JOURNAL OF HEALTH CARE FINANCE

Spring 2016

Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?

Diane Doebele Koch, JD, RN

INTRODUCTION

Approximately 112 million Americans or nearly one third of the United States population have been affected by breaches of so called "protected health information" ("PHI")[1] in 2015 alone.[2] During the last year, almost 100 million records were hacked from the network servers of just three organizations: Excellus Health Plan, Inc. with 10 million individuals affected, Premera Blue Cross with 11 million individuals affected and Anthem, Inc. Affiliated Covered Entity with a record 78.8 million individuals affected.[3] Based on the information reported in the United States Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") database, which publishes the breaches affecting 500 or more individuals, the majority of breaches or approximately 38% were due to "unauthorized access/disclosure;" however in the top ten breaches (i.e. affecting the most individuals) 90% were due to a "hacking/IT incident."[4] During the last three years 42.5% of all data breaches were attributable to the healthcare industry.[5] In the last two years an alarming 91% of healthcare companies reported a data breach.[6] Almost half of the breaches have been found to be criminal in nature.[7]

In a report published by the Ponemon Institute in May 2015 examining privacy and security data for healthcare covered entities and business associates, criminal attacks were identified as the main cause of healthcare data breaches and such attacks have grown over 125% during the last five years.[8] "Spear phishing" accounts for 88% of these criminal attacks and malware for 78% of all criminal activities.[9] So what is spear phishing? It is not a recreational activity. Spear phishing is a tool cybercriminals use to gain unauthorized access to sensitive information or to install malware on the targeted victim's computer.[10] This is accomplished by sending emails targeting

---

[1] Protected health information is personally identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Protected health information excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232(g) (1974), records described at 20 U.S.C. 1232(g)(a)(4)(B)(iv)(1974) and employment records held by a covered entity in its role as employer, http://www.NCBI.NLM.NIH.gov/books/NBK9576 (last visited March 18, 2016).

[2] Dan Munro, *Data Breaches In Healthcare Totaled Over 112 Million Records In 2015*, Forbes (Dec. 31, 2015), http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#c2ef4fb7fd5a (last visited March 18, 2016).

[3] *Id.*

[4] *Id*.

[5] Stephanie Tayengco, *Why are healthcare data breaches so common?* Becker's Hospital Review (Sept. 17, 2015), http://www.beckershospitalreview.com/healthcare-information-technology/why-are-healthcare-data-breaches-so-common (last visited March 18, 2016).

[6] *Id*.

[7] Shannon Pettypiece, *Rising Cyber Attacks Costing Health System $6 Billion Annually.* Bloomberg Business (May 7, 2015), http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually.

[8] Erin McCann, *Criminal Attacks Become No. 1 Cause of Data Breaches*, Healthcare IT news (May 7, 2015), http://www.healthcareitnews.com/news/criminal-attacks-healthcare-become-no-1-cause-data-breaches (last visited March 18, 2016).

[9] *Id.*

[10] Federal Bureau of Investigation. *Spear Phishers Angling to Steal Your Financial Info*, April 1, 2009, https://www.fbi.gov/news/stories/2009/april/spearphishing_040109 (last visited March 18, 2016).

select groups of people with a common bond, e.g. they work at the same company.[11] The e-mails appear to be legitimate, i.e. from a source the victim would know or normally get e-mails from (to appear legitimate the criminals sometimes hack into the organization's computer network).[12] Victims are asked to click on a hyper link inside the e-mail that bring them to a phony, but genuine looking website, where they are prompted to provide passwords, user IDs, access codes, etc.[13] Once criminals have this access information, they are able to obtain the sensitive data they are seeking. Spear phishing can also trick victims into downloading malicious codes or malware by clicking on a link embedded in the e-mail.[14] The second cause of health care data breaches was lost or stolen computers; representing 43% of all data breaches. [15] Notwithstanding the fact that criminal activity is now the main cause of data breaches in the healthcare industry, the majority of healthcare security personnel (70%) were more worried about employee negligence than cyberattacks (40%).[16] Generally breaches are discovered as a result of an audit (69%), notification from an employee (44%) or a patient complaint (30%).[17] Given the major breaches cited above, the healthcare industry is not responding aggressively enough to thwart these attacks. Why not?

Perhaps because the federal law relating to the security of an individual's PHI is too lax. The HIPAA Security Rule sets forth national standards to protect individuals' electronic personal health information ("ePHI") that is created, received, used, or maintained by a "Covered Entity" i.e. health plans, health care clearinghouses, and health care providers or their respective business associates who transmit health information in electronic form.[18] The Security Rule requires certain administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. [19] Within the Security Rule there are both "required" implementation specifications and "addressable" specifications.[20] While Covered Entities are mandated to take certain steps to protect ePHI, there is flexibility built in with the addressable specifications. Unfortunately the public is dependent on the Covered Entity to ensure its ePHI is safe and is unaware of what measures the Covered Entity has taken to meet the implementation specifications in the Security Rule. While HIPAA compliance appears to be an issue being addressed in the health care sector, more must be done to bolster the security requirements intended to protect ePHI in the current environment.

The current penalties for HIPAA breaches are not a strong enough deterrent to catalyze change. Although OCR can impose fines on organizations for unauthorized disclosures of PHI and failing to protect the public against loss, theft and disclosure of PHI, the penalties are ineffective given the increasing number and extent of recent breaches.[21] While OCR has imposed

[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] McCann, *supra* at 8.
[16] *Id.*
[17] *Id.*
[18] 45 CFR §160.103
[19] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals (Last visited March 18, 2016).
[20] *Id.*
[21] Munro, *supra* note 1.

several hefty fines this past year, in 2014 OCR received nearly 18,000 complaints yet only six formal actions were taken.[22] Is the decision to take action dependent upon who is affected by the breach?[23] As for the Anthem breach, penalties are laughable given the magnitude of the breach. Anthem's annual net income for the year ending December 31, 2014 was $2.5 billion. Is a maximum fine of $1.5 million really a deterrent? Obviously it is barely a slap on the wrist.[24] Who is protecting the average American? Clearly, the current HIPAA[25] Security Rule is not enough to protect our electronic PHI ("e-PHI") in the cyber age.

I. COST TO SOCIETY AND INDIVIDUALS

Nearly everyone who has been to the doctor in the last decade has signed an acknowledgement of receipt of the entity's Notice of Privacy Practices usually included amongst the new patient paperwork. We willingly divulge our most prized information, our identity or PHI, in exchange for the ability to receive medical care. Have we been naïve in doing this and not demanding better protection for our PHI?

Ramifications of a breach are numerous and far-reaching for the individuals affected, and prohibitively expensive for the healthcare industry and government. The cost to the United States healthcare systems from cyber attacks is estimated to be $6 billion dollars per year.[26] The estimate of cost to a hospital for an average data breach is $2.1 million.[27] For individuals the costs are different but often times have graver consequences. Not only can your financial information be stolen and used to take a loan in your name; someone may obtain medical care for free using your insurance information.[28] As far as cost to individuals the Medical Identity Fraud Alliance estimates that 65% victims of medical identity theft paid more than $13,000 to resolve the problem.[29] Additionally, some issues can't be resolved. Unlike when your credit card is stolen (and you get a new number), you can't change your actual medical history.[30] Medical records can become contaminated permanently. For example:

- In Oregon, a pregnant woman delivered a baby addicted to crack using another woman's social security number—and then abandoned the baby. Police arrested the victim and put her children into protective custody.
- A hospital's billing department notified a pregnant woman in Washington that someone had used her social security number to be treated for a crack overdose at the ER of the same facility where she was about to deliver her baby.

