REP. No. 104-747, at 2 (1996). Further, a 1996 House of Representatives report on healthcare fraud found that:
   1. Health care fraud schemes steal billions of dollars from public and private payers each year.
   2. The Department of Justice (DOJ) needs stronger and more direct statutory authority to deter fraud and abuse against public and private health care plans.
   3. Scarce enforcement resources are wasted in pursuit of the same fraudulent scheme

privacy requirements.[53] The Secretary of the U.S. Department of Health and Human Services ("HHS"), under the administrative simplification provisions of HIPAA, was obligated to create privacy regulations governing individually identifiable health information if Congress itself did not pass privacy legislation within three years from the date HIPAA was enacted.[54] The goal was to create uniform security standards and safeguards across the states since Congress acknowledged that "advances in electronic technology could erode the privacy of health information."[55] Shortly after the mandate was declared, Secretary Donna Shalala, on behalf of HHS, presented a report to Congress encouraging Congress to be responsible for passing the federal legislation and not HHS.[56] However, after introducing several unsuccessful bills that attempted to finalize privacy legislation, Congress ultimately did not pass privacy legislation within the timeframe.[57] Thus, HHS issued the Privacy and Security Rules to implement the requirements set out in HIPAA.[58] The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009.[59] In addition, under the Fourth Amendment, Congress delegated to the Attorney General a "very broad subpoena power in investigating potential fraud."[60]

---

against public and private health care plans in multiple jurisdictions.
Id. The report recommended that "Congress . . . enact legislation to make health care frauds against all public and private payers Federal criminal offenses." *Id.*

53. BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH, *supra* note 49, at 153, 155.

54. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html; *see* BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH, *supra* note 49, at 154 (stating that health plans requested Congress to set federal legislation for the electronic transmission of health information to help standardize the process of transmitting information).

55. BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH, *supra* note 49, at 154-55 (stating that the administrative simplification provisions of HIPAA required the formation of privacy standards for PHI).

56. *Id.* at 155.

57. *Id.* at 155-56 (stating that Congress attempted to pass eight privacy bills in the 1999 congressional session alone); *Summary of the HIPAA Privacy Rule*, *supra* note 54.

58. BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH, *supra* note 49, at 156-57 (stating that in order for HHS to develop the Privacy Rule we have today, HHS had to go through "four iterations of the Rule." The first version of the Rule was made public and received over 50,000 comments, which HHS took into consideration for the second version of the Rule.); *Summary of the HIPAA Privacy Rule*, *supra* note 54.

59. *What Is the HITECH Act?*, COMPLIANCY GROUP, https://compliancy-group.com/what-is-the-hitech-act (last visited Jan. 25, 2020) (stating that the American Recovery and Reinvestment Act of 2009 was "an economic stimulus bill").

60. Buckman, *supra* note 34, at § 2.

A. *HIPAA's Privacy and Security Regulations*

The HIPAA Final Privacy Rule was passed in 2000 and the HIPAA Final Security Rule was passed in 2003.[61] The HITECH Act became fully enforceable in 2010[62] and it expanded both the privacy and security laws.[63]

1. HIPAA's Privacy Rule

The purpose of the Privacy Rule is to create an optimal balance wherein people feel comfortable that their health information is properly safeguarded while still permitting healthcare practitioners to channel the information as necessary to provide superior quality of care.[64] The Privacy Rule mandates safeguards to protect the privacy of all protected health information.[65] PHI consists of individually identifiable health information that is "transmitted by electronic media" or "transmitted or maintained in any other form or medium."[66] However, PHI excludes specific records relating to students, education, and employment.[67] Individually identifiable health information is considered a subgroup of health information and includes demographic information gathered from an individual and created or received by a covered entity.[68] The information must also relate 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.[69] Moreover, the information must identify the individual or present a reasonable basis to identify the individual.[70]

The Privacy Rule applies to covered entities, which consist of health plans, healthcare clearinghouses, and health care providers.[71] It

---

61. *When Was HIPAA Enacted?*, *supra* note 33.

62. *Id.*

63. Ranjit Janardhanan, *Uncle Sam Knows What's in Your Medicine Cabinet: The Security and Privacy Protection of Health Records Under the HITECH Act*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 667, 682 (2014).

64. *Summary of the HIPAA Privacy Rule*, *supra* note 54.

65. *The HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (Apr. 16, 2015), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

66. 45 C.F.R. § 160.103 (2014).

67. *Id.* (stating that education records are covered by the Family Educational Rights and Privacy Act).

68. *Id.*

69. *Id.*

70. *Id.*; *see Summary of the HIPAA Privacy Rule*, *supra* note 54 (noting examples of common identifiers for individually identifiable health information, including birth dates, social security numbers, addresses, and names).

71. 45 C.F.R. § 160.102(a) (2013); *see* Buckman, *supra* note 34, § 5.5 (noting that a covered entity does not include the government, railroads, or the Federal Bureau of Investigation); *Summary of the HIPAA Privacy Rule*, *supra* note 54 (stating that health plans include both individual and

also applies to a business associate, which can be either a person or an organization that performs functions or activities on behalf of a covered entity or provides services to a covered entity.[72] For instance, a medical billing company can be the business associate of a hospital, which is the covered entity.[73] The functions or services of a business associate must involve the use or disclosure of PHI.[74] A covered entity must execute a business associate contract with each business associate it uses to perform its functions or services.[75] A business associate contract includes precise written safeguards that the business associate must adhere to in accordance with the Privacy Rule.[76] The Privacy Rule also establishes a protocol for covered entities if there is a breach or violation by the business associate.[77]

2. HIPAA's Security Rule

The Security Rule, which is part of the Privacy Rule, specifically protects electronic PHI that is generated, received, used, or preserved by a covered entity through both physical and technical safeguards.[78] In general, covered entities and business associates are required to "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits."[79] They must also use safeguards

---

group plans that provide medical care. Health care providers are those who electronically transmit health information in relation to a standard transaction, and healthcare clearinghouses are usually entities that handle nonstandard information services for health plans or health care providers).

72. *Summary of the HIPAA Privacy Rule, supra* note 54 (stating that functions and activities of a covered entity include processing, data analysis, and billing, whereas services are restricted to "legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services").

73. *See id.*

74. *Id.*

75. *Id.*

76. *Id.; see Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS. (May 24, 2019), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html ("Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions–not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.").

77. *Business Associates, supra* note 76 ("Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office of Civil Rights (OCR).").

78. Sharona Hoffman & Andy Podgurski, *Securing the HIPAA Security Rule*, 10 J. INTERNET L., Feb. 2007, at 7-8 (2007); *see The Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (May 12, 2017), https://www.hhs.gov/hipaa/for-professionals/security/index.html.

79. 45 C.F.R. § 164.306(a) (2013).

against any reasonably foreseen threats or hazards to the security of the information.[80] The Security Rule is known for its flexibility, which takes into consideration factors such as the covered entities' costs of security measures, technical infrastructure, and size.[81]

a. Physical Safeguards

HIPAA's Security Rule gives guidance on a facility's physical protections for electronic PHI.[82] It addresses both workstation use, workstation security, and device and media controls.[83] A workstation is defined as "an electronic computing device."[84] The following implementation specifications are addressable:

> (i) *Contingency operations (Addressable)*. Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency;[85]
>
> (ii) *Facility security plan (Addressable)*. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft;[86]
>
> (iii) *Access control and validation procedures (Addressable)*. Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision;[87] and
>
> (iv) *Maintenance records (Addressable)*. Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).[88]

There must be workstation physical safeguards in place that limit the electronic PHI access to only authorized users.[89] The covered entity or business associate must also have a policy and procedure that addresses the functions that need to be executed and how to carry out those functions.[90] The objective is to draw a connection between an individual's access to the electronic PHI and the individual's function

---

80. *Id.*
81. § 164.306(b).
82. 45 C.F.R. § 164.310(a) (2013).
83. § 164.310(b).
84. 45 C.F.R. § 164.304 (2013).
85. § 164.310(a)(2)(i).
86. § 164.310(a)(2)(ii).
87. § 164.310(a)(2)(iii).
88. § 164.310(a)(2)(iv).
89. § 164.310(c).
90. § 164.310(b).

within the entity.[91] The policy must also address physical features immediate to the workstation.[92] For example, the entity should consider whether the workstation is in a public space, and how many unauthorized individuals have access to the workstation.[93] Ultimately, it is the entity's responsibility to determine the precise physical safeguards that are necessary to protect electronic PHI and to implement those safeguards.[94]

b. Technical Safeguards

A covered entity or business associate must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified."[95] One such technical safeguard is encryption, but it is merely "addressable."[96] Under the Security Rule, "addressable" means that the covered entity or business associate must implement encryption as it considers "reasonable and appropriate."[97] The Rule provides no further definition of reasonable and appropriate and no standard for encryption.[98] If the entity chooses to not implement encryption, then it needs to document why it would not be reasonable and appropriate.[99] The entity must then implement an equivalent measure that is reasonable and appropriate.[100] The Rule provides no specific information describing what measure would be equivalent,[101] but it does contain factors that the entity is required to consider when selecting a security measure:

---

91. Elizabeth Snell, *A Review of Common HIPAA Physical Safeguards*, HEALTH IT SECURITY (July 10, 2015), https://healthitsecurity.com/news/a-review-of-common-hipaa-physical-safeguards.

