EVALUATING SOLUTIONS TO CYBER ATTACK BREACHES OF HEALTH DATA: HOW ENACTING A PRIVATE RIGHT OF ACTION FOR BREACH VICTIMS WOULD LOWER COSTS

Ryan L. Garner*

TABLE OF CONTENTS

* J.D., 2017, Indiana University Robert H. McKinney School of Law; B.S., 2013, Indiana University.

I. INTRODUCTION

On January 29, 2015, Anthem, Inc. ("Anthem") discovered that its data storage systems were breached by a cyber attack.[1] Anthem, the second largest health insurance corporation in the United States,[2] reported the breach occurred over several weeks in December 2014.[3] Nearly 80 million patients had their records breached.[4] The data breach

---

8u[1] *How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services*, ANTHEM (Aug. 25, 2015, 9:00), https://www.anthemfacts.com [https://perma.cc/2BB6-3N96] [hereinafter *Anthem Identity Theft Repair*].

[2] *See* Li Anne Wong, *Anthem hacked, millions of records likely stolen*, CNBC (Feb. 4, 2015, 10:00 PM), http://www.cnbc.com/2015/02/04/health-insurer-anthem-hit-by-hackers-report.html [https://perma.cc/LS4X-QB9F].

[3] *Anthem Identity Theft Repair*, *supra* note 1.

[4] Kelli B. Grant & Ben Popken, *What Anthem breach victims need to do now*, CNBC (Feb. 5, 2015, 11:53 AM),

included personal information of current customers, former customers, and employees.[5] According to Anthem, hackers were able to access personal information, including "names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information, including income data."[6] Initial reports indicated no evidence that payment information or medical data were stolen in the data breach.[7]

While Anthem was surprised that the cyber attack occurred, the events were reasonably foreseeable. In August 2014, following the breach of information in the systems of Community Health Network, the United States Federal Bureau of Investigation warned healthcare companies that patient health information was a continuous target of cyber attacks.[8] In 2015 alone, over 112 million health records were compromised as the result of data breaches.[9] While all cyber attacks are concerning, at nearly 80 million records, the

---

http://www.cnbc.com/2015/02/05/what-anthem-breach-victims-need-to-do-now.html [https://perma.cc/4D74-ZUBE].

[5] *Id.*

[6] *Anthem Identity Theft Repair*, *supra* note 1.

[7] *See* Grant & Popken, *supra* note 4. The authors point out that the "silver lining" was that medical data was not accessed, as this stolen information could lead to bribery. *Id.* However, the information breached poses greater risks for victims. *Id.* When payment information is stolen, credit cards can be immediately canceled, and bank accounts can be immediately frozen; but, when information such as Social Security numbers and birthdates are stolen, victims will have to monitor against fraud for the rest of their lives. *Id.*

[8] Wong, *supra* note 2.

[9] Dan Munro, *Data Breaches In Healthcare Totaled Over 112 Million Records In 2015*, FORBES (Dec. 31, 2015, 09:11 PM), http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/ [https://perma.cc/54Y4-G7PX].

Anthem breach was most noteworthy.[10] The Anthem breach was the largest reported healthcare data breach to date.[11] President Barack Obama's cyber security advisor, Michael Daniel, commented, "[o]bviously it's quite concerning that we would have yet another intrusion of this size . . . . It's particularly disturbing especially when it hits that many people."[12]

While the magnitude of the breach is rather certain, the complexity and method of attack is still hotly contested. Anthem CEO Joseph R. Swedish reported to his customers that the incident was a "very sophisticated external cyber attack."[13] Many industry leaders, including FireEye, Inc.—owner of cybersecurity unit Mandiant, the firm Anthem hired to investigate—agreed with Anthem.[14] FireEye managing director David Damato asserted, "The Anthem attack was 'sophisticated' and used techniques that appeared to have been customized, rather than broadly available tools, and were 'very advanced.'"[15]

---

[10] *Id.* "According to [Office of Civil Rights of the Department of Health and Human Services], there were 253 healthcare breaches that affected 500 individuals or more with a combined loss of over 112 million records." *Id.* Of those breaches, six affected more than one million people. *Id.* At nearly 80 million records, the Anthem breach was roughly seven-times larger than the next-largest breach of 2015. *Id.*

[11] Wong, *supra* note 2.

[12] *Obama cyber czar: Anthem hack 'quite concerning'*, CNBC (Feb. 5, 2015, 10:55 AM), http://www.cnbc.com/2015/02/05/obama-cyber-czar-anthem-hack-quite-concerning.html [https://perma.cc/7NPN-A9BY].

[13] *From the Desk of Joseph R. Swedish*, ANTHEM (Feb. 23, 2015, 6:00 AM), https://www.anthemfacts.com/ceo [https://perma.cc/SWS7-QF7H].

[14] Anna Wilde Mathews & Danny Yadron, *Health Insurer Anthem Hit by Hackers*, WALL ST. J. (Feb. 4, 2015, 9:39 PM), http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 [perma.cc/QR6Z-6KB5].

[15] *Id.*

However, some disagreed and asserted that the attack was much more rudimentary; these experts explained that the attack was initiated by sending out "phishing" emails to Anthem employees.[16] The attackers sent a large number of seemingly legitimate emails and hoped that at least one employee clicked on an embedded link in the email.[17] If the fake link was clicked by just one employee, attached malware could infect the Anthem system and allow the attackers to gather username and passwords.[18] Once equipped with valid employee credentials, the hackers simply had to login to Anthem's real systems.[19] Simply put, this cyber attack was akin to a carjacking,[20] except that the perpetrators pickpocketed the keys, unlocked the doors, and drove away without having to break any windows and hotwire the vehicle.

After the Anthem attack, victims were advised to monitor their existing accounts, sign up for credit monitoring and identify theft protection, sign up for fraud alerts, and remain vigilant.[21] Now the industry standard, all Anthem customers were eligible to receive two years of complimentary AllClear PRO service, which included credit monitoring and an identity theft insurance policy.[22]

---

[16] Jeremy Kirk, *Premera, Anthem data breaches linked by similar hacking tactics*, COMPUTER WORLD (Mar. 18, 2015, 3:37 AM), http://www.computerworld.com/article/2898419/data-breach/premera-anthem-data-breaches-linked-by-similar-hacking-tactics.html [perma.cc/K56L-FDVN].

[17] *See id.*

[18] *See id.*

[19] *See id.*

[20] *See, e.g.,* Fred Trotter, *Anthem Was Right Not to Encrypt*, THE HEALTH CARE BLOG (Feb 9, 2015), http://thehealthcareblog.com/blog/2015/02/09/anthem-was-right-not-to-encrypt [https://perma.cc/Q9R7-LTFK].

[21] Grant & Popken, *supra* note 4.

[22] *Anthem Identity Theft Repair*, *supra* note 1; s*ee also How Anthem is Protecting You*, ALLCLEAR ID, https://anthem.allclearid.com [perma.cc/X7TD-GSUU] (last visited Jan. 9, 2016).

A. Issue

Data breaches are expensive: a recent study by the Ponemon Institute examined the cost of data breach remediation for 350 companies across 16 industries in 11 countries.[23] It concluded that the average cost of a data breach is $154 per personally identifiable record ("PIR").[24] Compared with other countries, breaches in the United States were the highest; the average cost across all industries was $217 per PIR.[25]

Similarly, the cause of the data breach impacts the cost of the respective breach. In the United States, across all industries, the average cost of a malicious or criminal breach is $230 per PIR.[26] Comparatively, the average cost due to system glitches is $142 per PIR, and the cost of human error or negligence is $137 per PIR.[27]

Healthcare data breaches are the most expensive to rectify, compared to data breaches in other industries.[28] Worldwide, the cost of a breach in the healthcare industry was $363 per PIR.[29] In the United States, the average cost of a data breach in the healthcare industry was $398 per PIR.[30]

---

[23] Joseph Conn, *Healthcare data breaches are costliest: study*, MODERN HEALTHCARE (May 28, 2015), http://www.modernhealthcare.com/article/20150528/NEWS/150529899 [https://perma.cc/N8SL-5SJQ].

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] Brian Prince, *Data Breach Costs Rise, Healthcare Industry Hardest Hit*, SECURITY WEEK (May 27, 2015), http://www.securityweek.com/data-breach-costs-rise-healthcare-industry-hardest-hit [https://perma.cc/9B95-C4FP].