---

[22] *Id.*
[23] *Id.*
[24] Paul Bedard. *Brookings: Healthcare hacks up1800%, penalties on firms weak,* Washington Examiner (Feb. 13, 2015), http://www.washingtonexaminer.com/brookings-healthcare-hacks-up-1800-penalties-on-firms-weak/article/2560199
[25] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (H.R. 3103) (Aug. 21, 1996).
[26] Pettypiece, *supra* at 7.
[27] *Id.*
[28] *Id.*
[29] Consumer Affairs, http://www.consumeraffairs.com/news/class-action-suit-filed-against-ucla-health-over-patient-data-security-breach-072315.html (last visited April 2, 2016).
[30] *Id.*

- A patient in Texas used a California man's medical identity to obtain radiation treatment and other care. When the thief's records and the patient's records merge, healthcare providers will think the patient has a condition he doesn't have.

- Another woman couldn't get physical therapy following neck surgery because a Miami clinic that she had never visited claimed her insurance benefits had been maxed out.

- A teenager was denied the opportunity to give blood because the Red Cross flagged her social security number as belonging to a person who had tested positive for HIV. Another person had used her social security number at a free AIDS clinic in another state, and the clinic did not ask for physical copies of identification.[31]

Other examples provided by the World Privacy Forum are:

- A Massachusetts psychiatrist created false diagnoses of drug addiction and severe depression for people who were not his patients in order to submit medical insurance claims for psychiatric sessions that never occurred. One man discovered the false diagnoses when he applied for a job. He hadn't even been a patient.

- An identity thief in Missouri used the information of actual people to create false driver's licenses in their names. Using one of them, she was able to enter a regional health center, obtain the health records of a woman she was impersonating, and leave with a prescription in the woman's name.

- An Ohio woman working in a dental office gained access to protected information of Medicaid patients in order to illegally obtain prescription drugs.

- A Pennsylvania man found that an imposter had used his identity at five different hospitals in order to receive more than $100,000 in treatment. At each spot, the imposter left behind a medical history in his victim's name.

- A Colorado man whose Social Security number, name and address had been stolen received a bill for $44,000 for a surgery he not undergone.[32]

[31] R. Kam & C. Arevalo, *A glimpse inside the $234 billion world of medical fraud,* Government Health IT (Feb. 8, 2012), http://www.govhealthit.com/news/glimpse-inside-234-billion-world-medical-id-theft.
[32] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), http://khn.org/news/rise-of-indentity-theft/.

These are not examples of mere inconveniences. The consequence of another person stealing and utilizing your PHI can result in misdiagnosis, inability to receive treatment, credit problems and other unforeseen consequences as shown above.

Not only are hackers stealing information, they are hijacking hospital databases for ransom.[33] In what is now being called "cyber extortion" or "ransomware attacks," hackers take control of integral computer systems and prevent employees and hospital administrators from accessing the data or communication tools they need to conduct business.[34] These attacks can prevent access to email and although they do not necessarily prevent patients from being seen or totally disable all systems, they interfere enough to prompt hospitals to make ransom payment to stop the attack. [35] At Hollywood Presbyterian Medical Center, hackers seized control of critical computer systems until the hospital paid a $17,000 ransom to release them.[36] In another small hospital, Titus Regional Medical Center, an attack took a critical electronic medical record system offline until ransom was paid.[37] These are not in the media because they do not constitute HIPAA violations. Hackers are not necessarily getting access to the data or PHI in order to encrypt it and/or block others from using it.[38] Apparently hospitals have no choice but to pay. [39] Attackers sometimes demand payment in a currency called Bitcoins, a hard to trace currency used by online criminals. Bitcoins are a virtual currency created on the Internet by an individual using an alias.[40] Sounding more like fiction than fact, transactions are made anonymously with no transaction fees and no brokers.[41] Some retail merchants even accept bitcoins as payment.[42] Dell has researched this phenomenon and learned that one ransom payment server collected over one million dollars in just six months.[43] Health care organizations are more vulnerable because unlike the financial services industry, they have not yet implemented sophisticated backup systems and security tools needed to prevent the attacks.[44]

II. WHY PHI? WHY NOW?

The reason for the massive increase in data breaches and theft of ePHI is simple: valuable data and vulnerable systems. Cyber criminals have recognized that healthcare companies have allocated limited resources in the technology used to protect the massive amounts of valuable information they manage.[45] Unlike basic credit card information, obtaining a person's medical

[33] Stacey Cowley & Liam Stack, *Los Angeles Hospital Pays Hackers $17,000 after Attack,* N.Y. TIMES (Feb. 18, 2016), http://www.nytimes.com/2016/02/19/business/los-angeles-hospital-pays-hackers-17000-after-attack.html?_r=0.

[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] Tal Yellin, Dominic Aratari &Jose Pagliery, *What is Bitcoin*, CNN Money, http://money.cnn.com/infographic/technology/what-is-bitcoin/ (last visited April 8, 2016).
[42] *Id.*
[43] Cowley, *supra* at 33.
[44] *Id.*
[45] Poneman Institute, *Criminal Attacks: The New Leading Cause of Data Breach in Healthcare*

record is the mother lode of sought after identity data. It is one stop shopping for criminals and hackers. Also know as "doxing," hacker slang for compiling a dossier on people with information obtained on the Internet or from databases, criminals are using the information for purposes ranging from financial gain to espionage.[46] Previously financial institutions had been the targets of criminal syndicates until they discovered healthcare databases were more valuable.[47] Medical records contain social security numbers, insurance information, addresses, medical information and other information valuable to identity thieves.[48] Consequently PHI is much more lucrative on the market; it is worth approximately 20 times more than a stolen credit-card number.[49] Sadly, in a survey conducted by the Ponemon Institute, fifty percent (50%) of the health care companies surveyed disclosed that they didn't have the qualified personnel or resources to prevent or detect a breach quickly.[50]

III. LEGAL FRAMEWORK FOR PROTECTION OF PHI

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191, was passed to help improve efficiency in the health care system and included provisions that required HHS to create national standards for electronic health care transactions.[51] Also, Congress foresaw that electronic technology advances could jeopardize the privacy of health information and therefore Congress incorporated additional provisions requiring Federal privacy protections for individually identifiable health information within HIPAA.[52] HHS published a Privacy Rule in December 2000 providing national standards for the protection of PHI by three types of covered entities: (i) health plans, (ii) health care clearinghouses, and (iii) health care providers who utilize electronic means to conduct health care transactions.[53] Compliance with the Privacy Rule became effective April 14, 2003 (or for small health plans April 14, 2004).[54]

A. HIPAA SECURITY RULE

Additionally, HHS published a final Security Rule in February 2003 providing national standards to protect the integrity, confidentiality and availability of ePHI.[55] Prior to this, there was no uniform set of security standards for protecting ePHI. Covered Entities were required to comply with the Security Rule effective April 20, 2005 (or for small health plans April 20, 2006).[56] The security standards are divided into three categories (i) administrative, (ii) physical, and (iii)

(May 7, 2015, 9:00 am) http://www.ponemon.org/blog/criminal-attacks-the-new-leading-cause-of-data-breach-in-healthcare

[46] Fortune, *Whatever You Do, Don't Get Doxed* (Mar. 2, 2016, 10:22am), http://fortune.com/video/2016/03/02/doxing-cyber-espionage/

[47] Pettypiece, *supra* at 7.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/ (last visited March 18, 2016).