92. §164.310(b).

93. Snell, *supra* note 91.

94. *Id.*

95. 45 C.F.R. § 164.312(a)(1) (2013).

96. § 164.312(a)(2)(iv); § 164.312(e)(2)(ii) (stating "[e]ncryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information").

97. 45 C.F.R. § 164.306(d) (2013).

98. *See* Brandon S. Kulwicki, *It's Five O'Clock; Do You Know Where Your Records Are? Obligations of Individuals and Entities to Secure Protected Health Information*, 18 SMU SCI. & TECH. L. REV. 455, 463 (2015) (stating that the covered entity or business associate is left to determine what is reasonable and appropriate).

99. §164.306(d)(3)(ii)(B).

100. *Id.*

101. *See id.*

(i) The size, complexity, and capabilities of the covered entity or business associate;[102]
(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities;[103]
(iii) The costs of security measures;[104] and
(iv) The probability and criticality of potential risks to electronic protected health information.[105]

The Security Rule also requires covered entities to perform risk analysis on an ongoing basis.[106] The risk analysis includes assessing the probability and effect of potential risks to electronic PHI, addressing those risks, and documenting any steps taken to remedy them.[107] However, because the covered entities perform risk assessments on their own, the assessments can possibly lead a covered entity to temporarily modify its policies to appear more compliant during the self-assessment.[108]

3.   HITECH Act Passed to Protect Electronic PHI

Before the HITECH Act was passed, HHS could only levy civil penalties of up to $100 per HIPAA violation, with the total repeat or uncorrected violation penalties not to exceed $25,000 per year.[109] Under the HITECH Act, civil penalties for willful neglect of PHI increased up to $250,000 and the penalty for repeat or uncorrected violations is a maximum of $1.5 million.[110] In addition, HIPAA's civil and criminal penalties encompass business associates under particular circumstances.[111] The massive increase in the civil penalty maximum further supports that securing electronic PHI is imperative.[112]

The HHS Secretary considers various factors when determining the amount of civil penalties under the HITECH Act.[113] HHS uses a tier-based approach to determine civil penalties.[114] There are four major tiers

---

102. § 164.306(b)(2)(i).
103. § 164.306(b)(2)(ii).
104. § 164.306(b)(2)(iii).
105. § 164.306(b)(2)(iv).
106. *Summary of the HIPAA Privacy Rule*, *supra* note 54.
107. *Id.*
108. *Id.*; *see* Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 LOY. U. CHI. LJ. 175, 220 (2014) (discussing how covered entities are given advance notice of HIPAA compliance audits and, thus, "may modify their practices and procedures for the duration of the audit").
109. Janardhanan, *supra* note 63, at 678.
110. *What is the HITECH Act?*, *supra* note 59.
111. *Id.*
112. *See* Janardhanan, *supra* note 63, at 678.
113. *Id.* at 679.
114. *Id.* at 700.

of culpability: (1) unknowing, (2) reasonable cause, (3) willful neglect–corrected, and (4) willful neglect–uncorrected.[115] Tier one results in a fine ranging from $100 to $50,000 for each violation.[116] Tier two results in a fine ranging from $1,000 to $50,000 for each violation.[117] Tier three results in a fine ranging from $10,000 to $50,000 for each violation.[118] Tier four results in a fine of $50,000 for each violation.[119] For all four tiers, the maximum penalty for all such violations of an identical provision in a calendar year is $1.5 million.[120] The HHS Secretary considers the following factors to determine the ultimate penalty amount: (1) the nature of the violation, which includes the number of individuals affected and when the violation occurred; (2) the nature and extent of the harm that ensued because of the violation, which includes the physical harm, financial harm, reputational harm, and any interference with that individual's ability to acquire health care; (3) prior history of compliance with the HIPAA administrative simplification provisions, which includes "[h]ow the covered entity or business associate has responded to prior complaints;" and (4) the financial status of the entity and what the impact of the fine will be based on its size and ability to sustain its operations.[121]

The HITECH Act is most notable for establishing the Breach Notification Rule and holding business associates, just like covered entities, responsible for complying with HIPAA Rules.[122] The Breach Notification Rule clearly establishes a standard in the event of a breach

---

115. *HIPAA Omnibus Final Rule Implements Tiered Penalty Structure for HIPAA Violations*, MCGUIREWOODS (Feb. 14, 2013), https://www.mcguirewoods.com/client-resources/Alerts/2013/2/HIPAA-Omnibus-Final-Rule-Implements-Tiered-Penalty-Structure-HIPAA-Violations.

> Unknowing. The covered entity or business associate did not know and reasonably should not have known of the violation.
> Reasonable Care. The covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission was a violation, but the covered entity or business associate did not act with willful neglect.
> Willful Neglect–Corrected. The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA. However, the covered entity or business associate corrected the violation within 30 days of discovery.
> Willful Neglect–Uncorrected. The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA, and the covered entity or business associate did not correct the violation with 30 days of discovery.

Id. (emphasis omitted).

116. 45 C.F.R. § 160.404 (2016).
117. *Id.*
118. *Id.*
119. *Id.*
120. *Id.*
121. 45 C.F.R. § 160.408 (2013).
122. *When Was HIPAA Enacted?*, *supra* note 33.

of unsecured PHI, which does not include PHI that is "unusable, unreadable, or indecipherable to the unauthorized individuals."[123] Therefore, if the data is encrypted, meaning it is encoded and essentially unreadable, breach of that data does not trigger notification.[124] This essentially creates a "safe harbor for unauthorized disclosures of encrypted PHI" under the Breach Notification Rule.[125]

B. Enforcement of HIPAA

The U.S. Department of Health & Human Services Office of Civil Rights ("OCR") enforces HIPAA's Privacy, Security, and Breach Notification Rules.[126] OCR investigates complaints and conducts compliance reviews of covered entities.[127] If OCR determines that a covered entity is not in compliance, OCR can take corrective action or pursue a resolution agreement.[128] HHS is required to submit a report to Congress which specifies how many complaints HHS receives about breaches and if any action was taken by HHS as a result of the breach.[129] In 2013, OCR mandated covered entities or business associates to take corrective actions on nearly eighty percent of the breach compliance reviews concluded that year.[130] As of August 31, 2019, OCR most frequently requires general hospitals to take corrective action.[131] OCR stated that from 2009 to 2017, there were approximately 2178 reports OCR received involving breach of PHI involving 500 or more individuals.[132] Of those breaches, thirty-eight percent of the reports were based on theft, eight percent were based on loss, and twenty-seven percent were based on unauthorized access or disclosure.[133] Moreover,

---

123.   Janardhanan, *supra* note 63, at 683.

124.   *See id.*

125.   Kulwicki, *supra* note 98, at 474.

126.   *About Us*, U.S. DEP'T HEALTH & HUM. SERVS. (Oct. 8, 2019), https://www.hhs.gov/ocr/about-us/index.html.

127.   *How OCR Enforces the HIPAA Privacy & Security Rules*, U.S. DEP'T HEALTH & HUM. SERVS. (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html.

128.   *Id.*

129.   Janardhanan, *supra* note 63, at 689.

130.   U.S. DEP'T HEALTH & HUM. SERVS., ANNUAL REPORT TO CONGRESS ON HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION RULE COMPLIANCE 10 (2014), https://www.hhs.gov/sites/default/files/rtc-compliance-20132014.pdf.

131.   *Enforcement Highlights*, U.S. DEP'T HEALTH & HUM. SERVS. (Sept. 13, 2019), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

132.   Linda Sanches, *Update on Administration and Enforcement of the HIPAA Privacy, Security, and Breach Notification Rules*, U.S. DEP'T HEALTH & HUM. SERVS. (Jan. 18, 2018), http://src.bna.com/wyP.