[28] Conn, *supra* note 23.

[29] *Id.*

[30] *Id.* Because 80 million records were breached, the remediation cost of the Anthem breach could be as much as $32 billion.

Chris White, senior lead engineer of commercial data protection services at Booz Allen Hamilton, explained the variances as, "there is something inherent to the human condition that says health information is some of our most private information. The other piece is the damage that could be done with personal information."[31] Black market prices for medical records obtained in healthcare data breaches can run ten times higher than information stolen through data breaches in other industries.[32] The depth of information garnered from medical records accounts for the massive price gap.[33] Additionally, while financial data like credit cards can immediately be canceled, a patient often cannot immediately identify breached medical data; thus, hackers have years to utilize the records.[34]

A breach of medical data often causes greater harm in the future than in the present.[35] Further, victims are generally unable to sue for these future harms.[36] Additionally, potential financial harm is not always of utmost importance, as victims have the overwhelming task of monitoring their surroundings for the remainder of their natural lives.[37]

Industry leaders are beginning to understand that potential harm and anxiety of consumers have negative consequences for their businesses.[38] Further, common sense

---

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] Wong, *supra* note 2.

[35] Farai Chideya, *Data Theft Today Poses Indefinite Threat of "Future Harm"*, THE INTERCEPT (June 12, 2015, 12:26 PM), https://theintercept.com/2015/06/12/data-breach-threat-of-future-harm [https://perma.cc/TB3A-44LF].

[36] *Id. See also* Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138 (2013).

[37] Chideya, *supra* note 35.

[38] Beth D. Diamond, *Prepare for the inevitable: Post-data breach class actions*, BUS. INS. (Sept. 13, 2015, 12:01 AM), http://www.businessinsurance.com/article/20150913/ISSUE0401/3091

demands some recourse for victims whose literal identity is at risk as a result of cyber attack data breaches.

B. Roadmap

Recent events have highlighted the prevalence and resulting costs of data breaches in the healthcare industry. The magnitude of these breaches and costs has led to serious questions by experts and consumers alike. In an ever-changing healthcare and technology environment, the current security practices of relevant parties could and should be at the forefront of the investigations into these mass data breaches due to cyber attacks. This Note will address the current security landscape in the healthcare industry and how relevant parties can address any security shortfalls to prevent future data breaches due to cyber attacks.

First, this Note will provide background on the Health Insurance Portability and Accountability Act ("HIPAA"), examine the current regulations related to the HIPAA Security Rule, and outline the repercussions of a data breach under HIPAA. Next, this Note will examine how the current method addressing data breaches is insufficient. Then, the Note will examine alternatives to the current model, in hopes of providing justice to victims. Finally, the Note will conclude that enacting a private right of action regulation for HIPAA security violations will prove to be ultimately useful to both healthcare companies and patients by minimizing cyber attacks and thus decreasing costs as a result of these data breaches.[39]

39992/business-insurance-perspectives-preparation-for-post-data-breach?tags=%7C302%7C75%7C299 [https://perma.cc/6WDB-N7TG].

[39] The scope of this Note is limited to cyber attacks that result in HIPAA Security breaches. The magnitude of the Anthem breach

II. BACKGROUND

A. Health Insurance Portability and Accountability Act

1. HIPAA Background

HIPAA was enacted in 1996 with two main objectives.[40] The first objective, "Health Insurance Portability," aimed to ensure that individuals would be able to maintain their health insurance between jobs.[41] The second objective, "Accountability," aimed to ensure the security and confidentiality of patient data.[42] HIPAA gives the Secretary of the Department of Health and Human Services ("HHS") the authority to promulgate regulations consistent with the security and privacy requirements of HIPAA.[43] This Note

---

warrants an examination of the HIPAA Security Rule. However, while outside the scope of this Note, HIPAA Privacy breaches are also regularly occurring, and such breaches should not be dismissed. *See, e.g.*, Charles Ornstein & Annie Waldman, *Few Consequences For Health Privacy Law's Repeat Offenders*, PROPUBLICA (Dec. 29, 2015, 4:00 AM), https://www.propublica.org/article/few-consequences-for-health-privacy-law-repeat-offenders [https://perma.cc/TKX4-X23A]; Zen Chu & Maulik D. Majmudar, *What Apple's Standoff With the FBI Means for Your Medical Records*, FORTUNE (Mar. 3, 2016, 1:00 AM), http://fortune.com/2016/03/03/apple-tim-cook-fbi-2/ [https://perma.cc/48BB-75U3]; King & Spalding, *ALJ Upholds $239,800 In Civil Monetary Penalties For HIPAA Violations*, JD SUPRA BUS. ADVISOR (Feb. 19, 2016), http://www.jdsupra.com/legalnews/alj-upholds-239-800-in-civil-monetary-86126/ [https://perma.cc/HZF5-W2XX].

[40] *HIPAA Background*, U. CHI., 1, 1 (Oct. 23, 2006), http://hipaa.bsd.uchicago.edu/hipaa_background_20070122.pdf [https://perma.cc/86PY-AGTZ].

[41] *Id.*

[42] *Id.*

[43] 42 U.S.C. § 1302d-1 (2012).

focuses on the second objective, "Accountability," and specifically the regulations promulgated by HHS to maintain the security of patient health information.

However, HIPAA is not a standalone law. While HIPAA began the campaign to increase privacy and security of medical records, it was the Health Information Technology for Economic and Clinical Health ("HITECH") Act—passed as Title XIII of the American Recovery and Reinvestment Act of 2009—which focused on electronic medical records ("EMRs").[44] Among a variety of provisions, HITECH directed HHS to promulgate further regulations to expand and incentivize EMRs.[45] With the rapid expansion arose further privacy and security issues,[46] prompting HHS to roll out firmer regulations for "covered entities" and their "business associates."[47]

2. Definitions

a. Covered entity

Under HIPAA, a covered entity is: "(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form . . . ."[48] An entity that issues health insurance is considered a

---

[44] *See generally* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 226-79.

[45] *Id.*

[46] Conn, *supra* note 23.

[47] *HITECH Act Rulemaking and Implementation Update*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/security/guidance/HITECH-act-rulemakingimplementation-update/index.html [https://perma.cc/A7PG-PKDD] (last visited Feb. 13, 2016) [hereinafter *HITECH Act Rulemaking*].

[48] 45 C.F.R. § 160.103 (2013).

health plan under the covered entity provision.[49] A health insurance issuer is defined as "an insurance company, insurance service, or insurance organization . . . that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance."[50] Therefore, as a health insurance issuer, Anthem is a covered entity under HIPAA.

b. Business associate

Under HIPAA, a business associate ("BA") is a person who "creates, receives, maintains, or transmits" electronic protected health information ("ePHI") on behalf of a covered entity in the functions or activities set forth by HIPAA regulations.[51] Such functions include "claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and re-pricing."[52] A person can also be a BA if she provides certain services, including "legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial . . . " for a covered entity in which disclosure of ePHI is required.[53] Regardless of prescribed duties, a BA cannot be a member of the workforce of the covered entity; such a person is a member of the covered entity and must follow any HIPAA regulations that apply to covered entities.[54] However, as a result of the HITECH Act, BAs of covered entities must now

---

[49] *Id.*
[50] *Id. See also* 42 U.S.C. § 300gg-91(b)(2) (2012).
[51] 45 C.F.R. § 160.103.
[52] *Id.*
[53] *Id.*
[54] *Id.*

be HIPAA-compliant and face direct liability for breaches of ePHI.[55]

3. The Security Rule

The HIPAA Security Rule establishes federal standards in order to protect patients' ePHI that is "created, received, used, or maintained by a [HIPAA] covered entity."[56] The summary from the Federal Register regarding the applicable HIPAA Security Rule regulations states, "[t]he use of the security standards will improve the Medicare and Medicaid programs, and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information."[57]

Covered entities are required to:

> (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under [the HIPAA

[55] *HITECH Act Rulemaking*, *supra* note 47.

[56] *Health Information Privacy: The Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html [https://perma.cc/RA5R-RW2J] (last visited Jan. 9, 2016).

[57] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334, 8,334-35 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).