[52] *Id.*

[53] 45 C.F.R. § 160.103 (2014).

[54] *Supra* at 51.

[55] *Id.*

[56] *Id.*

technical safeguards.[57] Administrative safeguards include appointing someone responsible for the security and security training requirements.[58] Physical safeguards include taking the steps required to protect electronic systems, equipment and the data they hold, from being compromised, including restricting access to ePHI and maintaining computer backups at another location (off site).[59] Technical safeguards include the technical processes used to protect data and control access to data, such as authentication controls to verify that the person signing onto a computer is authorized to access the ePHI, or encrypting data as it is being stored and/or transmitted.[60] The Security standards are both mandatory and permissive:

> **(a)** ***General requirements.*** Covered entities and business associates must do the following:
> **(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 subpart E of this part.
> **(4)** Ensure compliance with this subpart by its workforce.
>
> **(b)** ***Flexibility of approach.***
> **(1)** Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
> **(2)** In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
> **(i)** The size, complexity, and capabilities of the covered entity or business associate.
> **(ii)** The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
> **(iii)** The costs of security measures.
> **(iv)** The probability and criticality of potential risks to electronic protected health information.[61]

Within the Security Rule there are implementation specifications, some of which are required, others are labeled addressable, meaning that the covered entity must implement the specification it if it is reasonable, but does not have to implement if (i) an alternative would accomplish the same purpose, or (ii) the standard can be met without implementing the specification.[62] To

[57] U.S. Dept. of Health and Human Services, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf, at pg.8 (last visited April 9, 2016).
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] 45 CFR §164.306.
[62] 45 CFR § 164.306(d).

provide guidance, in the preamble to the Security Rule, publications issued by the National Institute of Standards and Technology ("NIST") were cited as a resource for IT Security.[63] NIST is an agency of the United States Department of Commerce.[64] Federal agencies are required to comply with NIST standards and other industries have protocols for the security of the information they are responsible for.[65] The latitude the health care industry has been allowed with "addressable" vs. "required" implementation specifications is one explanation for the exponential rise in recent health care data breaches. If an implementation specification is "required," it must be implemented.[66] "Addressable" implementation specifications were introduced to provide covered entities some flexibility with respect to compliance with the security standards.[67] If the specification is "addressable," a covered entity must either: (a) implement the addressable implementation specifications; (b) implement an alternative security measure(s) to accomplish the same purpose; or (c) not implement (a) or (b).[68] The Covered Entity must document its decision whether the addressable implementation specification is a reasonable security measure within its particular security framework; whether there is an alternative that is reasonable; or if neither the standard nor alternative is reasonable and why.[69] The decision will be based on the risk analysis, risk mitigation strategies, security measures already in place, and costs of implementation.[70] The written documentation should include the results of the risk assessment that prompted the decision and the factors considered.[71] Attached as Exhibit A are the "required" and "addressable" Security Standards. Reviewing some of the "addressable" standards below will provide insight into why the HIPAA Security Rule needs amending. The following standards are **NOT** required but are considered addressable:

***Administrative Standard**: Workforce Security*[72]

- Authorization and/or Supervision: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

- Workforce Clearance procedure: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

- Termination Procedures: Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends.

---

[63] National Institute of Standards and Technology, http://www.nist.gov/healthcare/security/hipaasecurity.cfm. (last visited March 17, 2016).
[64] *Id.*
[65] *Id.*
[66] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html (last visited March 22, 2016).
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] 45 CFR § 164.308(a)(3).

***Administrative Standard**: Information Access Management*[73]

- Access Authorization: Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

- Access Establishment and Modification: Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

***Administrative Standard**: Security Awareness and Training* [74]

- Security Reminders: Implement periodic security updates.

- Protection from Malicious Software: Implement procedures for guarding against, detecting, and reporting malicious software.

- Login Monitoring: Implement procedures for monitoring log-in attempts and reporting discrepancies.

- Password Management: Implement procedures for creating, changing, and safeguarding passwords.

***Administrative Standard**: Contingency Plan*[75]

- Testing and revision procedures: Implement procedures for periodic testing and revision of contingency plans.

- Applications and data criticality analysis: Assess the relative criticality of specific applications and data in support of other contingency plan components.

***Physical Safeguards:** Facility Access Control*[76]

- Contingency Operations: 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.

- Facility Security Plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

[73] 45 CFR § 164.308(a)(4).
[74] 45 CFR § 164.308(a)(5).
[75] 45 CFR § 164.308(a)(7).
[76] 45 CFR § 164.310(a)(1).

- Access Control and Validation Procedures: 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.

- Maintenance Records: 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).

Physical Safeguards: *Device and Media Controls*[77]

- Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

- Data Back up and Storage: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Technical Safeguards: *Access Control*[78]

- Automatic logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

- Encryption and decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.

Technical Safeguards: *Integrity*[79]

- Mechanism to Authenticate Electronic Protected Health Information: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Technical Safeguards: *Transmission Security*[80]

- Integrity Controls: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

- Encryption: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

In reviewing these "addressable" standards it is obvious why there have been so many data breaches in the healthcare industry and why there is an urgent need to amend the HIPAA Security Rule. In its 2006 publication "HIPAA Security Guidance," HHS offers suggestions on

[77] 45 CFR § 164.310(d)(1).
[78] 45 CFR § 164.312(a)(1).
[79] 45 CFR § 164.312 (c)(1).
[80] 45 CFR § 164.312 (e)(1).

mitigating risks of unauthorized access of ePHI by implementing protocols suchs as using a "two-factor authentication for granting remote access to systems that contain ePHI (requires factors beyond usernames and passwords to gain access to systems, e.g., answering a security question such as "favorite pet's name"); creating other barriers if granting remote access; using anti-virus software; and having automatic log-offs.[81] Yet many of these protections are not implemented and create a portal for cyber criminals to gain access to supposedly "secure" systems and ultimately our PHI.

B. HITECH

While HIPAA created national standards for the privacy and security of protected health information, the Health Information Technology for Economic and Clinical Health Act ("HITECH") established breach notification requirements to allow for greater transparency with the public.[82] In addition, HITECH requires OCR to conduct periodic audits of Covered Entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules.[83] HITECH established mandatory penalties for willful neglect and requires patients and designated third parties access to their PHI in an electronic format. [84]. HITECH also requires business associates to comply with the measures provided for in the HIPAA Security Rule.[85]

IV. LEGAL CONSEQUENCES OF HIPAA VIOLATION

For HIPAA violations there are three main areas of controlling legal consequence: (i) the administrative remedies and civil monetary penalties provided under HIPAA; [86] (ii) an individual's private right to sue under State law tort claims;[87] and (iii) State Attorneys General authority to investigate and penalize HIPAA violators.[88] In addition, there can be criminal actions against individuals for HIPAA violations; FTC actions and class action lawsuits. [89] In the event of a HIPAA breach, Covered Entities must comply with the Breach Notification Rule.[90]

---

[81] U.S. Dept. of Health and Human Services, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf, page 4 (last visited April 9, 2016).
[82] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html (last visited March 18, 2016).
[83] *Id.*
[84] University of South Florida, http://www.usfhealthonline.com/resources/key-concepts/hitech-act-summary/#.VvgdMKvAHzI (last visited March 18, 2016).
[85] *Id.*
[86] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html (last visited March 18, 2016).
[87] Cullen Archer, *Does HIPAA preempt state law claims related to privacy of individually identifiable health information?(*May 19, 2015), https://www.law.utah.edu/does-hipaa-preempt-state-law-claims-related-to-privacy-of-individually-identifiable-health-information/.
[88] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/ (last visited March 18, 2016).
[89] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html (last visited March 18, 2016).
[90] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited March 18, 2016).