133.   *Id.*

sixteen percent of the breach reports involved a laptop and nine percent involved a portable electronic device.[134]

1. HIPAA's Audit Program: Phase I

Under HITECH, OCR is mandated to perform periodic audits of covered entity and business associate compliance with respect to all three HIPAA rules.[135] The goal of the audit program is not to punish noncompliance, but for OCR to better understand how entities are adhering to the requirements set out in the privacy, security and breach notification requirements.[136] Phase I of its HIPAA Audit Program, which was the pilot program, was completed by the end of 2012.[137] In an audit program, all covered entities and business associates are eligible to be selected for an audit.[138] Selection is solely at the discretion of OCR, and once an entity is selected, it is expected to fully cooperate with the audit.[139] During Phase I, OCR evaluated the controls and processes applied by 115 covered entities.[140] OCR's selection process aimed to cast a wide net and it selected various types and sizes of covered entities.[141] However, OCR did conduct on-site visits to all 115 entities after providing the entity with written notification thirty to ninety days prior to the expected on-site visit.[142] While on site, the compliance auditor interviewed main personnel and observed processes and operations to assist in evaluating compliance.[143] After OCR issued an audit report on the entity, if there was a significant compliance problem, OCR had the option to commence a compliance review to tackle the problem.[144]

---

134. *Id.*

135. *HIPAA Privacy, Security, and Breach Notification Audit Program*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement /audit/index.html.

136. James Swann, *Federal Privacy Audits Continue to Scare Health-Care Providers*, BLOOMBERG L. (Feb. 22, 2018), https://www.bloomberglaw.com/product/blaw/document/X96U8M MO000000?criteria_id=a06dcda3f81c8a9bfbd0c3cc9d1c630b&searchGuid=900c3fc9-b4d8-4670-84cf-21cd9668ae37&bna_news_filter=bloomberg-law-news.

137. *Audit Pilot Program*, U.S. DEP'T HEALTH & HUM. SERVS., (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/pilot-program/index.ht ml (stating that "[a]udits present a new opportunity to examine mechanisms for compliance, identify best practices, and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews").

138. *Id.*

139. *Id.*

140. *HIPAA Privacy, Security, and Breach Notification Audit Program*, *supra* note 135.

141. *Audit Pilot Program*, *supra* note 137.

142. *Id.*; *HIPAA Privacy, Security, and Breach Notification Audit Program*, *supra* note 135.

143. *Audit Pilot Program*, *supra* note 137.

144. *Id.*

2. HIPAA's Audit Program: Phase II

In 2016, OCR began Phase II of the HIPAA Audit Program, which was similar to Phase I with respect to the selection process.[145] OCR announced that it would not audit entities that had an ongoing complaint investigation or an entity presently undertaking a compliance review.[146] One crucial difference between Phase I and II was the audit process.[147] During Phase II, OCR conducted a desk audit for both covered entities and its business associates, and then conducted on-site audits.[148] The desk audits aimed to examine compliance with the Privacy, Security, or Breach Notification Rules, depending on which subject area OCR determined was the subject of the document request letter it sent to the entity ahead of time.[149] In comparison, the on-site visits aimed to observe a broader range of requirements from the HIPAA Rules than desk audits.[150] The total number of in-person site visit audits was fewer than Phase I.[151]

Phase II audits were concluded in 2017, but OCR is planning to advance a more permanent audit program in the future.[152] According to a presentation given by OCR in January 2018, eighty-nine percent of all covered entity desk audits thus far were performed on providers, ten percent were performed on health plans, and the remaining one percent were performed on healthcare clearinghouses.[153] Practitioners represented fifty-five percent of all providers.[154] At that time, OCR finished 166 desk audits of covered entities and forty-one desk audits of business associates.[155]

---

145. *HIPAA Privacy, Security, and Breach Notification Audit Program, supra* note 135.

146. *Id.*

147. *See id.* (stating that "[t]he audit program is an important tool to help assure compliance with HIPAA protections, for the benefit of individuals").

148. *Id.* ("The technical assistance and promising practices that OCR generates will also assist covered entities and business associates in improving their efforts to keep health records safe and secure.").

149. *Id.*

150. *Id.*

151. *Id.*

152. *Audit Pilot Program, supra* note 137; Reece Hirsch, *The Year Ahead in HIPAA: Does 2017 Reflect the "New Normal" for Enforcement?*, BLOOMBERG L. (Jan. 31, 2018), https://news.bloomberglaw.com/health-law-and-business/the-year-ahead-in-hipaa-does-2017-reflect-the-new-normal-for-enforcement (stating that there are some "factors [that] suggest that OCR may be challenged to keep up its previous HIPAA enforcement pace. OCR's budget request for 2018 is $33 million, $6 million less than its 2017 funding, with FTEs reduced by 17 from 179 and 162. The budget request also contemplates that OCR will reduce overhead and non-personnel costs, and support its enforcement activities using civil monetary settlement funds.").

153. Sanches, *supra* note 132.

154. *Id.*

155. Swann, *supra* note 136.

C. Basics of Encryption

One of the earliest forms of encoded texts, known as ciphers, can trace back to 700 B.C. when the Spartan military used skytales to send messages.[156] Both the sender and recipient had wooden rods, which had the same diameter and length.[157] The sender would tightly wind a piece of leather on the wooden rod and carve an encrypted message on it.[158] The unwound leather, without the wooden rod, would then be delivered to the recipient who would closely wind the leather on his own wooden rod to read the message.[159] Encryption, which involves cryptography, involves the use of algorithms to convert plaintext into encoded text.[160] The encoded text, once delivered to the recipient, requires a key to decrypt the information back into plain text.[161] Decryption is the process of changing the encoded text back into plaintext through the use of a cryptographic algorithm.[162] Data in transit "refers to data being accessed over a network—and which, therefore, could be intercepted by someone else on the network, or by someone with access to the physical media the network uses."[163] Whereas data at rest refers to "inactive data stored physically in any digital form," including end-user devices.[164]

In 1979, the National Bureau of Standards invented the Data Security Encryption Standard ("DES").[165] At the time, DES was a relatively strong encryption method and it was the first encryption method approved by the U.S. government for public use.[166] However, in 1998, the Electronic Frontier Foundation was able to decrypt a DES-

---

156. Ricky Ribeiro, *A History of Encryption Through the Ages*, BIZTECH (May 10, 2012), https://biztechmagazine.com/article/2012/05/history-encryption-through-ages-infographic.

157. *Id.*

158. *Id.*

159. *Id.* (stating that other people who came across the leather piece would only see jumbled letters with no meaning).

160. ELAINE BARKER & ALLEN ROGINSKY, U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-133 REVISION 1, RECOMMENDATION FOR CRYPTOGRAPHIC KEY GENERATION 2-3 (2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublication s/NIST.SP.800-133r1.pdf [hereinafter SPECIAL PUBLICATION 800-133]; Joe Baladi, Comment, *Building Castles Made of Glass—Security on the Internet*, 21 U. ARK. LITTLE ROCK L. REV. 251, 254-56 (1999).

161. Baladi, *supra* note 160, at 254.

162. SPECIAL PUBLICATION 800-133, *supra* note 160, at 2.

163. James Deck, *Why Healthcare Organizations Should Encrypt Everything*, BECKER'S HOSP. REV. (June 9, 2017), https://www.beckershospitalreview.com/healthcare-information-technology/w hy-healthcare-organizations-should-encrypt-everything.html.

164. *Id.*

165. Ribeiro, *supra* note 156.

166. Margaret Rouse, *Data Encryption Standard (DES)*, TECHTARGET, https://searchsecurity.t echtarget.com/definition/Data-Encryption-Standard (last visited Jan. 25, 2020) (stating that DES was originally designed by IBM and there have been speculations that its algorithm was not as strong as it could have been due to interference by the National Security Agency to weaken it).

encoded message in only fifty-six hours.[167] Subsequently, one year later the same Foundation was able to decrypt a DES-encoded message in as little as twenty-two hours.[168]

Following the collapse of DES encryption, the National Institute of Standards and Technology ("NIST") set out to choose a successor to DES encryption in 1997.[169] In 2000, NIST announced that it had selected the Rijndael Encryption Algorithm as its the Advanced Encryption Standard ("AES").[170] AES encryption, which typically has a 128-bit block length, can take approximately 500 billion years to decrypt.[171] Due to its advanced protection, AES encryption is still used today.[172] There are two main classes of encryption—symmetric and asymmetric.[173] Both classes have been approved for Federal government use.[174] In 2018, NIST released a study that approximates "a $250 billion economic impact" due to AES encryption enhancements within the past twenty years.[175] The impact of encryption is being recognized across industries.[176] In August 2017, the Federal Trade Commission ("FTC") announced a settlement with Uber because the company stored data in the cloud without proper security mechanisms in place, such as

---

167. *Id.* (discussing that the DES encryption used a 56-bit key, which was not strong enough to hold off hackers if compared to the "processing power of modern computers").

168. *Id.*

169. *Id.*

170. *Cryptographic Standards and Guidelines*, NAT'L INST. OF STANDARDS & HUM. TECH., https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development (last visited Jan. 25, 2020) (explaining that NIST "worked with industry and the cryptographic community" to create AES with the goal of creating a strong algorithm for use by the U.S. government).