> Privacy Rule] . . . . (4) Ensure compliance with this subpart by its workforce.[58]

Presently, HHS allows flexibility under the HIPAA Security Rule.[59] This latitude allows covered entities to enact any security measure to "reasonably and appropriately implement" HIPAA statutory and regulatory requirements.[60] HHS does, however, mandate that covered entities consider the following factors:

> (i) The size, complexity, and capabilities of the covered entity . . . (ii) The covered entity's . . . technical infrastructure, hardware, and software security capabilities, (iii) The costs of security measures, [and] (iv) The probability and criticality of potential risks to electronic protected health information.[61]

Ultimately, the Security Rule requires a covered entity to take appropriate safeguards in order to "ensure the confidentiality, integrity, and security of electronic protected health information."[62]

The Security Rule safeguards are divided into three categories: administrative, physical and technical safeguards.[63] The various safeguards are subdivided into

---

[58] 45 C.F.R. § 164.306(a).

[59] *Id*. § 164.306(b)(1).

[60] *Id*.

[61] *Id.* § 164.306(b)(2). Opponents of stronger security regulations often argue that too much security is simply too costly. *Trotter*, supra note 20.

[62] *Health Information Privacy: The Security Rule*, *supra* note 56.

[63] *Id.*

implementation specifications.[64] Security implementation specifications are designated by HHS as either "required" or "addressable" specifications.[65] "Required" specifications must be implemented by the covered entity.[66] "Addressable" specifications must be implemented when the covered entity determines that the specification is "a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution" to protect ePHI.[67] If the implementation is "reasonable and appropriate," the covered entity must implement the specification.[68] However, if the implementation is neither reasonable nor appropriate, the covered entity must document the rationale for this determination, as well as implement any other equivalent policy that is similarly deemed "reasonable and appropriate."[69]

Mere establishment of security polices is insufficient for HIPAA compliance. Covered entities must regularly review and modify their security measures in order to "continue provision of reasonable and appropriate protection" of ePHI.[70]

4. Relevant Safeguards

Before the Anthem and other similar breaches can be understood fully, and before appropriate pre-breach and post-breach solutions can be examined, the specific safeguards of the HIPAA Security Rule must be assessed.

---

[64] *See* 45 C.F.R. § 164.306(d)(1).

[65] *See id. See also* 45 C.F.R. § 164 app. A to subpt. C ("Security Standards: Matrix").

[66] 45 C.F.R. § 164.306(d)(2).

[67] *Id.* § 164.306(d)(3)(i).

[68] *Id.* § 164.306(d)(3)(ii)(A).

[69] *Id.* § 164.306(d)(3)(ii)(B).

[70] *Id.* § 164.306(e).

a. Administrative safeguards

HHS defines administrative safeguards as, "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."[71] The administrative safeguards encompass over half of the Security Rule requirements.[72] The administrative safeguards require a covered entity to examine the current administrative policies in place for protecting patients' ePHI, to conduct a comprehensive risk analysis of those current policies, and to complete documentation on how the policies comply with the "required" and "addressable" administrative safeguards.[73]

There are several HIPAA administrative safeguards relevant to cyber attacks that covered entities must consider when implementing security policies. One standard is to establish a security management process, in which the covered entity must "implement policies and procedures to prevent, detect, contain, and correct security violations."[74] To satisfy this standard, the covered entity, through the security polices, is required to include risk analysis, risk management, a sanction policy, and a process to review all information system activity.[75]

---

[71] *Id.* § 164.304.

[72] *Security Standards: Administrative Safeguards*, U.S. DEP'T OF HEALTH & HUM. SERVS., 1, 2-3 (Mar. 2007), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf [https://perma.cc/P7RB-9ZD4].

[73] *Id.*

[74] Administrative Safeguards, 45 C.F.R. § 164.308(a)(1)(i) (2017).

[75] *Id.*

A second relevant administrative safeguard standard requires covered entities to appoint a designated Security Official, who is responsible for the "development and implementation of the policies and procedures" mandated by the Security Rule.[76] This individual retains the responsibility of implementing and continuously examining the covered entity's security policies in order to keep the entity HIPAA-compliant.[77] This position is analogous to the Privacy Official mandated by the HIPAA Privacy Rule.[78]

A third relevant administrative safeguard standard requires the covered entity to consider security as it relates to their workforce. A covered entity must implement policies and procedures to ensure that members required to have access to ePHI have access, and similarly to prevent access by those who should not have access.[79] All of the required implantation specifications, which include authorization and supervision, clearance procedures termination procedures, are "addressable."[80]

A fourth relevant administrative safeguard standard pertains to management of information access. Covered

---

[76] *Id.* § 164.308(a)(2).

[77] *Security Standards: Administrative Safeguards*, *supra* note 72. Critics of HIPAA regularly argue that compliance is prohibitively expensive, in part because the regulations mandate a Security Officer. KEVIN BEAVER & REBECCA HEROLD, THE PRACTICAL GUIDE TO HIPAA PRIVACY AND SECURITY COMPLIANCE, 32-3 (2003). (noting that the estimated range is $30,000 to $300,000. *Id.* Many owners and managers see HIPAA compliance as an unnecessary business expense affecting the bottom-line. *Id.* To remain compliant while limited business expenses, small covered entities should designate their office manager to handle HIPAA compliance, medium-sized covered entities should designate a HIPAA Officer to handle both privacy and security, and large covered entities should hire two separate positions, the Privacy Officer and Security Officer, respectively). *Id.*

[78] *Security Standards: Administrative Safeguards*, *supra* note 72.

[79] 45 C.F.R. § 164.308(a)(3)(i).

[80] *Id.* § 164.308(a)(3)(ii).

entities must implement policies and procedures for authorizing access to ePHI that comply with the HIPAA Privacy Rule.[81] Covered entitles must isolate health care clearinghouse functions from all other healthcare organization functions.[82] Covered entities must likewise address authorization, establishment, and modification of access to systems containing ePHI.[83]

A fifth relevant administrative safeguard standard requires covered entities to implement a program for security awareness and training for all members of its workforce, including management.[84] "Addressable" implementation specifications include security reminders, malicious software protection, monitoring of login activity, and password management.[85]

A sixth relevant administrative safeguard standard requires covered entities to implement policies and procedures to address security incidents when they occur.[86] The security response and subsequent manner of security incident reporting are "addressable" specifications.[87]

A seventh relevant administrative safeguard standard requires a security contingency plan, in which covered entities must create policies and procedures for responding to an emergency that damages systems that contain electronic PHI.[88] Plans for data backup, disaster recovery, and emergency operation are "required" specifications.[89] Two "addressable" specifications include procedures for

[81] *Id.* § 164.308(a)(4)(i).
[82] *Id.* § 164.308(a)(4)(ii)(A).
[83] *Id.* § 164.308(a)(4)(ii).
[84] *Id.* § 164.308(a)(5)(i).
[85] *Id.* § 164.308(a)(5)(ii).
[86] *Id.* § 164.308(a)(6)(i).
[87] *Id.* § 164.308(a)(6)(ii).
[88] *Id*. § 164.308(a)(7)(i).
[89] *Id.* § 164.308(a)(7)(ii).

testing and revision, as well as analysis of "applications and data criticality."[90]

An eighth relevant administrative safeguard standard of requires "technical and nontechnical evaluation" of the covered entity's systems.[91] The periodic evaluation must consider the existing security polices of the covered entity, changes to those policies and procedures, as well as present environmental or operational changes that potentially affect the security of ePHI.[92]

b. Physical safeguards

HHS defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."[93] These requirements require the Security Official to consider all of the actual and potential physical access points to patients' ePHI.[94]

There are several HIPAA physical safeguards relevant to cyber attacks that covered entities must consider when implementing security policies. One standard is to control ePHI facility access.[95] Covered entities must limit physical access to its electronic information systems to those with authorized access.[96] Covered entities must address

---

[90] *Id.*

[91] *Id.* § 164.308(a)(8).

[92] *Id.*

[93] *Id.* § 164.304.

[94] *Security Standards: Physical Safeguards*, U.S. DEP'T OF HEALTH & HUM. SERVS., 1, 2 (Mar. 2007), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf [https://perma.cc/X37W-6KND].

[95] 45 C.F.R. § 164.310(a)(1).