A. ADMINISTRATIVE REMEDIES

If an entity subject to HIPAA violates the HIPAA rules, OCR may investigate, enter into a resolution agreement or impose civil and criminal penalties against the covered entity or business associate.[91] Basically, a resolution agreement is a settlement agreement between HHS and the health care entity. The entity agrees to certain obligations (sometimes including payment of a resolution amount) and reporting requirements usually for a period of three years.[92] As a last resort, civil monetary penalties (CMP's) may be imposed upon an entity that does not fulfill its obligations.[93] As mentioned above, these penalties appear inadequate given the magnitude of recent breaches.[94] If OCR accepts a complaint for investigation, it notifies both the complainant and the covered entity.[95] Then both parties present information about the incident set forth in the complaint. [96] HIPAA regulation requires covered entities to cooperate with complaint investigations.[97] If a complaint alleges facts that could be deemed a violation of the criminal provision of HIPAA (42 U.S.C. 1320d-6), the United States Department of Justice ("DOJ") may receive the complaint from OCR for DOJ investigation.[98] Once the evidence is evaluated, OCR determines the resolution and/or any corrective action needed.[99]

If the Covered Entity does not take the action necessary to bring the matter to resolution, OCR may impose CMPs on the Covered Entity.[100] If CMPs are imposed, an administrative hearing may be requested by the entity in which an HHS administrative law judge evaluates whether the penalties are justified based on the evidence. [101] The penalties are deposited in the U.S. Treasury.[102] The complainants do not receive any portion of the penalties.[103] The penalties were updated following the introduction of the Omnibus Rule.[104] The Omnibus Rule took effect on March 26, 2013.[105] The new penalties can be applied to Covered Entities and their Business Associates for violation of HIPAA Rules.[106] The new penalty structure is tiered, relative to the knowledge the breaching party had of the violation.[107] OCR can seek a penalty based on the

[91] U.S. Dept. of Health and Human Services, HIPAA For Professionals, Compliance Enforcement, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (last visited February 12, 2016).
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html (last visited February 28, 2016).
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] Department of Health and Human Services, https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf, at pg. 5583 (last visited April 9, 2016).
[105] *Id.*
[106] *Id.*
[107] 45 C.F.R. §160.404 (2013).

gravity of the HIPAA violation and some other factors.[108]

> For violations occurring on or after February 18, 2009, the new HITECH penalty scheme, as follows: (1) For violations in which it is established that the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision, an amount not less than $100 or more than $50,000 for each violation; (2) for a violation in which it is established that the violation was due to reasonable cause and not to willful neglect, an amount not less than $1000 or more than $50,000 for each violation; (3) for a violation in which it is established that the violation was due to willful neglect and was timely corrected, an amount not less than $10,000 or more than $50,000 for each violation; and (4) for a violation in which it is established that the violation was due to willful neglect and was not timely corrected, an amount not less than $50,000 for each violation; except that a penalty for violations of the same requirement or prohibition under any of these categories may not exceed $1,500,000 in a calendar year.[109]

OCR may not impose penalties if the covered entity or business associate did not act with willful neglect and the violation was corrected within 30 days.[110]

Breach Notification requirements mandate that in the event of a breach of unsecured PHI, notification must be provided to the individuals affected, the HHS Secretary and the media in the event the breach affects more than 500 individuals.[111] Business Associates must notify the covered entity if a breach occurs.[112] Reports of breaches affecting 500 or more individuals may be viewed at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

B. STATE LAW CLAIMS

Notwithstanding that HIPAA does not give individuals a private cause of action, HIPAA may now be used as a standard of care under a State law negligence claim involving improper disclosure of a patient's PHI (*Byrne v. Avery Center for Obstetrics and Gynecology*, P.C., 2014 WL 5507439 (Conn. Nov. 11, 2014). In *Byrne*, the Connecticut Supreme Court did not dismiss plaintiff's negligence claim because of HIPAA preemption and noted that HIPAA may be considered as the applicable standard of care in negligence cases where health care providers breach the patient's right of confidentiality (in this case divulging medical records).[113]

Preemption of a State law that conflicts with a Federal law originates from The Supremacy Clause of the United States Constitution. "This Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be

---

[108] *Id.*
[109] *Id.*
[110] 45 C.F.R. §160.410(b) (2013).
[111] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited April 9, 2016).
[112] *Id.*
[113] *Byrne v. Avery Ctr. for Obstetrics & Gynecology*, P.C., 102 A.3d 32, 36 (Conn. 2014).

made, under the authority of the United States, shall be the supreme law of the land."[114] Generally the Constitution can be thought of as a floor not a ceiling. State law can provide for more stringent regulation, as is the case under HIPAA.[115] While HIPAA preempts State law generally, exceptions exist for State law tort claims (negligence, breach of confidentiality) discussed below. In those cases, the plaintiff is not suing based on violation of HIPAA, they are using a different theory of liability but using a HIPAA violation as the standard of care to prove that the entity breached a duty owed to the patient under relevant State law.[116]

In addition to the *Byrne* decision in Connecticut, other states have allowed private causes of action using a HIPAA violation as the standard of care. Despite HIPAA preemption North Carolina, Utah and Indiana have allowed state law tort claims where there has been a breach of patient confidentiality and/or their medical information. In the North Carolina case *Acosta v. Byrum*, Heather Acosta ("Acosta") was both a patient and employee of Dr. David Faber whom she accused of improperly allowing the office manager, Robin Byrum ("Byrum") to access Acosta's medical and psychiatric records by using Faber's access credentials all without Acosta's consent.[117] Byrum then disclosed Acosta's confidential information to third parties without Acosta's authorization.[118] "Acosta "alleged that she experienced severe emotional distress, humiliation, and anguish from the exposure of her medical records to third parties… and that Dr. Faber knew or should have known that his negligence would cause severe emotional distress."[119] Acosta also alleged that Faber's negligence in allowing Byrum to use his access information violated HIPAA in addition to several healthcare organizational policies.[120] In reversing the trial court's decision to grant Faber's motion to dismiss, the Court acknowledged that Acosta did not seek a cause of action under HIPAA but instead utilized HIPAA as evidence of the standard of care, which is an element of a negligence cause of action.[121]

In the Utah case *Sorensen v. Barbuto*, Nicholas Sorensen ("Sorensen") had been a passenger in a car accident and suffered brain and back injuries.[122] He was initially treated by Dr. Barbuto for seizures and head injuries until after one and one-half years, Sorensen had to change physicians because his medical insurance no longer included Dr. Barbuto as an approved provider.[123] Sorensen went to another physician, and subsequently filed a personal injury action. Sorensen's medical records were submitted in the case as evidence and the insurer's defense counsel subpoenaed Dr. Barbuto to testify.[124] A delay ensued and during that time, Dr. Barbuto had ex parte communications with the defense team and agreed to testify as an expert witness on behalf of the insurance company against Sorensen. This was the basis for Sorensen's tort claims against Dr. Barbuto.[125] Dr. Barbuto filed a motion to dismiss, which was granted by the trial court.