171. *See* JOAN DAEMAN & VINCENT RIJMEN, NAT'L INST. OF STANDARDS & HUMAN TECH., NOTE ON NAMING: RIJNDAEL 1 (2003), https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/aes-development/Rijndael-ammended.pdf ("AES fixes the block length to 128 bits, and supports key lengths of 128, 192, or 256 bits only."); Lance Gutteridge, *What's the Deal with Encryption Strength – Is 128 Bit Encryption Enough or Do You Need More?*, MEDIUM (May 6, 2016), https://medium.com/@drgutteridge/whats-the-deal-with-encryption-strength-is-128-bit-encryption-enough-or-do-you-need-more-3338b53f1e3d.

172. *See Cryptographic Standards and Guidelines*, *supra* note 170.

173. Baladi, *supra* note 160, at 254.

174. SPECIAL PUBLICATION 800-133, *supra* note 160, at 1, 6.

175. *NIST's Encryption Standard Has Minimum $250 Billion Economic Benefit, According to New Study*, NAT'L INST. OF STANDARDS & HUM. TECH. (Sept. 19, 2018), https://www.nist.gov/news-events/news/2018/09/nists-encryption-standard-has-minimum-250-billion-economic-benefit (relying on "a survey of government and private sector consumers of encryption systems and private integrators who develop and produce encryption hardware or software").

176. *See* Kevin Coy & Arnall G. Gregory, *Data Security and Breach Response Still Hot Issues: Lessons From 2017 Enforcement Actions*, L. TECH. NEWS (Nov. 3, 2017), https://www.law.com/legaltechnews/sites/legaltechnews/2017/11/03/data-security-and-breach-response-still-hot-issues-lessons-from-2017-enforcement-actions/?slreturn=20200022132108.

encryption.[177] In 2011, hackers leaked information for approximately 4000 clients of Stratfor, which is a global intelligence agency.[178]

1. Symmetric Encryption

When using symmetric encryption, the sender uses the same secret key to encrypt the text as the recipient uses to decrypt the text.[179] For example, if individual A sends information using a secret-key cryptographic algorithm to individuals B and C, then individual A must deliver that same secret key to B and C in order for them to decrypt the information.[180] This is a basic form of encryption and, because it involves the use of one key to both encrypt and decrypt, serious precautions must be taken to ensure that the key is secured.[181] The secret key may be generated by one of the entities that is sharing the key or by a trusted party.[182] The key can be dispersed manually to other entities or by using a key transport or key wrapping method to ensure security while being distributed.[183] A key is compromised if there is an unapproved disclosure, alteration, or use of sensitive data.[184] In the event of a compromise to the secret key, it should be replaced immediately by a rekeying process.[185] If there is a compromise by an unauthorized user, the best safeguard is for the key to be rekeyed.[186]

2. Asymmetric Encryption

In contrast, asymmetric encryption involves the use of two different keys, a public key for the sender to encrypt the plain text and a private key for the recipient to decrypt the text.[187] Asymmetric encryption is most commonly referred to as public-key encryption.[188] The public key may be identified by anyone and made public, but the private key must

---

177. *Id.*; *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Jan. 25, 2020) (declaring that the FTC's mission is "[p]rotecting consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity").

178. Nicole Perlroth, *Hackers Breach the Web Site of Stratfor Global Intelligence*, N.Y. TIMES (Dec. 26, 2011), https://www.nytimes.com/2011/12/26/technology/hackers-breach-the-web-site-of-stratfor-global-intelligence.html.

179. Baladi, *supra* note 160, at 254.

180. *See id.*

181. *Id.*

182. SPECIAL PUBLICATION 800-133, *supra* note 160, at 13.

183. *Id.* at 14.

184. *Id.* at 1.

185. *Id.* at 17 (defining rekeying as a process wherein a new independent key is generated in the same manner as the original key).

186. *See id.*

187. Baladi, *supra* note 160, at 254.

188. *Id.*; SPECIAL PUBLICATION 800-133, *supra* note 160, at 1.

only be known by the person intended to be able to decrypt the information.[189] The key pairs may be generated by the key-pair owner or a trusted party.[190] For example, if an individual within entity A makes a public key known to entities B and C, then entity A can control who can decrypt the information by providing a completely different secret key to only specific individuals within entities B and C.[191] Since the two keys for encrypting and decrypting are different, entity A has more secure control over the information.[192]

3. Key Management

NIST is a non-regulatory agency of the U.S. Department of Commerce and is one of the oldest physical science laboratories.[193] NIST stresses the importance of maintaining the security of secret keys and strongly encourages entities to develop key management processes.[194] If an entity elects to store a duplicate key, it should store it in a secured key repository or on physically secured removable media.[195] A key can be stored on a local hard drive, a Universal Serial Bus ("USB") flash drive, or a Trusted Platform Module ("TPM") chip, depending on the technology used for encryption.[196] Access to the stored keys must be restricted, and having multiple methods of authentication before access is ideal.[197] Mechanisms can include passwords, cryptographic tokens, or smart cards.[198]

III.   HIPAA'S PHI SAFEGUARDS: AMBIGUITIES LEAD TO BREACHES

The full extent of HIPAA is rather complex and as a result, it can lead to various ambiguities.[199] Subpart A explains the ambiguities that

---

189. SPECIAL PUBLICATION 800-133, *supra* note 160, at 12.

190. *Id.* at 11.

191. *See id.* at 12.

192. Baladi, *supra* note 160, at 254.

193. *About NIST*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/about-nist (last visited Jan. 25, 2020); *NIST General Information*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/director/pao/nist-general-information (last visited Jan. 25, 2020).

194. KAREN SCARFONE ET AL., NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-111, GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES 4-3 (2007), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf [hereinafter SPECIAL PUBLICATION 800-111].

195. *Id.* at 4-3, 4-4.

196. *Id.*; *see Trusted Platform Module (TPM) Summary*, TRUSTED COMPUTING GROUP, https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary (last visited Jan. 25, 2020) (explaining that TPM is a hardware-based computer chip that utilizes cryptography to protect information, such as encryption keys, from external attacks).

197. SPECIAL PUBLICATION 800-111, *supra* note 194, at 4-4.

198. *Id.*

199. Erica Teichert, *At 20, Is HIPAA Hitting Its Stride, or Is It Over the Hill?*, MODERN

result from HIPAA in detail.[200] Subpart B compares current state laws regarding encryption of PHI.[201] Subpart C provides an overview of recent breaches that have occurred and their impact.[202]

A. *Ambiguities Resulting from the Complexity of HIPAA*

The technical safeguards under HIPAA's Security Rule are significantly inadequate and result in ambiguities.[203] Since encryption is addressable, covered entities have one of two options.[204] They first need to determine if encryption is reasonable and appropriate.[205] If the covered entity deems that encryption does not meet that standard, then it must document why it is not reasonable and appropriate and implement an alternative that is reasonable and appropriate.[206] In turn, HIPAA creates a "race to the bottom," wherein covered entities will only perform the "bare minimum" in hopes of satisfying HIPAA regulations.[207] Moreover, the only guidance HIPAA gives regarding encryption is to "[i]mplement a mechanism to encrypt and decrypt electronic protected health information."[208] Without providing current standards on encryption, such as techniques and protocols, the probability that covered entities will make serious errors by performing only the bare minimum increases.[209]

HEALTHCARE (Aug. 13, 2016), https://www.modernhealthcare.com/article/20160813/MAGAZINE /308139964/at-20-is-hipaa-hitting-its-stride-or-is-it-over-the-hill (stating that opponents of HIPAA contend that HIPAA emanates an illusion that individuals' privacy is protected, since many providers still have insufficient privacy protocols).

200. *See infra* Part III.A.

201. *See infra* Part III.B.

202. *See infra* Part III.C.

203. Hoffman & Podgurski, *supra* note 78, at 10.

204. 45 C.F.R. § 164.306(d)(3)(i) (2013).

205. *Id.*

206. § 164.306(d)(3)(ii)(B).

207. David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 368 (2014) (internal quotation omitted).

208. 45 C.F.R. § 164.312(a)(2)(iv) (2013).

209. Hoffman & Podgurski, *supra* note 78, at 6; *Views on Health Information Security Issues from Jon Warner CEO-RX4 Group-The Business of Health*, BLOOMBERG L. (Nov. 9, 2015), https://news.bloomberglaw.com/health-law-and-business/views-on-health-information-security-issu es-from-jon-warner-ceo-rx4-group-the-business-of-health. Warner responded to Bloomberg BNA's question of whether there are safeguards that the health-care sector should be mindful of as follows:

> Best-practice in defense against cyberattacks, as exemplified in the military, nuclear industry and financial services, includes multi-layered defenses and well-planned and executed approaches of essentially breaking up and storing data in ways that make useful information very difficult to assemble. For example, banks automatically encrypt payment data and then "tokenize" it and store the information in often far-flung storage databases to create a triple layer of protection. In contrast to these, health-care providers, are at a more primitive and vulnerable stage of information technology security.