[96] *Id.*

contingency operations, facility security plan, access control and validation procedures, and maintenance records.[97]

A second relevant physical safeguard standard requires covered entities to establish policies for proper workstation use.[98] The covered entity must implement appropriate policies and procedures that detail the "proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation" in which ePHI can be accessed.[99]

A third relevant physical safeguard standard requires covered entities to establish policies for workstation security.[100] All workstations that access ePHI must have appropriate security measures to allow access only to authorized users."[101]

A fourth relevant physical safeguard standard requires covered entities to control devices and media at the facility.[102] Covered entities must establish policies and procedures that control the delivery and removal of hardware and media that contain ePHI into and out of the facility, as well as the transport of these devices within the facility.[103] The policies and procedures are required to cover disposal and re-use.[104] Accountability for hardware transfer, as well as data backup and storage of devices and media, are specifications that must be addressed.[105]

---

[97] *Id.* § 164.310(a)(2).
[98] *Id.* § 164.310(b).
[99] *Id.*
[100] *Id.* § 164.310(c).
[101] *Id.*
[102] *Id.* § 164.310(d).
[103] *Id.* § 164.310(d)(1).
[104] *Id.* § 164.310(d)(2).
[105] *Id.*

c. Technical safeguards

HHS defines technical safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."[106] The technical safeguards exceedingly reflect the Security Rule's flexibility and scalability.[107] Covered entities are not mandated to use any specific technology; rather, the task for determining HIPAA-compliant status rests with the covered entity.[108] The Security Official is charged with "reasonably and appropriately" implementing the standards and specifications of the technical safeguards.[109] While HHS has provided guidance in this area, the Secretary stresses that any provided examples are mere illustrations of compliance with the technical safeguards.[110] However, one thing remains all-but-certain: as technology becomes increasingly complex, HIPAA technical safeguards become increasingly more important.[111]

There are several HIPAA technical safeguards relevant to cyber attacks that covered entities must consider when implementing security policies. One standard is to establish an access control policy, in which the covered entity must "implement technical policies and procedures for electronic information systems" that support ePHI in order to restrict access to authorized "persons or software programs that have been granted access rights" by the covered entity.[112] The

---

[106] *Id.* § 164.304.

[107] *Security Standards: Technical Safeguards*, U.S. DEP'T OF HEALTH & HUM. SERVS., 1, 2-3 (Mar. 2007), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf [https://perma.cc/KD9K-U2D3].

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] 45 C.F.R. § 164.312(a)(1).

covered entity is required to establish unique user identification and emergency access procedures for authorized users.[113] Automatic logoff functionality and encryption-decryption programs are "addressable" specifications.[114]

A second relevant technical safeguard standard requires the implementation of audit controls for the covered entity's information systems.[115] Specifically, covered entities must install hardware, software, and related procedural mechanisms to record and assess activity in the systems that maintain ePHI.[116]

A third relevant technical safeguard standard recognizes the importance of data integrity, in which covered entities must implement policies and procedures to safeguard ePHI from "improper alteration or destruction."[117] Specifically, the covered entity must examine if mechanisms to authenticate the alteration or destruction of ePHI reasonable and appropriate for the present information systems.[118]

A fourth relevant technical safeguard standard requires policies and procedures for the authentication of a person or entity.[119] In order to gain authorized access to ePHI systems, the person or entity must be verified to be the actual person or entity to prevent unauthorized access.[120]

A fifth relevant technical safeguard standard requires security in the transmission of ePHI; covered entities must implement measures to protect against unauthorized access to ePHI "transmitted over an electronic communications

---

[113] *Id.* § 164.312(a)(2).
[114] *Id.*
[115] *Id.* § 164.312(b).
[116] *Id.*
[117] *Id.* § 164.312(c)(1).
[118] *Id.* § 164.312(c)(2).
[119] *Id.* § 164.312(d).
[120] *Id.*

network."[121] Integrity controls and data encryption are "addressable" specifications.[122]

5. HIPAA Breach Notification

The requirements for breach notification have evolved since HIPAA was first enacted.[123] The most recent regulations were developed and promulgated by the HHS's Office of Civil Rights ("OCR") in 2013.[124] According to the final rule, a security breach is now defined as "an acquisition, access, use, or disclosure of protected health information in a manner not permitted . . . [and] is presumed to be a breach, unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised."[125] HHS has ruled, "breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that PHI has been compromised."[126]

HHS has further detailed the notice requirements to individuals after a data breach. A covered entity must provide notice to each individual whose unsecured ePHI has actually been breached.[127] Further, the covered entity must also notify any individuals whose ePHI it reasonably believes was breached.[128] The notice must be provided

---

[121] *Id.* § 164.312(e)(1).

[122] *Id.* § 164.312(e)(2).

[123] *HIPAA Rule Brings Changes to Breach Notification*, MARSH & MCLENNAN COMPANIES, 1 (Feb. 2013), http://www.ucop.edu/risk-services/_files/hipaa-final-rule-022013.pdf, [http://perma.cc/HKK3-RNBJ].

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] 45 C.F.R. § 164.404(a)(1) (2009).

[128] *Id.*

"without unreasonable delay" and not more than 60 calendar days after the data breach was discovered.[129] For the benefit of the individual, all breach notices must be written in plain language.[130] Further, specific detailed information must be communicated in the breach notification.[131]

Breach notification requirements were strengthened by the HITECH Act.[132] When a breach of unsecured PHI involves 500 or greater individuals, the breach is posted by OCR on the online, publically-accessible "Wall of Shame."[133] From October 2009 through February 2016,

---

[129] *Id.* § 164.404(b).

[130] *Id.* § 164.404(c)(2).

[131] *Id.* § 164.404(c)(1).

> (''(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) Any steps individuals should take to protect themselves from potential harm resulting from the breach; (D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (E) Contact procedures for individuals to ask questions or learn additional information, which shall include a tollfree telephone number, an e-mail address, Web site, or postal address.").

[132] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. DEP'T HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [https://perma.cc/KRY5-DKYD] (last visited Feb. 12, 2016) [hereinafter *Breach Portal*].

[133] *Id.* The term "Wall of Shame" is used colloquially by industry experts. *See, e.g.,* Lucas Mearian, '*Wall of Shame' exposes 21M medical record breaches*, COMPUTER WORLD (Aug. 7, 2012, 7:00 AM), http://www.computerworld.com/article/2505546/data-security/-wall-of-

more than 1400 covered entities and business associates found themselves on the OCR's "Wall of Shame."[134]

6. HIPAA Violations

In 2005, the United States Department of Justice clarified the criminal charges for violating HIPAA.[135] An individual who knowingly violates HIPAA may be held criminally liable.[136] The penalty is a fine of up to $50,000 and up to one year in prison.[137] If the offense was committed under false pretenses, the penalty increases to a fine of up to $100,000 and imprisonment up to five years.[138] If the offender committed the violation with the intent to "sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm," the penalties further increase to fines up to $250,000 and up to ten years in prison.[139]

If HHS determines that a covered entity or BA violated a HIPAA regulation, the OCR will impose money damages

---

shame--exposes-21m-medical-record-breaches.html [https://perma.cc/EK2K-BLSH]; William Maruca, *A Peek Behind the OCR Wall of Shame*, FOX ROTHSCHILD LLP (July 17, 2012), http://hipaahealthlaw.foxrothschild.com/2012/07/articles/hipaa-enforcement/a-peek-behind-the-ocr-wall-of-shame/ [https://perma.cc/YZL2-V547].

[134] *Breach Portal*, *supra* note 132.

[135] George F. Indest III, *Failure to Comply With HIPAA Can Result in Both Civil and Criminal Penalties*, THE HEALTH L. FIRM (Nov. 11, 2014), http://www.thehealthlawfirm.com/blog/posts/failure-to-comply-with-hipaa-can-result-in-both-civil-and-criminal-penalties.html [https://perma.cc/E3VL-2YAX].

[136] 42 U.S.C. § 1320d-6 (2012).

[137] Indest, *supra* note 135.