---

[114] U.S. CONST. art VI, cl. 2.
[115] Cullen, *supra* at 87.
[116] *Id.*
[117] *Acosta v. Byrum*, 638 S.E.2d 246, 249 (N.C. App. 2006).
[118] *Id*.
[119] Id. at 251.
[120] *Id.* at 250.
[121] *Id.* at 253.
[122] *Sorensen v. Barbuto*, 143 P.3d 295, 298 (Utah Ct. App. 2006) aff'd and remanded, 177 P.3d 614 (Utah 2008).
[123] *Id.*
[124] *Id.*
[125] *Id.*

However on appeal, Sorensen asserted that Dr. Barbuto breached his fiduciary duties of confidentiality and loyalty and also violated professional standards.[126] Although Barbuto tried to argue that no private right of action existed for breach of professional standards, the Court clarified that Sorensen did not contend a private right of action.[127] Instead, Sorenson cited HIPAA, the AMA's Principles of Medical Ethics and the Hippocratic Oath to help define the standard of care.[128] Reversing the trial court, the Appeals Court allowed Sorenson to pursue his breach of confidentiality claim under state law tort theory.[129] Ultimately, Utah's Supreme Court affirmed the appellate court decision which held that Dr. Barbuto's ex parte communications with opposing counsel in Sorensen's personal injury action violated Dr. Barbuto's fiduciary duty of confidentiality.[130]

In *Byrne*, the Court allowed plaintiff's state law cases for negligence and negligent infliction of emotional distress against the clinic where the plaintiff was a patient.[131] In the midst of a paternity suit between Andro Mendoza and Emily Byrne, Mendoza subpoenaed Byrne's medical records.[132] Byrne had instructed the Avery Center for Obstetrics and Gynecology, P.C. ("the Center") not to release her medical records to Mendoza, however the Center disregarded her instructions and complied with the subpoena.[133] Byrne sued the Center for negligence and negligent infliction of emotional distress because after viewing her medical records, Mendoza began harassing and attempting to extort Byrne.[134] In this case, the Court: (i) allowed Plaintiff's common law action to remedy a healthcare provider's breach of confidentiality (even while complying with a subpoena); (ii) stated that HIPAA does not preempt the plaintiff's state common-law causes of action; and (iii) determined that HHS regulations implementing HIPAA may inform the applicable standard of care in certain circumstances.[135]

Finally, in the Indiana case *Walgreen Co. v. Hinchy*, the Indiana Court of Appeals reviewed the trial Court's decision awarding Abigail Hinchy 1.8 million in her state law tort claims arising from Walgreen's alleged breach of confidentiality.[136] The facts of this case include a pharmacist for Walgreen (Audra Withers) who improperly accessed and disclosed Abigail Hinchy's medication profile to Withers' boyfriend (Davion Peterson) who had a previous relationship with Abigail Hinchy, after Peterson advised Withers that he might have exposed her to genital herpes.[137] After learning this, Hinchy sued Withers on the theories of negligence/professional malpractice, invasion of privacy/public disclosure of private facts, and invasion of privacy/intrusion; and sued Walgreen under the theory of respondeat superior (i.e. the employer is responsible for the actions of employees performed within the course of their employment) as well as suing Walgreen directly for negligent training, negligent supervision, negligent retention,

[126] *Id.* at 299.
[127] *Id*.
[128] *Id.*
[129] *Id.*
[130] *Sorensen v. Barbuto*, 177 P.3d 614, 620 (Utah 2008).
[131] *Byrne*, 102 A.3d 32, 36.
[132] *Id.*
[133] *Id.*
[134] *Id.* at 36-37.
[135] *Id*.
[136] *Walgreen Co. v. Hinchy*, 21 N.E. 99, 105 (Ind. Ct. App. 2014) on rehearing, 25 N.E.3d 748 (Ind. Ct. App. 2015).
[137] *Id.* at 104.

and negligence/professional malpractice.[138] The result in Hinchy reaffirms once again that HIPAA does not preempt state law claims for privacy breaches and that it may be used as the standard of care for such tort claims.

C. STATE ATTORNEY GENERALS AND DOJ INVESTIGATIONS

State Attorneys General may bring civil actions on behalf of their residents for violations of the HIPAA Privacy and Security Rules.[139] The Connecticut Attorney General's office issued the first HIPAA fine against HealthNet Inc., in the amount of $250,000, for losing a hard drive that contained the ePHI of 1.5 million individuals.[140] A number of other states have issued HIPAA fines, including Connecticut, Massachusetts, Vermont and New York, for HIPAA breaches that have affected their respective residents. [141]

Finally, the DOJ investigates who may be criminally liable under HIPAA.[142] If an individual or entity 'knowingly' obtains or discloses PHI, they could face a fine of up to $50,000 and imprisonment up to one year.[143] Knowingly means knowledge of the actions that constitute an offense and not specific knowledge of an action being in violation of the HIPAA statute.[144] If a violation is committed under false pretenses, the penalties may be increased to $100,000 and a maximum of five years in prison. [145] Those violations committed with intent to sell or use PHI for commercial or personal gain or malicious harm allow fines of $250,000 and imprisonment for up to ten years.[146] Additionally, the DOJ stated that criminal penalties for a violation of HIPAA are directly applicable to Covered Entities and their directors, employees, or officers, where the covered entity is not an individual under a theory of "corporate criminal liability."[147]

D. STATE PRIVACY LAWS

In the United States, approximately 47 states, D.C., Guam, Puerto Rico and the Virgin Islands have legislation requiring entities (private or public i.e., governmental or educational) to notify individuals of security breaches of information involving personally identifiable information.[148] These laws generally set forth what entities must comply with the law (e.g., businesses, data/ information brokers, government entities, etc); define "personal information," e.g. name combined with SSN, drivers license or state ID, account numbers, etc.; define what constitutes a breach; provide for the requirements for notice; and include exemptions, e.g., for encrypted

---

[138] *Id.* at 105.
[139] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/ (last visited April 2, 2016).
[140] HIPAA Journal (Dec. 8, 2015), http://www.hipaajournal.com/ny-attorney-general-hipaa-fine-urmc-8206/.
[141] *Id.*
[142] American Medical Association, http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page? (last visited April 2, 2016).
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited March 28, 2016).

information.[149] Attached, as Exhibit B is a table of State privacy laws.

E. FEDERAL TRADE COMMISSION

In yet another twist that could prove upsetting to the healthcare industry if they don't step up their efforts in regard to the security of ePHI, the third Circuit held that the Federal Trade Commission has authority to regulate cyber security.[150] In the case *FTC v. Wyndham Worldwide Corporation, et al*., 799 F.3d 236 (3rd Cir. August 24, 2015), it was held that the Federal Trade Commission ("FTC") has authority to regulate cyber security pursuant to Section 5(a) of the Federal Trade Commission Act 15 U.S.C.§ 45(a). In this case the FTC alleged that Wyndham did not sufficiently protect its customers' personal information allowing a breach to occur that compromised its customers' information.[151]

F. DATA BREACH CLASS ACTION LAWSUITS

Recent decisions in data breach class action lawsuits, brought by a group of individuals or businesses affected by a data breach, have made it easier to sue organizations. Generally to bring a lawsuit in Federal court, the plaintiff needs standing to sue. This means the person or entity has a legal right or justification to bring the action, i.e. they have suffered an injury, there is a relationship between the injury and conduct complained of and there is likelihood that a favorable decision will remedy the injury.[152]

The U.S. Supreme Court opined in 2013 in the case *Clapper v. Amnesty International*, that to meet constitutional requirements to sue in federal court, plaintiffs have to allege they are at imminent risk of suffering a concrete injury.[153] This case has prevented lawsuits in which the threshold of injury is speculative. [154] However recent cases have removed this hurdle by acknowledging that after a data breach with personal information, there is injury by those affected by the breach.[155]