B.   *The Importance of Setting a Federal Encryption Standard Rather Than a Patchwork of State Laws*

HIPAA sets the "floor" for regulations regarding the privacy of personal health information.[210] States are not preempted by HIPAA if they enact privacy legislation that is more stringent than HIPAA's standards.[211] As of 2015, New Jersey, Massachusetts, Connecticut, and Nevada have recognized the importance of PHI encryption.[212] The primary consequence of leaving states to fend for themselves by creating their own encryption laws is that there are significant gaps within their legislation.[213] More specifically, the scope of the state-specific laws are inconsistent.[214]

For example, Massachusetts' encryption mandate has a broader scope than New Jersey's law.[215] New Jersey enacted a law that requires all personal information to be encrypted on all end-user computer systems.[216] However, the law only applies to health insurance carriers and is limited to "records transmitted across public networks."[217] In contrast, Massachusetts' law requires all companies that store any type of personal information, both paper and electronic, to implement a

---

Id.

210. Michael D. Greenberg & M. Susan Ridgely, *Patient Identifiers and the National Health Information Network: Debunking a False Front in the Privacy Wars*, 4 SUFFOLK U. L. SCH. J. HEALTH & BIOMEDICAL L. 31, 44 (2008).

211. *Id.* at 44-45; Buckman, *supra* note 34, § 2 ("Though the Privacy Rule places some limits on the disclosure of health care information [], it does not protect materials that are relevant to litigation from disclosure [].").

212. Joseph J. Lazzaroti & Jeffrey M. Schlossberg, *Connecticut Adds Significant Data Security Mandates for State Contractors, Certain Health Insurance Industry Business*, JACKSON LEWIS (July 23, 2015), https://www.jacksonlewis.com/publication/connecticut-adds-significant-data-security-mandates-state-contractors-certain-health-insurance-industry-businesses; *New Jersey Enacts Health Information Encryption Requirement*, ALSTON & BIRD: PRIVACY & DATA SECURITY BLOG (Jan. 13, 2015), https://www.alstonprivacy.com/new-jersey-enacts-health-information-encryption-requirement; *cf.* Sara A. Needles, Comment, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 304 (2009) (arguing that the market will drive states to create their own breach notification policies, in the absence of a federal blanket).

213. Michael Paluzzi, *Paying Prices for Swiped Devices: Addressing the Issue of Medical Identity Theft from Unencrypted Stolen Laptops*, 2019 U. ILL. L. REV. 1415, 1425 (2019).

214. *Id.*

215. *New Jersey Enacts Health Information Encryption Requirement, supra* note 212.

216. N.J. REV. STAT. § 56:8-197 (2015); *New Jersey Enacts Health Information Encryption Requirement, supra* note 212; Elizabeth Snell, *New Jersey Passes Health Data Encryption Law*, HEALTH IT SECURITY (Jan. 12, 2015), https://healthitsecurity.com/news/new-jersey-passes-health-data-encryption-law (stating that the legislation also applies to "computerized records transmitted across public networks"); *see* Deck, *supra* note 163 (noting how potentially easy it is to access PHI from unencrypted end-user devices — "a thief can simply remove the hard drive, install it on another computer, and copy the data").

217. § 56:8-197.

comprehensive information security program.[218] Massachusetts' law also mandates precise encryption requirements for electronic transfer or storage of personal information.[219] Encryption is explicitly defined as the use of 128-bit or higher algorithmic process, which provides much more clarity than New Jersey's law.[220] Moreover, the Massachusetts law requires encryption of all personal information stored on laptops and other transportable devices that is transmitted not only across public networks, but also wirelessly.[221] In that sense, Massachusetts currently represents the "gold standard" and all other states that fail to uphold such a standard have legislation that is meaningfully lacking.[222]

In 2010, Nevada amended its data security law to mandate encryption of personal information on data storage devices that are moved beyond the logical or physical controls of the business.[223] The Massachusetts regulation is also broader than that of Nevada's because the Massachusetts standard "require[s] encryption of personal information on portable devices even if such devices do not leave the premises of the business."[224] In Nevada, data storage devices include computers and cellular phones.[225] Nevada legislation also specifies that encryption technology must use an established standard, such as the NIST.[226]

On the other hand, entities in states that have not adopted any encryption mandate are even less protected.[227] For example, New York does not have an encryption mandate for PHI.[228] As recently as November 2019, the University of Rochester Medical Center had to pay "a $3 million HIPAA penalty for the failure to encrypt mobile devices

---

218. 201 MASS. CODE REGS. 17.01, 17.03 (2017).

219. 17.04(3), (5); John L. Nicholson & Meighan E. O'Reardon, *Data Protection Basics: A Primer for College and University Counsel*, 36 J.C. & U.L. 101, 124 (2009).

220. MASS. GEN. LAWS ch. 93H, § 1 (2007); *see also* § 56:8-197.

221. 201 MASS. CODE REGS. 17.04(3), (5) (2018).

222. Kevin D. Lyles et al., *Massachusetts Law Raises the Bar for Data Security*, JONES DAY (Feb. 2010), https://www.jonesday.com/en/insights/2010/02/massachusetts-law-raises-the-bar-for-data-security.

223. S.B. 227, 2009 Leg., 75th Sess. (Nev. 2009).

224. Lyles et al., *supra* note 222.

225. S.B. 227.

226. *Id.*

227. *See Lack of Encryption Leads to $3 Million HIPAA Penalty for New York Medical Center*, HIPAA J. (Nov. 6, 2019), https://www.hipaajournal.com/lack-of-encryption-leads-to-3-million-hipaa-penalty-for-new-york-medical-center.

228. Joseph J. Lazzarotti et al., *New York Enacts SHIELD Act*, NAT'L L. REV. (July 26, 2019), https://www.natlawreview.com/article/new-york-enacts-shield-act (stating the security requirements for personal information require a person or business to "develop, implement, and maintain reasonable safeguards").

and other HIPAA violations."[229] Other states such as Delaware, Oregon, and Illinois also have similar reasonable standards like New York, rather than a required encryption standard as in Massachusetts.[230] The result is less secure PHI, which leaves confidential information vulnerable to data breaches by unauthorized individuals.[231]

C. *Current Impact of Breaches on Entities and Consumers*

In June 2018, OCR announced a $4.3 million civil penalty on the University of Texas MD Anderson Cancer Center.[232] The penalty was due to three data breaches that occurred in 2012 and 2013.[233] The first breach occurred because an unencrypted laptop was stolen from an employee's home and the other two breaches were due to lost unencrypted USB devices.[234] MD Anderson had identified the key risk area between 2010 and 2011, but did not take steps to mitigate the problem, which resulted in over 34,000 patients' PHI being potentially exposed to unauthorized users.[235]

A recent data breach settlement, and the largest, occurred in August 2018 when Anthem Health Insurance, a large health insurance company, settled a class-action lawsuit for $115 million.[236] The class-action consisted of 19.1 million consumers affected by a data breach that exposed 78 million people's PHI.[237] The breach occurred due to a

---

229. *Lack of Encryption Leads to $3 Million HIPAA Penalty for New York Medical Center*, *supra* note 227.

230.   815 ILL. COMP. STAT. 530/45 (2017); Nicholson & O'Reardon, *supra* note 219, at 124; David Krone, *Delaware Amends Data Breach Notification Law to Require Reasonable Data Security and Expand the Scope of Personal Information Requiring Notice*, REED SMITH LLP (Aug. 28, 2017), https://www.technologylawdispatch.com/2017/08/privacy-data-protection/delaware-amends-data-breach-notification-law-to-require-reasonable-data-security-and-expand-the-scope-of-personal-information-requiring-notice; *Oregon Updates Data Breach Notification Law to Include Vendors of Covered Entities*, HIPPA J. (June 7, 2019), https://www.hipaajournal.com/oregon-updates-data-breach-notification-law-to-include-vendors-of-covered-entities.

231.   Elizabeth Snell, *Healthcare Data Encryption Not 'Required,' but Very Necessary*, HEALTH IT SECURITY (June 14, 2017), https://healthitsecurity.com/news/healthcare-data-encryption-not-required-but-very-necessary.

232.   *OCR Announces $4.3 Million Civil Monetary Penalty for University of Texas MD Anderson Cancer Center*, HIPAA J. (June 19, 2018), https://www.hipaajournal.com/ocr-4-3-million-cmp-university-texas-md-anderson-cancer-center (stating that, at the time, it was the fourth largest HIPAA violation penalty).