[138] *Id.*

[139] *Id.*

on the covered entity or BA.[140] Penalties range from $100 per violation to an annual maximum of $1.5 million, depending on the severity of the breach, reasonableness, and post-breach corrective action.[141] Furthermore, a covered entity is liable for money damages in accordance with the common law principle of agency for a HIPAA violation by any entity, including a BA, acting within the scope of the agency.[142] Similarly, a BA is liable for money damages in accordance with the common law principle of agency for a HIPAA violation by any entity, including a subcontractor, acting within the scope of the agency.[143] The civil money penalty for a HIPAA violation depends on the type and severity of violation and the actions taken to remediate the violation.[144] Importantly, a penalty imposed by OCR does not exclude "any other penalty prescribed by law."[145] Since the introduction of the HITECH Act, states' attorneys general may bring civil action in federal courts against covered entities or BAs who violate HIPAA and expose ePHI of citizens of the respective state.[146]

---

[140] 45 C.F.R. § 160.402(a) (2013). *See also What are the Penalties for HIPAA Violations?*, HIPAA J. (Jun. 24, 2015), http://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ [https://perma.cc/CW8F-9QN7] [hereinafter *What are the Penalties?*].

[141] Indest, *supra* note 135.

[142] 45 C.F.R. § 160.402(c)(1) (2013).

[143] *Id.* § 160.402(c)(2).

[144] *See generally* 45 C.F.R. § 160.404 (2016); *see also* 45 C.F.R. § 160.408 (2013).

[145] 45 C.F.R. § 160.418 (2013).

[146] *What are the Penalties?*, *supra* note 140.

B. Recourse for Data Breach Victims

1. OCR Complaint

While penalties have continually increased for covered entities that suffer breaches, the remedies available to an individual patient, whose ePHI was breached, are very limited. OCR complaints are the most commonly-used remedy, and anyone who believes that a covered entity or BA has violated any portion of HIPAA may file a complaint with OCR.[147] Specifically, the complaint must be filed in writing within 180 days of when the complainant "knew or should have known" of the HIPAA violation.[148] The complaint must provide the name of the covered entity and describe the alleged violation of the subject of the complaint.[149] After a complaint is correctly filed, OCR will review any submission "when a preliminary review of the facts indicates a possible violation due to willful neglect."[150]

2. No Private Right of Action

The text of HIPAA does not explicitly confer a private right of action to a victim of a HIPAA violation.[151] Further, many courts have declined to create an implied private right of action following a HIPAA violation.[152]

---

[147] 45 C.F.R. § 160.306(a) (2013); *see also Health Information Privacy: How to File a Complaint*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html [https://perma.cc/8QGD-C5NZ] (last visited Feb. 8, 2017).

[148] 45 C.F.R. § 160.306(b) (2013).

[149] *Id.*

[150] *Id.* § 160.306(c)(1) (2013).

[151] *See* 42 U.S.C. § 1320d-6 (2012); *see* 45 C.F.R. §§ 160, 164 (2013).

[152] Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 41 (Conn. 2014). *See also* Agee v. U.S., 72 Fed. Cl. 284 (2006);

In *Acara v. Banks*, the court neatly detailed its rationale for declining to extend a private right of action to an individual as the victim of a HIPAA violation.[153] The underlying rationale was that Congress must create "private rights of action to enforce federal law[s]."[154] The *Banks* court correctly observed, "HIPAA has no express provision creating a private cause of action. . . ."[155] Thus, plaintiffs asserting the existence of such a claim have a very heavy burden to prove an implied right of action in a federal statute.[156] The text of HIPAA "focuses on regulating persons that have access to individually identifiable medical information and who conduct certain electronic health care transactions."[157] The text explicitly limits enforcement of HIPAA to HHS.[158] As the *Acara* court importantly notes, "[b]ecause HIPAA specifically delegates enforcement, there is a strong indication that Congress intended to preclude private enforcement."[159] HHS has not yet promulgated regulations that establish a private right of action.[160]

Walker v. Gerald, No. 05-6649, 2006 U.S. Dist. LEXIS 43677, 2006 WL 1997635 (E.D. La. June 27, 2006); Poli v. Mountain Valley's Health Ctrs., Inc., No. 2:05-2015-GEB-KJM, 2006 U.S. Dist. LEXIS 2559, 2006 WL 83378 (E.D. Cal. Jan. 11, 2006); Cassidy v. Nicolo, No. 03-CV-6603-CJS, 2005 U.S. Dist. LEXIS 34160, 2005 WL 3334523 (W.D.N.Y. Dec. 7, 2005); Johnson v. Quander, 370 F. Supp. 2d 79 (D.D.C. 2005); Univ. of Colo. Hosp. Auth., 340 F. Supp. 2d 1142 (D. Colo. 2004); O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176 (D. Wyo. 2001); Means v. Ind. Life & Accident Ins. Co., 963 F. Supp. 1131 (M.D. Ala. 1997); Wright v. Combined Ins. Co. of Am., 959 F. Supp. 356 (N.D. Miss. 1997).

[153] Acara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006).

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *Id.*

[160] *See* 45 C.F.R. §§ 160, 164 (2013).

Indiana courts have likewise declined to create a private right of action for a HIPAA violation.[161] In *Walgreens*, the court expressly wrote that HIPAA did not create a private right of action by citing a 7th Circuit case quoting *Acara*.[162]

3. Future Harms of Victims

Companies affected by data breaches may suffer in the short-term from a public relations standpoint.[163] However, the date breach victims often suffer the greater future harm.[164] Because no cause of action for the victims of these data breaches exists, individuals are generally unable to sue the covered entities for these future harms.[165] Further, these future harms are often difficult to prove because they may manifest years, and even decades, into the future.[166] Victims of ePHI data breaches must often be on guard for the rest of their lives, as they often cannot immediately identify which specific medical data have been breached.[167] Most frightening, many are forced to endure the "digital-era equivalent of constantly looking over their shoulder."[168]

---

[161] Canty v. Walgreens Co., No. 2:11-CV-232-JVB, 2012 U.S. Dist. LEXIS 44405, at *6-7 (N.D. Ind. Mar. 28, 2012).

[162] *Id.*; *see also* Carpenter v. Phillips, 419 Fed. Appx. 658, 659 (7th Cir. 2011).

[163] *See* Chideya, *supra* note 35.

[164] *Id.*

[165] *Id.*; *see also* Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138, 1155 (2013).

[166] Chideya, *supra* note 35.

[167] Wong, *supra* note 2.

[168] Chideya, *supra* note 35.

III. ANALYSIS

A. Examining Changes to the Current System

1. HIPAA and the Negligence Standard of Care

In *Byrne v. Avery Center for Obstetrics & Gynecology*, the plaintiff-patient sued for breach of contract, negligence of releasing her medical file without authorization, negligent misrepresentation of Avery Center's privacy policy, and negligent infliction of emotional distress.[169] The Supreme Court of Connecticut expressly denied that HIPAA entitled an aggrieved patient a private right of action for a breach.[170] However, the Connecticut court examined whether HIPAA could be used as the basis for the standard of care to which Avery Center allegedly owed Byrne.[171] The court examined cases from other jurisdictions which "utilize[d] HIPAA as [a] 'guidepost for determining the standard of care.'"[172] The *Byrne* court held that HIPAA could be used when determining the standard of care for the plaintiff's claims of negligence and negligent infliction of emotional distress.[173] Many state courts have followed similar reasoning to *Byrne* by declining a private right of action but allowing HIPAA to be used to determine the standard of care in common law tort cases.[174]

---

[169] Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 35-37 (Conn. 2014).

[170] *Id.* at 45.

[171] *Id.* at 45-49.

[172] *Id.* at 47-48 (quoting Fanean v. Rite Aid Corp. of Del., Inc., 984 A.2d 812, 823 (Del. Super. Ct. 2009)).

[173] Byrne, 102 A.3d at 49.

[174] *See* Fanean, 984 A.2d at 823 (concluding that claim of negligence per se could not be based on HIPAA violation, but holding that a common law negligence claim could utilize HIPAA as a "guidepost for determining the standard of care"); Young v. Carran, 289 S.W.3d 586,

2. Burden Shifting to the Covered Entity

Akin to the plaintiff in *Byrne*, most plaintiffs bear the burden of proof in a medical negligence case.[175] In the case of an ePHI breach, the plaintiff would be forced to show, by a preponderance of the evidence, that the covered entity was negligent in their data-keeping practices.[176] However, common sense shows that the covered entity is in complete control of all of the evidence, and the patient has very limited access to their ePHI.[177]

The glaring issue is that, in nearly every state with medical record ownership laws, the provider and/or physician own their patients' medical records.[178] As of 2015,

---

588-89 (Ky. Ct. App. 2008) (rejecting HIPPA as the basis for damages claim under state negligence per se statute, but noting that the state's case law permits use of federal statutes to inform the standard of care analysis in common law negligence claims); R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 715, 722-24 (W. Va. 2012) (concluding that HIPAA did not preempt state law claims for negligence, outrageous conduct, and invasion of privacy, and that the remedies in HIPAA and the common law claims converge to "protect the privacy of an individual's health care information" (quoting Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 49 (Minn. Ct. App. 2009))).