In the case *In re Target Corp. Customer Data Security Breach Litigation*, customer payment card information had been stolen.[156] Plaintiffs were granted standing to sue alleging financial harms including unlawful charges, blocked access to bank accounts, late payment fees, and the inability to pay other bills.[157] A more recent case, *Remijas v. Neiman Marcus Group*,

---

[149] *Id.*
[150] National Law Review, *Third Circuit Finds that the FTC Has Authority to Sue Companies for Inadequate Cybersecurity Practices as an "Unfair" Practice* (Sept. 6, 2015), http://www.natlawreview.com/article/third-circuit-finds-ftc-has-authority-to-sue-companies-inadequate-cybersecurity (last visited April 2, 2016).
[151] *Id.*
[152] *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).
[153] *Clapper v. Amnesty Intern. USA, 133 S.Ct. 1138 (2013).*
[154] Robert D. Fram, Simon J. Frankel and Amanda C. Lynch, *Standing in Data Breach Cases: A Review of Recent Trends*, NA (Nov. 9, 2015), http://www.bna.com/standing-data-breach-n57982063308/.
[155] *Id.*
[156] *In re Target Corp. Customer Data Security Breach Litigation, 66 F. Supp. 3d 1154 (D. Minn. 2014),*
[157] *Id.*

approximately 350,000 payment cards were infected by malware that was in the Neiman Marcus computer system.[158] Of those approximately 9,200 cards were used fraudulently. [159]The Seventh Circuit granted standing to the 9,200 and distinguished the case from *Clapper*.[160] The Court stated that plaintiffs in a data breach case are different from plaintiffs in a national security surveillance case as in *Clapper*.[161] The victims of the Neiman Marcus breach knew what was stolen whereas in Clapper plaintiffs' could not give evidence that there was injury. Additionally, the Court held there was an "objectively reasonable likelihood" that identity theft would occur and therefore that plaintiffs had standing; "Why else would hackers break into a store's database and steal consumers' private information?"[162]

V. ANALYSIS

As has been shown, recent, large-scale data breaches in healthcare are more prevalent than in other industries.[163] Financial institutions, retailers, and other organizations have all suffered major breaches, but the health care sector is an increasingly attractive target for hackers due to the economic benefit on the black market and the lax security.[164] Even the FBI has alerted the healthcare industry to the threats they are facing.[165] On April 8, 2014, the FBI sent private notices to healthcare providers, warning them that their cyber security systems are "lax" compared to other sectors, and are consequently making them vulnerable to attacks by hackers seeking PHI; "The healthcare industry is not as resilient to cyberintrusions compared to the financial and retail sectors, therefore the possibility of increased cyberintrusions is likely," said the FBI's private notice, obtained by Reuters news.[166] In another major report on the issue, the SANS Institute detailed the threat to the healthcare industry.[167] The SANS Institute is a private research and education cooperative that provides a global network of cyber security training, research and certification.[168] In this report, data specific to the health care sector collected between September 2012 and October 2013 was analyzed to determine the source and extent of cyber threat. As far as source of malicious traffic, this is the breakdown: (i) health care providers (72%); (ii) health care business associates (9.9%); (iii) other related health care entities (8.5%); (iv) health plans (6.1%); (v) pharmaceutical (2.9%); and (vi) health care clearinghouses (0 .5%).[169] The research revealed that a variety of devices, applications and systems can be

[158] *Remijas v. Neiman Marcus Group*, LLC, No. 14-3122 (7th Cir. 2015).
[159] *Id.*
[160] *Id.*
[161] *Id.*
[162] *Id.* at 9.
[163] Niam Yaraghi and Joshua Bleiburg, *The Anthem hack shows there is no such thing as privacy in the health care industry*, Brookings (Feb. 12, 2015), http://www.brookings.edu/blogs/techtank/posts/2015/02/12-anthem-hack-health-privacy.
[164] American Hospital Association, http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf (last visited April 9, 2016).
[165] *Id.*
[166] Jim Finkle, Exclusive: FBI warns healthcare sector vulnerable to cyber attacks, Reuters (Apr. 23, 2014), http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423.
[167] Barbara Filkins, *Healthcare Cyberthreat Report*, SANS ANALYST WHITEPAPER (SANS INSTITUTE) (February 2014), http://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735.
[168] *Id.*
[169] *Id.*

compromised, including "radiology imaging software, video conferencing systems, digital video systems, call contact software, security systems and edge devices such as VPNs, firewalls and routers."[170] "The data not only confirmed how vulnerable the industry had become, it also revealed how far behind industry-related cyber security strategies and controls have fallen."[171]

> The results of this analysis show that health care's critical information assets are poorly protected and are often compromised. Edge security and access systems, medical devices, video imaging systems and call centers have all been suborned in compromises that, in some cases, went on for the duration of the data collection period of 13 months. Providers, insurers, business partners and health care exchanges of all sizes were sending malicious traffic that was caught up in Norse's global threat intelligence sensors for issuing malicious, potentially illicit traffic. Many of the organizations sending the traffic are large entities that should have the resources to conduct the basic inventory, assessment and configuration controls needed to protect their systems from being compromised and used maliciously. This report, however, shows that the systems were compromised for long periods of time, and even when alerted to their system's actions, the organizations did not repair the vulnerabilities. The report is a snapshot of what's happening throughout the industry. This data shows that no health care organization is immune. Reports of breaches against health care organizations, large and small, continue to rise—as do the regulatory fines they are facing for the exposure of protected patient data. With new forms of health care taking hold, and more open exchanges of health care information between patients, insurers, doctors and pharmacists, these threats will only increase. The time to act is *yesterday*. Organizations must become aware of the many attack surfaces in their organizations and follow best practices for configuring these systems and monitoring them for abuse.[172]

There are numerous reasons why healthcare has been slow to prioritize data security. First, there is no mandate other than the HIPAA Security Rule, which gives latitude for implementation and imposes minimal penalties for failure to comply. Second, there is limited competition in the healthcare industry and a stable customer base. If your Target credit card account is breached you may stop shopping at Target. In healthcare, your insurance carrier or employer limits your choices. Third, the industry is operating on thin operating margins, due to ACA, which is changing payment models and creating other hoops for the healthcare organizations to jump through to obtain government reimbursement for its services; this creates more stress in an industry that already operates on small profit margins.[173] Finally, investing in a cyber security infrastructure is expensive; healthcare organizations are at the bottom of the pack when it comes to investing in data security.[174]

---

[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] Stephen Barlas, *Hospitals Struggle With ACA Challenges: More Regulatory Changes Are in the Offing in 2015*, Pharmacy and Therapeutics, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4159055/ (last visited April 2, 2016).
[174] Beth Kutscher, *Healthcare underspends on Cybersecurity as attacks accelerate, Modern Healthcare* (Mar. 3, 2016),
http://www.modernhealthcare.com/article/20160303/NEWS/160309922/healthcare-underspends-on-cybersecurity-

As discussed above, the HIPAA Security Rule has "required" and "addressable" standards.[175] Given the multitude of breaches and related costs, the concept of "addressable" needs to be revisited. The Security Rule and HITECH were both implemented prior to the explosion of the electronic medical record, the widespread connectivity of wireless devices or Internet of Things ("IoT") and the proliferation of the healthcare data breaches of recent years. The fact is the penalties and consequences for organizations that fail to protect our PHI are not a deterrent. If we look at the massive Anthem breach affecting almost 80 million people, the maximum penalty is $1.5 million.