233. *Id.*

234. *Id.*

235. *Id.* (finding that "[i]f MD Anderson had implemented encryption on all portable devices containing ePHI, the three breaches would have been prevented").

236. Daniel R. Stroller, *Anthem $115 Million Data Breach Settlement Approved by Judge*, BLOOMBERG L. (Aug. 16, 2018), https://news.bloomberglaw.com/privacy-and-data-security/anthem-115-million-ddata-breach-settlement-approved-by-judge-1.

237. *Id.*

cyber-attack that began with an employee opening a phishing email.[238] The PHI included Social Security numbers, dates of birth, names, and healthcare ID numbers.[239] The class member pool was given a cap of $15 million for out-of-pocket expenses and free credit monitoring.[240] Anthem agreed to improve its data security strategies and implement encryption protocols.[241] Aside from the settlement, Anthem spent $2.5 million on expert consultants, $31 million on breach notifications to individuals, and $112 million for free credit reporting prior to the settlement.[242]

Between 2009 and 2018, there were approximately 2546 data breaches.[243] This resulted in 189,945,874 healthcare records being either stolen or exposed, representing sixty percent of the United States population.[244] Over the years, providers have had the most amount of breaches compared to health plans and business associates.[245]

One of the biggest challenges for state courts is to determine the amount of damages for data breach cases, such as with Anthem.[246] The crux of the problem is that breaches do not typically have "specific victims who could tie identity loss or financial crimes to the incidents despite affecting millions of people."[247] In October 2018, the Trump Administration announced plans to develop an intricate proposal wherein money may be obtained from the penalty imposed on hospitals or health systems when they violate federal health privacy laws and may then be given to the individuals that are affected by the data breaches.[248] The effect of sharing penalties and settlements with those individuals that are harmed by the breaches can lead to an increase of data breach

---

238. Marianne K. McGee, *A New In-Depth Analysis of Anthem Breach*, BANK INFO SECURITY (Jan. 10, 2017), https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627.

239. Stroller, *supra* note 236.

240. *Id.*

241. *Id.*

242. McGee, *supra* note 238.

243. *Healthcare Data Breach Statistics*, HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics (last visited Jan. 25, 2020) (noting "[h]ealthcare data breaches are now being reported at a rate of more than one per day").

244. *Id.*

245. *Id.* In 2009, there was a total of eighteen breaches, wherein fourteen were from providers, one from a health plan, and three from business associates. *Id.* In contrast, there was a total of 269 breaches in 2015. *Id.* Of those, 196 were from providers, 62 were from health plans, and 11 were from business associates. *Id.* Most recently in 2018, there were 365 breaches in total. *Id.* Of those, 273 were from providers, 53 were from health plans, and 39 were from business associates. *Id.*

246. Alex Ruoff, *Hospital Data Breaches Could Mean a Payday for Their Patients*, BLOOMBERG L. (Oct. 17, 2018), https://www.bloomberglaw.com/document/X91QMUOK000000?b na_news_filter=health-law-and-business&jcsearch=BNA%2520000001668318deb4a166df1a5d6f0 002#jcite.

247. *Id.*

248. *Id.*

reports and hospitals improving their information security.[249] The complexity of the Trump administration's potential proposal lies in determining "what it means to be harmed by a data breach, when someone's health records or information about their health status is divulged without their consent, and how much someone should receive for it."[250] HHS began to accept comments about sharing the penalties and settlements in January 2019.[251] Opponents to the proposed change, which predominantly consists of physicians groups and hospital groups, are anticipated to contend that HHS would unduly burden health systems if it were to impose a penalty amount that would provide compensation to those who had their records compromised.[252]

IV. CLEARING A PATH TO IMPROVED PHI SECURITY BEGINS WITH AMENDING HIPAA

The Internet Architecture Board, which is a committee of the Internet Engineering Task Force, released a statement in 2014 calling for encryption to become the "norm for Internet traffic."[253] It has been over twenty years since HIPAA was enacted and as technology advances, HIPAA desperately needs to be updated.[254] Subpart A discusses how HIPAA should be amended.[255] Subpart B discusses the importance of independent audits in creating greater compliance.[256] Subpart C discusses the future implications of HIPAA.[257]

---

249. *Id.*

250. *Id.*

251. *Id.*

252. *Id.*

253. Sharon Shea, *Encryption Everywhere: Debating the Risks and Rewards*, TECHTARGET (Nov. 21, 2014), https://searchsecurity.techtarget.com/news/2240235173/Encryption-everywhere-Debating-the-risks-and-rewards; *see About*, IETF, https://www.ietf.org/about (last visited Jan. 25, 2020) ("The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.").

254. Dan Bowman, *Why HIPAA Needs an Update*, FIERCE HEALTHCARE (Nov. 4, 2016), https://www.fiercehealthcare.com/regulatory/why-hipaa-needs-update   (stating   that   innovation occurs over time and although HIPAA may have been innovative in 1996, the challenges we face with data privacy and security today are different).

255. *See infra* Part IV.A.

256. *See infra* Part IV.B.

257. *See infra* Part IV.C.

A.   *Legislative Action: HIPAA Should Mandate Encryption of PHI on All End-User Devices*

This Note proposes that Congress should amend HIPAA to mandate encryption.[258] The language of the technical safeguards under the Security Rule should be amended as follows: *"Encryption and decryption on end-user devices (Mandatory).*[259] Implement a mechanism to encrypt and decrypt electronic protected health information."[260] This will help eliminate a vast amount of ambiguities regarding technical safeguards and it will make encryption uniform across states.[261] End-user devices should be defined to include "laptops, smartphones, tablets, and any portable device."[262] This amended language should continue to apply to both covered entities and business associates on all end-user devices.[263] A report by WinMagic Data Security suggests that a method for protecting mobile devices should be incorporated into the infrastructure and data security strategy of a business since devices may run on different operating systems.[264] Opponents of encryption contend that implementation of encryption on all computing devices within an entity becomes an IT nightmare.[265] However, methods of encryption have advanced and if an entity invests in a "well-designed encryption

---

258.   *See infra* Part IV.A.

259.   *See* 45 C.F.R. § 164.312(a)(2)(iv) (2013) (stating that encryption is currently only "addressable").

260.   *See id.*

261.   Tim Wafa, *How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy*, 30 N. ILL. U. L. REV. 531, 539, 541 (2010) (stating that because data can presently be protected through a variety of different methods, it becomes overwhelming for providers to choose an appropriate technology standard).

262.   SPECIAL PUBLICATION 800-111, *supra* note 194, at B-1 (defining an end-user device as "[a] personal computer (desktop or laptop), consumer device (e.g., personal digital assistant [PDA], smart phone), or removable storage media (e.g., USB flash drive, memory card, external hard drive, writeable CD or DVD) that can store information").

263.   *See* Kulwicki, *supra* note 98, at 475-76 (stating that portable devices are likely to be stolen and so they should be encrypted); *see also Views on Health Information Security Issues from Jon Warner CEO-RX4 Group-The Business of Health*, *supra* note 209 ("Responding is not merely waiting for an attack, but rather proactive and well-thought through governance and risk mitigation.").

264.   Michelle McNickle, *7 Commons Myths About Data Encryption*, HEALTHCARE IT NEWS (May 14, 2012), https://www.healthcareitnews.com/news/7-common-myths-about-data-encryption (finding that "[m]odern solutions allow you to monitor the data security status of all devices used by a user, irrespective of the form factor or operating system used, within a single administration console").

265.   *Data Encryption Demystified: Seven Common Misconceptions and the Solutions That Dispel Them*, WINMAGIC DATA SECURITY 5 (2012), http://docs.media.bitpipe.com/io_10x/io_10484 1/item_535783/WM_Data_Encryption_Demystified_White_Paper_20120316.pdf.

solution and central administrative management tools" it can ensure that encryption has a nominal effect on users.[266]

Asymmetric keys should be required to be used in hospitals and health insurance companies.[267] Asymmetric cryptographic keys are more costly in time and resources than symmetric cryptographic keys because they are much longer.[268] Accordingly, the first provision of the implementation section of the amended Security Rule should state: "Hospitals and insurance companies are required to implement asymmetric encryption on all end-user devices."[269] On the other hand, smaller covered entities and business associates should be required to use, at minimum, symmetric encryption keys.[270] The second provision of the implementation section should state: "All other entities are required to implement symmetric encryption on all end-user devices."[271] However, entities need to conduct independent audits to determine if they have adequate protection because symmetric encryption may not be enough.[272] Therefore, the second provision should be expanded to include: "(a) All entities that use symmetric encryption must conduct risk analysis assessments each year to determine if the gap in security necessitates asymmetric encryption.[273] If asymmetric encryption would abridge the security gap, then the entity must implement it."[274] Based on risk assessments and other factors, such as financial feasibility, size, and complexity of the entity, entities may be required to use asymmetric encryption.[275] Accordingly, the second provision should also be expanded to include: "(b) Entities should also consider factors such as

---

266. *Id.*

267. *See* Ashley Blume, *Healthcare Data Encryption Methods for Healthcare Providers*, HEALTH IT SECURITY (Nov. 7, 2012), https://healthitsecurity.com/news/healthcare-data-encryption-methods-for-healthcare-providers (discussing that symmetric key encryption may be easier for healthcare employees, such as doctors and nurses, but when there are many users within an entity, the information is not as likely to remain secure).