[175] *See, e.g.*, Sweeney v. Erving, 228 U.S. 233, 237-42 (1913).

[176] *See, e.g.*, *id.*; *see also* Byrne, 102 A.3d at 38.

[177] *See generally* 45 C.F.R. § 164.524 (2014). Regulations promulgated after the HITECH Act gave patients the right to request access to their medical records. *See generally id.* However, some exceptions do exist, including in the case of psychotherapy notes. *Id.* § 164.524(a)(1)(i). Covered entities must provide the records in a reasonable time and manner. *Id.* § 164.524(c)(3). However, they are allowed to also charge a reasonable fee for time and expenses spent compiling and sending the record to the requesting individual. *Id.* § 164.524(c)(4).

[178] *Who Owns Medical Records: 50 State Comparison*, HEALTH INFO. & THE L., http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison [https://perma.cc/F26T-2AZA] (last updated Aug. 20, 2015).

twenty-one states have codified this policy.[179] In several other states, including Michigan and Illinois, the state supreme courts have ruled similarly for providers.[180] Only in New Hampshire do patients own their medical record.[181] In Indiana, the provider is the owner of the original health record.[182]

One logical proposal is to return ownership of the medical record to the patient. Some physicians believe, for the best interest of the patient, that the patient should own the medical record.[183] In the absence of perfect communication between all of a patient's treating physicians in all specialties, the only person who is aware of the patient's entire medical history is the patient herself.[184] Further, a recent study by Dr. Jonathan Pell, assistant professor at University of Colorado in Denver, found that patients, physicians, and nursing staff all benefited when patients had greater access to their medical record.[185]

Even if patients own their medical records, it makes most sense for providers to keep and maintain the records.[186] In an era of EMRs, providers have the technology necessary to house the records.[187] If patients owned their medical records

---

[179] *Id.*

[180] *See id.*

[181] *Id.*

[182] *Id.*; *see also* IND. CODE § 16-39-5-3 (2016).

[183] Neil Chesanow, *Who Should Own a Medical Record -- The Doctor or the Patient?* MEDSCAPE (Jan. 13, 2015), http://www.medscape.com/viewarticle/837393 [https://perma.cc/56JY-WTGZ].

[184] *See id.*

[185] Lisa Rapaport, *New Study Suggests Patients Should Have Access To Their Own Medical Records*, HUFFINGTON POST (March 9, 2015, 11:00 AM), http://www.huffingtonpost.com/2015/03/09/patients-medical-records_n_6831350.html [https://perma.cc/RMP7-KYLR] (last updated May 9, 2015).

[186] *See* Chesanow, *supra* note 183.

[187] Chesanow, *supra* note 183.

but providers stored and maintained them, a bailment would exist. A bailment is formed "by the delivery of personal property by one person to another in trust for a specific purpose, pursuant to an express or implied contract to fulfill that trust."[188] Further, "[i]nherent in the bailment relationship is the requirement that the property be returned to the bailor, or duly accounted for by the bailee, when the purpose of the bailment is accomplished, or that it be kept until it is reclaimed by the bailor."[189] In Indiana, where a bailment for mutual benefit exists, the bailee (the covered entity) owes the bailor (the patient) the duty of "ordinary care" and would be held liable if "ordinary care" was not exercised.[190]

In the present discussion, a covered entity would retain possession of the patient's medical records while the patient had a relationship with the covered entity. While in possession of a patient's medical records, the covered entity would owe the patient a duty of ordinary care. As many state courts have done in the past for other negligence claims, HIPAA regulations would inform the standard of care of the bailee. If the patient was treated by a new physician or provider, she could take her medical records with her, with little-to-no cost and effort.

The patient-focused bailment relationship would entail a burden-shifting mechanism in the case of a data breach.[191] While the plaintiff retains the ultimate burden of persuasion,

---

[188] 8A AM. JUR. 2D *Bailments* § 1 (2016).

[189] *Id.*

[190] *See* Plant v. Howard Johnson's Motor Lodge, 500 N.E.2d 1271, 1273-74 (Ind. Ct. App. 1986), *trans. denied* 514 N.E.2d 1048 (Ind. 1987).

[191] RAY ANDREWS BROWN, THE LAW OF PERSONAL PROPERTY, § 11.8, 289-93 (W.B. Raushenbusch ed., 3d ed. 1975), *reprinted in* SHELDON F. KURTZ ET AL., CASES AND MATERIALS ON AMERICAN PROPERTY LAW, 183-84 (6th ed. 2012).

after a prima facie case of negligence has been established, the defendant must to produce evidence showing ordinary care was indeed taken.[192] If the defendant is unable to produce sufficient evidence, the trier of fact should rule for the plaintiff.[193] The public policy rationale for this burden-shifting rests in the fact that the bailee, at the time of breach, exercises sole control over the bailor's property.[194] The bailor is unlikely to have any evidence to prove any alleged wrongdoing by the bailee, erasing any chance of recovery for the wronged party.[195] Here, the patient is unlikely to have any evidence to show that a covered entity negligently maintained electronic medical records, so public policy favors the burden-shifting scheme.

3. The "Actual Harm" Issue

In a case of alleged negligence, the aggrieved party must prove he "in fact suffered harm of a kind legally compensable by damages."[196] However, in the case of an ePHI breach, the actual harm may be suffered in the future, years or even decades after the breach.[197] Further, the proximate causal link between the breach and the potential harm to one's identity years later also presents unique challenges.[198] These considerations exemplify where the tort approach for data breaches falls short; even though one's data may never be used in a negative manner, the fear of future harm should be equally considered an actual harm.[199]

---

[192] *Id.*
[193] *See id.*
[194] *See id.*
[195] *See id.*
[196] RESTATEMENT (SECOND) OF TORTS § 328A (1965).
[197] *See* Chideya, *supra* note 35.
[198] *See* RESTATEMENT (SECOND) OF TORTS § 328A (1965).
[199] *See* Chideya, *supra* note 35.

B. Expanding HIPAA Regulations

Relying on a tort liability model presents evidentiary challenges. An alternative would be to institute regulatory recovery for victims of data breaches. Presently, most of HIPAA penalties are regulations promulgated by HHS.[200] However, HHS is not the only administrative entity which has a stake in data security.

1. Authority of the Federal Government to Regulate Cyber Security

While *FTC v. Wyndham Worldwide* is not a healthcare case, the holding is very relevant to healthcare data breaches.[201] In *Wyndham Worldwide*, the Federal Trade Commission ("FTC") claimed that Wyndham's data security practices were both unfair and deceptive, causing substantial consumer injury.[202] The Third Circuit upheld the district court's ruling that the FTC could use the "prohibition on unfair practices" section of the FTC Act to challenge alleged lapses in data security.[203]

Broadly, the FTC was established to eliminate "unfair methods of competition in commerce."[204] Later amendments added a prohibition on "unfair or deceptive acts or practices

---

[200] *See generally* 45 C.F.R. § 160.400 (2013).

[201] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

[202] Bryan Fung, *The FTC Was Built 100 Years Ago to Fight Monopolists. Now, It's Washington's Most Powerful Technology Cop.*, WASH. POST (Sept. 25, 2014). https://www.washingtonpost.com/news/the-switch/wp/2014/09/25/the-ftc-was-built-100-years-ago-to-fight-monopolists-now-its-washingtons-most-powerful-technology-cop [https://perma.cc/CFS5-JC3G].

[203] Wyndham Worldwide, 799 F.3d at 249.

[204] *Id.* at 243 (citing 15 U.S.C. § 45 (a)).

in or affecting commerce."[205] The FTC created a three-prong test to determine if a practice was unlawful:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; and (3) whether it causes substantial injury to consumers (or competitors or other businessmen).[206]

Further, the court in *FTC v. Sperry* held the FTC could deem a practice unfair based on the third prong—substantial consumer injury—without finding that at least one of the other two prongs was also satisfied.[207] Ed Felten, current Princeton University professor and the FTC's first chief technologist, remarked, "[t]he FTC has established a principle that companies have a responsibility to protect consumers' private data."[208]

Ultimately, the *Wyndham Worldwide* decision strengthens the federal regulatory power of the FTC.[209] Subpar security practices that lead to breaches of consumer data are thus deemed to be both unfair and deceptive business practices that cause substantial consumer injury.