> To put this in perspective, note that the net income of Anthem in 12 months ending in December 31st, 2014 was $2.5 billion. If Anthem were proven guilty of willful neglect, which is very unlikely, it could lose 0.00058 percent of its net income. Anthem makes that much money in one hour and 15 minutes. In a market where such major security breaches have little to no effect on the revenue stream of the organizations, there is no economic incentive to invest in digital security and prevent a data breach.[176]

Unlike consumers in other industries, healthcare consumers can't easily switch healthcare companies and are constrained by the limits of the healthcare plans of our employer or the government (provider networks, our employer, costs of going out of network, etc.). Additionally, healthcare consumers build relationships with providers who tend to work at certain hospitals or facilities. This is not the same model as buying products available at multiple stores.

The impact of implementing new ACA programs has had an uneven financial impact on hospitals.[177] An analysis of earnings reports for about 200 hospitals/health systems (whether public or not for profit), reported that notwithstanding a better economy, hospital margins that narrowed drastically during 2013.[178] The analysis reported an average operating margin in 2013 of 3.1%.[179] This was a decrease from 3.6% in 2012 and was based on data for 179 health systems.[180] Approximately 61.3% of the organizations in the analysis reported their operating margins decreased from the previous year.[181]

There is an inverse relationship; with cyber attacks on the rise healthcare providers are spending less than other industries when it comes to investments in protecting data.[182] While the government spends 16% of its IT budget on security, financial and banking institutions spend between 12% to 15%, healthcare providers average less than 6% of their IT budget expenditures on security, according to a survey by HIMSS Analytics and Symantec.[183] David Finn, Health IT Officer at Symantec says "We can't be as secure as those industries because we're not spending

---

as-attacks-accelerate.
[175] 45 CFR § 164.306(d).
[176] Yaraghi, *supra* at 163.
[177] Barlas, s*upra* at 173.
[178] *Id.*
[179] *Id.*
[180] *Id.*
[181] *Id.*
[182] Kutscher, *supra* at 174.
[183] *Id.*

the money. Information and information technology were never really strategic to healthcare. We never thought of that data as being strategic and important."[184] As the statistics show, healthcare attacks over the past five years have dramatically increased because the industry is an easy target and PHI is 50 times more valuable on the black market than financial information.[185] Despite this, 60% of healthcare boards of directors only get security updates on an as-needed basis, compared to the regular quarterly reports they get on financials and operations.[186] Finn continued "It's still very event-focused, it's very 'put out a fire as it comes in."[187] Unfortunately it is like a game of whack-a-mole, as you bat down one problem, another pops up. Due to new platforms, wearable devices and mobile applications, there are new points of entry and vulnerabilities that must be addressed.[188] Less than 50% of providers surveyed by HIMSS Analytics' had begun addressing potential security issues around medical devices, which can be used as a portal into a hospital's PHI.[189] Some vendors have begun to offer new technologies for cyber security to verify identity, such as using biometric scanning or voice activation to replace the easily compromised.[190] Iboss, a company providing solutions for thousands of organizations, service providers and government networks against cyber-threats, gives the following as reasons for the rise in healthcare data breaches:

- Not enough investment in cybersecurity: Healthcare profit margins have shrunk and some analysts estimate that as little as three percent of healthcare IT budgets are earmarked for security.

- Weak internal controls: Website The Big Read reports that Anthem failed to implement internal controls such as two-factor authentication, requiring that users change their passwords and controlling employee access to client PHI beyond the scope of their jobs. It is probably safe to say, Anthem isn't the only healthcare company to have these issues.

- Increase in hospital mergers: As hospital groups merge, IT systems are often overlooked or given low priority. The spate of mergers and acquisitions in recent years may have resulted in cyber security issues taking a backseat or falling through the cracks.

- High value of stolen healthcare credentials: The cost of healthcare and the millions that remain uninsured, despite the Affordable Care Act, means that health records have become a lucrative haul for data thieves. Also, as stolen credit card numbers flood the market, the value of healthcare data increases.

- Attacks are more sophisticated: Just as security vendors have strived to improve preventive measure for defending against targeted threats, criminal

[184] *Id.*
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Id.*

> hackers continue to refine their ability to bypass them. Stopping 100% of malware is no longer a realistic goal and hackers know they can find a way into a target if they are persistent.[191]

OCR statistics say based on their cumulative data, compliance issues investigated most are, in order of frequency: "(i) Impermissible uses and disclosures of protected health information; (ii) Lack of safeguards of protected health information; (iii) Lack of patient access to their protected health information; (iv) Use or disclosure of more than the minimum necessary protected health information; and (v) Lack of administrative safeguards of electronic protected health information."[192] Security Rule compliance is in the top 5 (lack of administrative safeguards of ePHI). During 2015 ABA Health law section webinar; an OCR representative highlighted some specific Security Rule compliance problems often seen during investigations, such as:

a. There was no risk analysis performed;
b. The risk analysis was not performed on an enterprise-wide basis, i.e. not all ePHI is caught and identified;
c. There was a failure to keep risk analyses current, i.e. to reflect changes in operations;
d. There was a failure to sufficiently address issues with mobile devices;
e. Either there was no risk management plan or if there was a risk management plan, there were issues with the implementation;
f. "Addressable" implementation standards were treated as optional—entities need good reason not to implement an addressable standard; and
g. The policies and procedures were merely a regurgitation of the rules and did not reflect the environment of the entity.[193]

This information is screaming that the current HIPAA Security Rule is not enough to protect patients' ePHI. Covered Entities are not self motivated to be proactive in this area. The Anthem breach provides the best support for this. According to a Wall Street Journal article, Anthem "doesn't expect the incident to affect its 2015 financial outlook, primarily as a result of normal contingency planning and preparation."[194] What is the message when a major security breach has no effect on the financial status of the organization and "normal contingency planning" can handle a data breach affecting 80 million people? Obviously protecting PHI is not a top priority and the consequences of losing control of the data are a mere cost of doing business.

---

[191] Iboss Cybersecurity Team, *Rise in healthcare Data Breaches in 2015 threatens HIPAA Compliance*, (Jan. 7, 2016), http://blog.iboss.com/executives/rise-in-healthcare-data-breaches-in-2015-threatens-hipaa-compliance

[192] U.S. Dept. of Health and Human Services, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[193] Joshua Sutin, Jillian Gordon Foerster, HIPAA Security Rule: What you need to know about Compliance and OCR's enforcement efforts, Inside Counsel (Jun. 24, 2015). http://www.insidecounsel.com/2015/06/24/hipaa-security-rule-what-you-need-to-know-about-co?page=3&slreturn=1459271898.

[194] Anna Wilde Matthews & Danny Yadron, *Health Insurer Anthem Hit By Hackers*, WALL ST. J. (Feb. 4, 2015), http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720.