268. Matt Blumenthal, Encryption: Strengths and Weaknesses of Public-Key Cryptography 3 (unpublished manuscript) (on file with Villanova University), http://www.csc.villanova.edu/~mdam ian/Past/csc3990fa08/csrs2007/01-pp1-7-MattBlumenthal.pdf.

269. *See* Blume, *supra* note 267.

270. *Id.* (stating that symmetric key encryption would be easier for healthcare employees in a small business with not as many authorized users who have access to the secret key).

271. *See id.*

272. *See infra* Part IV.B.

273. *See Guidance on Risk Analysis*, U.S. DEP'T HEALTH & HUM. SERVS. (July 22, 2019), https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (stating that risk analysis is very helpful for businesses to determine their HIPAA compliance).

274. *See id.*

275. *See* Kulwicki, *supra* note 98, at 463 (stating that entities should consider size, complexity, technical infrastructure, and costs when selecting an appropriate security measure).

size, complexity, technical infrastructure, and costs when selecting an appropriate security measure."[276]

Opponents of encryption claim that the costs associated with it will burden companies that may not have the resources.[277] However, this argument is unsound because the costs that a company may incur due to HIPAA breach civil penalties ultimately outweigh encryption costs in the long-run.[278] Business executives and health providers are not security experts and so they rely on their IT team to protect the entity from breaches.[279] Large companies tend to have more vulnerabilities.[280] Small companies tend to have smaller security budgets.[281] Most companies, no matter the size, may be hesitant to allocate funds for encryption and digital security voluntarily.[282] By mandating encryption, top executives will have to provide IT teams with an adequate budget to protect PHI sufficiently.[283]

Furthermore, in order to create a basic level of uniformity, the Security Rule should also be amended to include: *"Standard.* All encryption technology used for end-user devices should comply with an established standard, such as the National Institute of Standards and Technology."[284] The encryption standard in the proposed amendment to HIPAA is consistent with the financial industry, which is one of the most regulated in the world.[285] The Federal Financial Institutions Examination Council ("FFIEC") and the new European Union General Data Protection Regulation ("GDPR") both recommend encryption for financial institutions.[286] NIST guidelines efficiently assimilate with

---

276. 45 C.F.R. § 164.306(b)(2) (2013); *see* Kulwicki, *supra* note 98, at 463.

277. Jen Stone, *How Much Does HIPAA Compliance Cost?*, SECURITYMETRICS: BLOG, https://www.securitymetrics.com/blog/how-much-does-hipaa-compliance-cost (last visited Jan. 25, 2020).

278. *Id.*

279. *Why Isn't Everyone Using Encryption in Health Care?*, VIRTRU, https://www.virtru.com/blog/encryption-in-health-care/#newsletter (last visited Jan. 25, 2020).

280. Stone, *supra* note 277.

281. *Id.*

282. *Id.*

283. *See id.*

284. *See* SPECIAL PUBLICATION 800-133, *supra* note 160, at 1-6.

285. Luke Probasco, *Encryption Requirements for Banks & Financial Services*, TOWNSEND SECURITY DATA PRIVACY: BLOG, https://info.townsendsecurity.com/encryption-requirements-for-banks-financial-services (last visited Jan. 25, 2020).

286. Aamir Lakhani, *For Financial Services, Encryption is Essential—But So Is Performance*, INT'L DATA GROUP COMM. (June 26, 2018), https://www.csoonline.com/article/3284351/security/fo r-financial-services-encryption-is-essential-but-so-is-performance.html (noting that the FFIEC "provides standards and principles for the supervision of financial institutions, [and] states that financial services should incorporate encryption to protect personal data in transit and storage"). In contrast, the GDPR, which took effect in May 2018, "expects financial firms to have state-of-the-art security in place to protect data. While these rules do not provide specific security tool

FFIEC guidelines.[287] Therefore, banks and financial services also use the NIST's AES encryption standard.[288] Similar to HIPAA, compliance regulations for financial industries also have a safe harbor if the loss of financial data was encrypted.[289]

B. *Mandatory Annual Independent Audits by Covered Entities*

The most recent HHS OCR audit of covered entities and business associates began in 2016.[290] The results from Phase I of the audit program, based on those released thus far from the desk audits of Phase II, indicate that providers and health plans are not satisfying OCR's compliance requirements.[291] However, there has been no initiative on behalf of OCR to attempt to abridge the knowledge gap and provide educational materials to healthcare providers on compliance.[292] OCR likely does not have the resources to conduct audits frequently and the Office of the Inspector General in 2013 issued a report finding that the OCR was lacking in supervising the audit process of covered entities.[293]

Thus, covered entities should be mandated to undergo independent audits every year under HIPAA to protect patients from breaches.[294] The independent auditor should use the latest OCR HIPAA audit protocol as a guideline.[295] The resulting compliance reports should be used internally by the covered entity to gauge the effectiveness of safeguards and the covered entity should remedy any problems.[296] Any remedies taken by the covered entity should be thoroughly documented.[297] Thereafter, the audit compliance report, along with the document entailing the actions taken by the covered entity, should be kept on file internally for six

---

requirements, Article 32 of the regulation does recommend the use of pseudonymization and encryption." *Id.*

287. Randy Lindberg, *How NIST Is Helping Financial Institutions with Cybersecurity*, RIVAL (Apr. 4, 2018), https://www.rivialsecurity.com/blog/how-nist-is-helpng-financial-institutions-with-cybersecurity (stating that FFIEC announced a Cybersecurity Assessment Tool ("CAT") in 2015, which was constructed to integrate with the NIST framework).

288. Probasco, *supra* note 285.

289. *Id.*

290. *HIPAA Privacy, Security, and Breach Notification Audit Program*, *supra* note 135.

291. Swann, *supra* note 136.

292. *Id.*

293. Hsieh, *supra* note 108, at 189-90.

294. *See id.* at 179 (discussing how an increase in audits would "better protect patients from all . . . types of privacy breaches").

295. *See HIPAA Privacy, Security, and Breach Notification Audit Program*, *supra* note 135.

296. Hsieh, *supra* note 108, at 189 (stating that "requiring corrective action is an effective way of obtaining compliance with HIPAA because it allows covered entities to change their internal policies to better comply with HIPAA regulations moving forward").

297. *See* 45 C.F.R. § 164.316(b)(1) (2013).

years.[298] If a breach occurs, then OCR can require the covered entity to produce the compliance reports for the previous six years.[299] This solution will force the covered entity to take corrective action on its own every year, and, in the case that a breach occurs, there will be more transparency between OCR and the covered entity.[300]

C. *Future Implications of Encryption on Healthcare*

As technology advances, HIPAA must also evolve to address the challenges faced by healthcare providers to protect PHI.[301] Mandating encryption is a pivotal step towards protecting PHI as more information is accessed through end-user devices.[302] Mandatory encryption will help prevent data breaches by safeguarding against threats.[303] The impact it will have on network performance will be minimal if managers utilize the proper methods of encryption.[304]

We are in "the machine-learning phase of the Digital Age."[305] A prime example is artificial intelligence ("AI").[306] AI can be defined differently based on the industry, but in healthcare it means "'a collection of multiple technologies enabling machines to sense, comprehend, act and learn' so they can perform administrative and clinical health-care functions."[307] AI is used within the healthcare

---

298. *See* § 164.316(b)(2)(i) (stating that when an entity elects to not implement encryption or an alternative, the entity must document its reasoning and retain it for six years).

299. *Cf.* § 164.316(b)(2)(ii) (stating that the documentation must be made available to "those persons responsible for implementing the procedures to which the documentation pertains").

300. *Openness and Transparency*, *supra* note 32 (discussing the Openness and Transparency Principle, which encourages health organizations to be more transparent with regards to how they protect an individual's identifiable health information).

301. *See* Shea, *supra* note 253.

302. Nick Jovanovic, *Using Encryption to Help Fight Data Breaches*, GCN (July 13, 2018), https://gcn.com/articles/2018/07/13/encryption-key-management-cloud.aspx (discussing how there is "no silver bullet" to cybersecurity since a comprehensive plan involving different technologies, policies, and training is most effective, and deploying encryption technology is crucial to the plan).