---

[205] *Id.*

[206] *Id.*; *see also* 15 U.S.C. § 45(n) (2012).

[207] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); *see also* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 n.5 (1972).

[208] Fung, *supra* note 202.

[209] *See* Wyndham Worldwide, 799 F.3d at 240.

Therefore, it follows that *Wyndham Worldwide* also gives the FTC the authority to regulate the security practices of covered entities in order to prevent data breaches of the consumer-patients' ePHI.

However, recent developments potentially curb FTC's authority to regulate in this area. In 2013, the FTC brought a formal complaint against clinical testing laboratory LabMD for failing to "provide 'reasonable and appropriate' security for personal information maintained on LabMD's computer networks" following two security incidents.[210] The FTC claimed that LabMD's conduct "caused or is likely to cause 'substantial consumer injury,'" and therefore LabMD engaged in "unfair acts or practices" in violation of the FTC Act.[211] In these actions, FTC has the burden of proving the "substantial consumer injury."[212] In a November 2015 ruling, the administrative law judge in *LabMD* ruled that the Commission had not met that burden because "[p]roof of likely substantial consumer injury . . . requires proof of something more than an unspecified and hypothetical 'risk' of future harm."[213] Commentators predict *LabMD* will have a "profound effect" on future FTC actions, because the ruling's interpretation of "substantial consumer injury" will alter the Commission's case selection going forward.[214] Given this ruling, the FTC's attempts to regulate companies' soft security practices appear to be merely suggestions of "best practices" rather than "some sort of 'common law'"

---

[210] LabMD, Inc., 2015 FTC LEXIS 272, at *1 (F.T.C. Nov. 13, 2015).

[211] *Id.* at *1 (internal quotations omitted).

[212] *Id.* at *200.

[213] *Id.*

[214] Teri Robinson, *Administrative Judge Dismisses FTC Case Against LabMD*, SC MAG. (Nov. 17, 2015), http://www.scmagazine.com/dismissed-labmd-case-could-impact-ftc-authority/article/454278/ [https://perma.cc/2K2W-QZJJ].

developed by the FTC to reign in unfair business practices.[215]

2. Strengthening HIPAA Regulations – Data Encryption

If the FTC cannot sufficiently regulate data breaches under the current laws, perhaps HHS should strengthen the existing HIPAA Security Rule regulations. A prevailing misconception is that physical security is the most important form of security.[216] However, while limiting the theft of the physical computers and other hardware is important for both ePHI security and privacy, another layer of protection is available to protect patient data at all times, in all locations—encryption.[217]

Presently, data encryption is an "addressable" specification.[218] Many in the security industry recommend encrypting data both "at rest" and "in motion."[219] While not required, some argue that encryption of ePHI is always

---

[215] Alan L. Friel & Gerald J. Ferguson, *LabMD and Wyndham Decisions Curtail FTC's Data Privacy and Security Reach*, DATA PRIVACY MONITOR (Jan. 5, 2016), http://www.dataprivacymonitor.com/hipaahitech/labmd-and-wyndham-decisions-curtail-ftcs-data-privacy-and-security-reach/ [https://perma.cc/SG42-G7SU].

[216] Derrick Wlodarz, *5 Big Myths Surrounding Computer Security and HIPAA Compliance*, BETANEWS (Sept. 2, 2013), http://betanews.com/2013/09/02/5-big-myths-surrounding-computer-security-and-hipaa-compliance/ [http://perma.cc/ND6Z-UQS5].

[217] *Id.*

[218] 45 C.F.R. § 164.312(a)(2) (2013).

[219] Gilad Parann-Nissany, *HIPAA and Encryption Lower the Cost of Healthcare*, ELECTRONIC HEALTH REP. (Aug. 4, 2015), http://electronichealthreporter.com/hipaa-and-encryption-lower-the-cost-of-healthcare/ [https://perma.cc/KY5Z-ZPPR].

"reasonable and appropriate."[220] An HHS guidance publication recommended data encryption as a best practice.[221] In fact, HHS also provides a safe harbor for covered entities who suffer a loss of encrypted data.[222] Gilad Parann-Nissany, founder and CEO of Porticor Cloud Security, asserts "[b]y using accepted HIPAA encryption techniques, companies can mitigate risks and reduce their exposure to costly data breaches, thereby reducing the cost of healthcare."[223] HIPAA aims to reduce healthcare costs by, among other things, increasing security of ePHI.[224] If industry experts believe that encryption will increase security and reduce costs, encryption should be converted from an "addressable" specification to a "required" specification.

Data encryption would increase data protection in the event of a breach. However, the rate at which companies worldwide face cyber attacks was enough for one company director to conclude that data breaches are a "statistical certainty."[225] If breaches of ePHI are inevitable, incentives for covered entities to follow security regulations are understandably diminished.[226] If pressure from victims or potential victims was strong enough (i.e. expensive enough),

---

[220] *Id.*; *see also* Donald F. Lee III, *Is Encryption Required by HIPAA? Yes.*, ALGONQUIN STUDIOS BLOG (June 19, 2013), http://blog.algonquinstudios.com/2013/06/19/is-encryption-required-by-hipaa-yes/ [https://perma.cc/6D7U-U65J].

[221] 74 Fed. Reg. 19006-10 (Apr. 27, 2009).

[222] *Id.*

[223] Parann-Nissany, *supra* note 219.

[224] 42 U.S.C. § 1320d-1(b) (2012).

[225] Jaikumar Vijayan, *90% of Companies Say They've Been Hacked: Survey*, COMPUTER WORLD (June 22, 2011, 4:07 PM), http://www.computerworld.com/article/2509366/security0/90--of-companies-say-they-ve-been-hacked--survey.html [https://perma.cc/YWJ7-NP87].

[226] *See* Trotter, *supra* note 20.

would this create incentives for organizations to mitigate risks by diligently following the security regulations?

3. Health Data Security and Proposed Private Right of Action in Europe

The European Union ("EU") appears to believe that consumer protection will provide the necessary incentives to decrease data breaches. In EU, consumer data protection is governed by Article 16 of the "Treaty on the functioning of the European Union."[227] The European Union grants all Europeans "the right to the protection of personal data concerning them."[228] Further, the upside of a single, unifying law "will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion[229] a year."[230] Presently, Europeans whose data is compromised have the option to submit a complaint.[231] This recourse is akin to submitting a

---

[227] *Data Protection in the EU*, EUR. COMMISSION, http://ec.europa.eu/health/data_collection/data_protection/in_eu/index_en.htm, [https://perma.cc/K59Z-G4XP] (last visited Feb. 8, 2017).

[228] *Id.*

[229] Based on the March 11, 2016 exchange rate, €2.3 billion is equivalent to $2.56 billion. *XE Currency Converter*, XE.COM, http://www.xe.com/currencyconverter/convert/?Amount=2.3&From=EUR&To=USD, [https://perma.cc/DYT4-ZBEN] (last visited March 11, 2016).

[230] *Reform of EU Data Protection Rules*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/reform/index_en.htm [https://perma.cc/ZZQ9-GW24] [hereinafter *EU Data Reform*] (last updated June 1, 2016).

[231] *Protection of Personal Data in the European Union*, EUR. COMMISSION (Nov. 2010), *http://ec.europa.eu/justice/data-protection/files/eujls08b-1002_-_protection_of_personnal_data_a4_en.pdf* [https://perma.cc/B5VU-R5U2].

HIPAA violation complaint to OCR in the United States.[232] However, Europeans then have the right to then take the complaint to the European Court of Justice and receive money damages if harm was, in fact, suffered.[233] A proposed EU directive creates a private right of action against the data controller—quivalent to a covered entity—who allegedly caused the data beach.[234]

4. Proposed Private Right of Action in the United States

The myriad of jurisdictions declining to create a private right of action for a HIPAA violation is well documented in Section II.[235] Most commonly, the courts look first to the text of the statute and regulations for an express right; if an express right of action is not found, the courts then look to congressional and agency intent.[236] For example, the *Byrne* court reasoned that, because HHS explicitly outlined very detailed regulations regarding civil and criminal liabilities for covered entities, the exclusion of any private right of action was also explicit.[237]

---

[232] *See Breach Portal*, *supra* note 132.