303. *Id.* (stating that encryption "offers increased protection to known and unknown sensitive data in advanced technology environments").

304. *Id.* (stating that the current notion people have regarding the impact of encryption on network performance is inaccurate because methods of encryption have advanced since the early days when encryption was software-based).

305. R.L. Adams, *10 Powerful Examples of Artificial Intelligence in Use Today*, FORBES (Jan. 10, 2017), https://www.forbes.com/sites/robertadams/2017/01/10/10-powerful-examples-of-artificia l-intelligence-in-use-today/#3271098b420d (stating that AI technology is still at its early stage and "[a] true artificially-intelligent system is one that can learn on its own").

306. *Artificial Intelligence: What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/in sights/analytics/what-is-artificial-intelligence.html (last visited Jan. 25, 2020) (stating that artificial intelligence research began in 1950s and ten years later, the U.S. Department of Defense started its own projects to develop "thinking machines," and today, many industries aim to benefit from AI technologies).

307. James Swann, *Talking to a Robot: Technology Comes to Health Insurance (2)*,

industry to deliver personalized medicine and x-ray readings.[308] Moreover, AI personal assistants can personify life coaches that remind patients to take their medications or to exercise.[309] AI algorithms have the potential to bring major advancements in healthcare because they can help bring our attention to "relationships and patterns that escape us."[310]

HIPAA requires companies to secure PHI, irrespective of the technology, so long as it has the potential to impact the privacy or security of the data.[311] However, AI technologies also raise new privacy and security risks that HIPAA will eventually need to address.[312] It largely depends on whether AI uses the health data it collects for health care operations or for developing a new commercial product.[313] Three major companies that use AI and have a vision for the future of healthcare are IBM, Google, and Amazon.[314]

The federal government is also at the forefront of AI as it announced in 2018 that it will launch "a competition next year to find the best ways to use artificial intelligence to transform the delivery of health care."[315] Meanwhile, HHS released a Request for Information

---

BLOOMBERG L. (Aug. 8, 2018), https://news.bloomberglaw.com/health-law-and-business/talking-to-a-robot-technology-comes-to-health-insurance-2 (stating that "[d]evelopers of artificial intelligence solutions can expect a high level of growth as insurers continue to look for ways to cut costs and improve patient health").

308. *Artificial Intelligence: What It Is and Why It Matters*, *supra* note 306.

309. *Id.*

310. *Id.*

311. Abner Weintraub, *Consider HIPAA When Using A.I. & Machine Learning*, MEDSTACK (Nov. 14, 2017), https://medstack.co/blog/consider-hipaa-using-machine-learning.

312. *See* James Swann, *AI Overcoming Bad Records to Help Hospitals Run Themselves*, BLOOMBERG L. (Nov. 30, 2018), https://news.bloomberglaw.com/health-law-and-business/ai-overcoming-bad-records-to-help-hospitals-run-themselves (stating that patient privacy is a concern because AI is able to process a large amount of data).

313. *Id.* (stating that using AI for developing a commercial product may result in a HIPAA violation).

314. Clare McGrane, *Amazon Unveils New Service to Mine and Decode Medical Records Using Artificial Intelligence*, GEEKWIRE (Nov. 27, 2018), https://www.geekwire.com/2018/amazon-unveils-new-service-mine-decode-medical-records-using-artificial-intelligence (stating that Amazon is using Comprehend Medical, which is "a new machine learning service that uses natural language processing to decode the information in unstructured writing like medical records or even doctor's notes"); Parmy Olson, *Why Google Just Tightened Its Grip on DeepMind*, FORBES (Nov. 14, 2018), https://www.forbes.com/sites/parmyolson/2018/11/14/why-google-just-tightened-its-grip-on-deepm ind/#79edacef2789 (stating that Google acquired DeepMind, an artificial intelligence startup, and it is directly managing DeepMind Health to "achieve its social mission"); *Watson Health: Get the Facts*, IBM (Nov. 19, 2018), https://www.ibm.com/blogs/watson-health/watson-health-get-facts (stating that IBM Watson Health has eighty AI Services, including Annotator for Clinical Data, Insights for Patient Data, Patient Similarity, and Medical Insights. Most notably, Watson is using AI in the field of oncology "in more than 270 hospitals and health organizations, and a large, growing body of evidence supports the use of Watson in healthcare"); Weintraub, *supra* note 311.

315. Mike Miliard, *CMS Innovation Center Set to Launch AI Health Outcomes Challenge*, HEALTHCARE IT NEWS (Nov. 20, 2018), https://www.healthcareitnews.com/news/cms-innovation-

("RFI") in December 2018 to obtain input on how HIPAA Rules should be modified to promote value-based healthcare.[316] The opioid crisis was a key driver for HHS to issue an RFI in the first place.[317]

V. CONCLUSION

While some data breaches may inevitably occur, it is important for health care providers to implement safeguards to protect the personal health information of patients.[318] After all, the purpose of HIPAA when it was created in 1996 was to prevent fraud and abuse of health information.[319] Amending HIPAA will encourage covered entities and business associates to actively protect PHI in all corners of healthcare.[320] The proposed legislation is specifically designed to help bridge gaps in the HIPAA security safeguards and takes into consideration various entities' size, complexity, and costs.[321] The encryption of end-user devices and mandatory independent audits will notably improve PHI security and diminish the probability of future breaches.[322] Entities will ultimately be compelled to take a preventative approach, rather than

---

center-set-launch-ai-health-outcomes-challenge (stating that the "cross-industry competition [is] seeking new strategies to innovate how AI can be safely implemented in existing and proposed new models of care"); Swann, *supra* note 312 (stating that the competition will be funded through the America COMPETES Reauthorization Act and it will be CMS's first competition under the Act).

316. Press Release, U.S. Dep't Health & Hum. Servs., HHS Seeks Input on Improving Care Coordination and Reducing the Regulatory Burdens of HIPAA Rules (Dec. 12, 2018), https://www.hhs.gov/about/news/2018/12/12/hhs-seeks-public-input-improving-care-coordination-and-reducing-regulatory-burdens-hipaa-rules.html (stating that "RFI is part of the Regulatory Sprint to Coordinated Care, an initiative led by Deputy Secretary Eric Hargan") [hereinafter Press Release, U.S. Dep't Health & Hum. Servs.].

317. Rajiv Leventhal, *Report: Privacy Laws to Remain Intact as Opioids Bill Nears Completion*, HEALTHCARE INNOVATION (Sept. 25, 2018), https://www.hcinnovationgroup.com/cyb ersecurity/news/13030740/report-privacy-laws-to-remain-intact-as-opioids-bill-nears-completion (stating that under federal law, mental health records are required to be kept "separate from other health records and prevents the sharing of these confidential treatment records without a patient's one-time consent"); Kirk J. Nahra, *Insight: The Top Five Health Care Privacy and Security Issues to Watch in 2019*, BLOOMBERG L. (Dec. 21, 2018), https://news.bloomberglaw.com/health-law-and-business/insight-the-top-five-health-care-privacy-and-security-issues-to-watch-in-2019 (stating that the RFI, which occurs nine years after the HITECH Act was announced, may lead to "meaningful change to some of the core provisions of the HIPAA Rules"); Press Release, U.S. Dep't Health & Hum. Servs., *supra* note 316 (stating that HHS received concerns that the Privacy Rule may "impede" care coordination, which resulted in patients not being able to access holistic care).

318. Elizabeth Snell, *How Administrative Safeguards Can Prevent Data Breaches*, HEALTH IT SECURITY (Dec. 29, 2015), https://healthitsecurity.com/news/how-administrative-safeguards-can-prevent-data-breaches.

319. *See supra* Part II.

320. *See supra* Part IV.B.

321. *See supra* Part IV.A.

322. *See supra* Part IV.B–C.

completely rely on an identify-and-contain approach.[323] This would partly be due to the elimination of ambiguities regarding HIPAA encryption standards and the drive towards uniformity of the standard across states for both covered entities and business associates.[324] While the costs of implementing encryption across all end-user devices may be high, it is still likely to be much lower than the fines associated with a HIPAA violation.[325] It is a beneficial tradeoff that can save the entity HHS fines, attorneys fees, patient loss, technology repairs for corrective action post-breach, and breach notification costs.[326]

Nina Patel*

---

323. *See* Snell, *supra* note 318.

324. *See supra* Parts III.A, IV.A.

325. *Data Encryption Advisable but Not Mandatory Under HIPAA*, HIPAA J. (Feb. 1, 2013), https://www.hipaajournal.com/data-encryption-advisable-mandatory-hipaa.

326. Stone, *supra* note 277 (finding that lawyer fees can be over $2,000, breach notification costs can exceed $1,000, technology repairs can exceed $2,000, HHS fines can be up to $1.5 million per violation per year, and patient loss can be up to 40%).

***