[233] Commission Regulation (EC) 45/2001, 2001 O.J. (L 8) 1, 16, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=en [https://perma.cc/97KY-S5KA].

[234] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final, 1, 89-94 (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, [https://perma.cc/RRL6-CX43] [hereinafter *Proposal for a Regulation*].

[235] *See supra* Section II.

[236] *See, e.g.*, Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 45-47 (Conn. 2014).

[237] *Id.*

However, the total number of ePHI data breaches now numbers in the hundreds of millions.[238] Healthcare costs are high and are continuously growing higher.[239] Data breaches generally are expensive, but cyber attacks on health data are the most expensive data breaches.[240]

Some experts argue that covered entities must adopt a "culture of security."[241] The recent mega data breaches, including the Anthem breach, indicate that companies do not take security as seriously as they ought to.[242] This lack of seriousness leads to expansive—and *expensive*—data breaches.[243] Could recognizing a private right of action to victims of a data breach help incentivize a "culture of security" in these companies? Possibly—if the cost incentives are present.[244]

C. Costs of Security Data Breaches

1. Costs to the Covered Entity

HIPAA was enacted and its regulations promulgated, in part, to decrease healthcare costs.[245] From a recent study discussed in Section I, in the United States, the cost of a malicious data breach is $230 per personally identifiable

---

[238] *See* Munro, *supra* note 9.

[239] Lita Epstein, *6 Reasons Healthcare Is So Expensive in the U.S.*, INVESTOPEDIA (Aug. 6, 2015, 6:40 PM), http://www.investopedia.com/articles/personal-finance/080615/6-reasons-healthcare-so-expensive-us.asp, [https://perma.cc/2D2B-BEW7].

[240] Pence, *supra* note 27.

[241] Munro, *supra* note 9.

[242] *Id.*

[243] *Id.*

[244] Trotter, *supra* note 20.

[245] 42 U.S.C. § 1320d-1(b) (2012).

record,[246] and the cost is $398 per healthcare record; thus, at nearly 80 million records stolen, the Anthem data breach could cost upwards of $32 billion.[247] However, even if the full cost was realized, the figure is only a percentage of what Anthem earned in 2014 alone: $73.8 billion.[248] One reporter commented, "[t]he losses involved are so small compared to the revenue that it's easier to take a chance and write off any losses should they occur. In other words, worrying about data breaches isn't worth it to [companies]."[249]

Experts assert that HIPAA compliance is not as prohibitively expensive as many companies argue compliance to be.[250] For small covered entities, compliance generally costs $4,000 to $12,000.[251] For medium to large covered entities, approximate costs begin at $50,000 and vary, depending on the circumstances.[252] However, the costs of HIPAA non-compliance can range in the hundreds of

---

[246] Pence, *supra* note 27.

[247] Conn, *supra* note 23; *see supra* text accompanying note 30.

[248] *Redefining, Reinventing, Reassuring: 2014 Annual Report*, ANTHEM, 1, 12 (2014) http://media.corporate-ir.net/media_files/IROL/13/130104/2014AR/export7/pdfs/Anthem_2014AR.pdf [https://perma.cc/PRP4-93AM] [hereinafter *2014 Annual Report*].

[249] Erik Sherman, *The Reason Companies Don't Fix Cybersecurity*, CBS NEWS (Mar. 12, 2015, 5:30 AM), http://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity [https://perma.cc/NXZ8-BALY].

[250] *See* Tod Ferran, *How Much Does HIPAA Compliance Cost?*, SECURITY METRICS BLOG, http://blog.securitymetrics.com/2015/04/how-much-does-hipaa-cost.html [https://perma.cc/W6C6-JSEF] (last visited Feb. 8, 2017); Jay Hodes, *HIPAA – Can You Afford to be Compliant?*, COLINGTON SECURITY (Feb. 3, 2016), http://colingtonsecurity.com/hipaa-can-you-afford-to-be-compliant/ [https://perma.cc/MT42-94FX].

[251] Ferran, *supra* note 250.

[252] *Id.*

thousands to millions of dollars.[253] While HHS's cost approximation of compliance—$1040 per organization—is certainly unrealistic, even the most expensive measures are significantly lower in cost than the potential cost of a data breach.[254] HIPAA compliance simply makes financial sense for the covered entity.

2. Costs to the Consumer

Comparatively, victims face far greater possibilities of harm.[255] With no private right of actions, most victims will be unable to sue for any distant future harms.[256] Further, these future harms are often difficult to prove because they may manifest years, and even decades, into the future.[257] Those individuals who encounter actual harm soon after the breach must rely on standard negligence claims for any hopes of recovery.[258] However, many victims of data breaches must often remain vigilant for the rest of their lives, in order to detect any harm—even decades later.[259]

IV. CONCLUSION

As discussed in Sections II and III, HIPAA does not currently provide a private right of action claim for harm suffered as a result of a HIPAA violation.[260] However, an increasing number of state courts are recognizing that

---

[253] *Id.*; *see also* Hodes, *supra* 250.

[254] Ferran, *supra* note 250.

[255] *See* Chideya, *supra* note 35.

[256] *See id.*; *see also* Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138, 1155 (2013).

[257] Chideya, *supra* note 35.

[258] *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32 (Conn. 2014).

[259] Wong, *supra* note 2.

[260] *See supra* Sections II, III.

HIPAA can be used in the determination of the standard of care in negligence claims.[261] However, moving from a tort model to a regulatory model shows promise: per *Wyndham Worldwide*, the FTC now has the power to regulate unreasonable cyber security polices and practices, as they are "unfair or deceptive acts or practice."[262] Although recently limited by *LabMD*,[263] the national trend overall indicates increased security regulations for dismal data protection.

Unlike the United States, the EU has stronger security regulations and offers slightly stronger remedies.[264] Proposed legislation would create even more stringent security regulations, while also giving the victim a private right of action against an organization who misused or otherwise did not appropriate secure the person's personal data.[265] The EU projects $2.56 billion in yearly savings as a direct result of the new legislation.[266]

Among all relevant countries, data breaches in the United States are the most expensive.[267] Further, among all industries in the United States, breaches of healthcare data are the most expensive breaches.[268] Malicious breaches—including cyber attacks, as in the Anthem breach—are more expensive than breaches due to technical failure and ordinary negligence.[269]

---

[261] *See, e.g.* Byrne, 102 A.3d at 32.

[262] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

[263] LabMD, Inc., 2015 FTC LEXIS 272, at *1 (F.T.C. Nov. 13, 2015).

[264] *See EU Data Reform*, *supra* note 230.

[265] *Proposal for a Regulation*, *supra* note 234, at 89–94.

[266] *EU Data Reform*, *supra* note 230; *XE Currency Converter*, *supra* note 229.

[267] Conn, *supra* note 23.

[268] *Id.*

[269] Pence, *supra* note 27.

While major corporations may take an initial economic hit from notifications, remediation, and diminished reputation, the data clearly shows the numbers are dwarfed in comparison to yearly earnings and routine expenditures.[270] Individual consumers are harmed significantly more than the companies that were breached.[271] Consumers must be vigilant for the rest of their life. Fraud, identify theft, or medical identity theft could truly be devastating to an individual.

Allowing victims of a data breach as a result of a cyber attack to exercise a private right of action, in conjunction with stricter and prohibitively expensive regulatory penalties, could put pressure on companies to create a culture of security.[272] Instead of writing off security and the risk of breach as another business expense, companies would invest in their future by strengthening their security policies and procedures.[273] It is unlikely to cost the company as much to implement stronger security than it costs society when major breaches of consumer data occur.

If OCR enacted stronger federal regulations, including a private right of action for violation of HIPAA security provisions from cyber attacks, covered entities and business associates would strengthen their security practices in order to mitigate the risk of liability. This strengthening of security to protect ePHI would lead to less data breaches as a result of cyber attacks. Cyber attacks are prohibitively expensive, so a decrease in attacks will decrease overall costs, both presently and in the future.

---

[270] *2014 Annual Report*, *supra* note 248.
[271] Chideya, *supra* note 35.
[272] *See, e.g.*, Munro, *supra* note 9.
[273] Sherman, *supra* note 249.