VI. BOARD OVERSIGHT

Because the risk of cyber security breach is on the radar of most companies, Boards need to focus and understand the nuances of this problem, including their role in overseeing this issue.[195] Due to an increased use of mobile devices, social media and cloud usage; the growth of the Internet of things a/k/a IoT or smart consumer products with Internet connectivity, attention to cyber security threats must be the new reality.[196] There have been reports of several smart appliances (including televisions and at least one refrigerator) used a portal to initiate a large-scale cyber attack utilizing malicious emails.[197]

Cyber security breaches can create significant financial and reputational damage.[198] Estimates calculate the average total cost to a US company from a data breach is in the ballpark of $5.4 million.[199] This does not include resulting collateral damage, such as loss of confidence by consumers, regulatory action, potential for litigation, damage to reputation and for public companies impact on the stock price.[200] Boards must also be aware that the FTC can bring action in addition to the OCR or DOJ; By 2014, the FTC brought over 40 regulatory actions for "unfair or deceptive acts" against companies for failure to prevent unauthorized access to consumers' personal information.[201] To settle these, companies may enter consent decrees for up to 20 years mandating better data security programs and annual independent audits.[202] Additionally, individual States may have their own unfair and deceptive trade practices acts that provide a private cause of action and cyber security breaches may give rise to negligence and breach of contract claims.[203] The stakes are very high.

So what's a Board to do? In managing corporate affairs, there is the obligation to protect corporate assets.[204] These include the "confidential and proprietary information, reputation and goodwill" of the organization; including the systems used to manage risks to the organization's business operations.[205] Although cyber security is a top concern for the Board, surveys of directors indicate many Board members do not feel equipped to deal with it because they lack the "technical" experience.[206] However if there is appropriate expertise on the management team and the Board is being advised regularly, this should not be an issue.[207] The Board's focus should be on big picture items such as policies and processes that mitigate risks related to cyber security. For example, ensuring that employees are educated and there are adequate corporate resources

[195] Holly J. Gregory, *Board Oversight of Cybersecurity Risks*, Practical Law (March 2014), http://www.sidley.com/~/media/files/newsinsights/publications/2014/03/board-oversight-of-cybersecurity-risks/files/view-article/fileattachment/board-oversight-of-cybersecurity-risks--march-2014.pdf, page 24.
[196] *Id.* page 25.
[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] *Id.*
[201] *Id.*
[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.*

for cyber security are valid concerns for the Board.[208] Ultimately, Board decisions will be viewed against their fiduciary standards of care, i.e. loyalty and good faith in dealings.[209]

In addition to the general principles of risk oversight that should govern the Board's efforts relating to cyber security issues, Boards can also utilize the guidance provided by the recently released the Cyber security Framework ("CSF") in addressing the company's risk management of cyber security issues.[210] NIST promulgated CSF pursuant to President Obama's Executive Order 13636, titled Improving Critical Infrastructure Cyber security, which required NIST to develop a voluntary standards and best practices to reduce risks to the nation's "critical infrastructure," i.e. physical or virtual systems deemed so "vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these areas."[211] See http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Companies, in assessing their cyber security program can utilize CSF as a benchmark. CSF has five core functions:

- Identify cyber security risks and vulnerabilities. Companies should develop the institutional understanding to manage cyber security risks to organizational systems, assets, data and capability.
- Protect critical infrastructure assets. Companies should develop and implement the appropriate safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure services.
- Detect the occurrence of a cyber event. Companies should develop and implement the appropriate activities to identify the occurrence of a cyber security event.
- Respond to a detected event. Companies should develop and implement the appropriate activities, prioritized through the organization's risk management process (including effective planning), to take action regarding a detected cyber security event.
- Recover from a cyber event. Companies should develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a cyber security event.[212]

Although adopting CSF is voluntary, it may become a reference for regulators, insurance companies and the plaintiffs' in assessing whether an organization took reasonable steps to mitigate cyber security risks.[213] In a survey conducted by PricewaterhouseCoopers LLP, companies that detected more security incidents and had less financial loss per incident, shared certain similarities: (i) they had an IT strategy; (ii) They had a chief information officer who reported to the CEO or similar level position; (iii) within the last year they had evaluated the effectiveness of their security plan; and (iv) they had an understanding of any security events that

[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] *Id.*
[213] *Id.*

happened in the last year. [214] Accordingly, to address cyber security risks, Boards should: (i) make sure they have enough information about the organization's IT system and cyber security, (ii) make sure enough time is reserved on the Board agenda to discuss cyber security; (iii) discuss whether it is appropriate to have a Board member with a high level of understanding of cyber security issues; (iv) obtain updates regularly; (v) make sure there are adequate resources to manage cyber security; (vi) review and understand the crisis management plan for a breach and (vi) consider insurance specifically for a cyber security breach. [215] Commercial insurance policies do not necessarily cover data theft or other consequences of a data breach. [216] Cyber security insurance may cover things such as breach notification costs, business interruption and lost revenue, ransom payments due to cyber extortion and costs due to defending claims, and payment of settlement and damages. [217]

Underscoring the importance of the Board's role in healthcare organizations, the OIG issued a guidance document recently to assist Board members in understanding how to be fully engaged in their oversight responsibilities.[218] In one section entitled "Encouraging Accountability and Compliance" suggestions are made to guide Boards with compliance oversight, such as linking compliance goals to compensation. [219] The Guidance document also reiterates that OIG is increasingly requiring certifications of compliance from managers outside of the compliance department.[220] Suggesting executives should have some skin in the game to take compliance matters more seriously may be the jumpstart the healthcare industry needs to step up the efforts in security of ePHI.[221]

VII. BEST PRACTICES

The DOJ Cybersecurity Unit has issued a document detailing best practices to deal with a potential cyber attack and best responses if an attack occurs. [222] It includes a "Cyber Incident Preparedness Checklist:"

Before a cyber attack or intrusion include (i) identify mission critical data and assets (i.e., your "Crown Jewels") and institute tiered security measures to appropriately protect those assets; (ii) review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework; (iii) create an actionable incident response plan and test plan with exercises and keep plan current to reflect changes in personnel and

[214] *Id.*
[215] *Id.*
[216] *Id.*
[217] *Id.*
[218] U.S. Dept. of Health and Human Services, http://oig.hhs.gov/compliance/compliance-guidance/docs/Practical-Guidance-for-Health-Care-Boards-on-Compliance-Oversight.pdf (last visited April 10, 2016).

[219] *Id.*
[220] *Id.*
[221] *Id.*
[222] U.S. Department of Justice Cybersecurity Unit, *Best Practices for Victim Response and Reporting of Cyber Incidents* (April 2015), https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf.

structure; (iv) have the technology in place (or ensure that it is easily obtainable) that will be used to address an incident; (v) have procedures in place that will permit lawful network monitoring; (vi) have legal counsel that is familiar with legal issues associated with cyber incidents ; (vii) align other policies (e.g., human resources and personnel policies) with your incident response plan; and (viii) develop proactive relationships with relevant law enforcement agencies, outside counsel, public relations firms, and investigative and cyber security firms that you may require in the event of an incident. [223]

During a Cyber Attack or Intrusion: (i) make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch; (ii) minimize continuing damage consistent with your cyber incident response plan; (iii) collect and preserve data related to the incident, "Image" the network and keep all logs, notes, and other records, keep records of ongoing attacks; (iv) consistent with your incident response plan, notify: appropriate management and personnel within the organization, law enforcement, other possible victims, Department of Homeland Security; (v) do not use compromised systems to communicate or "hack back" or intrude upon another network.[224]

After Recovering from a Cyber Attack or Intrusion: (i) continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network; and (ii) conduct a post-incident review to identify deficiencies in planning and execution of your incident response plan. [225]

VIII. CONCLUSION

In conclusion, there are multiple ways to address the increasing problem of data breaches within the healthcare industry and the resulting consequences for patients, healthcare organizations and the nation. Being proactive, investing resources, having Board oversight, linking compliance and management accountability to compensation, and purchasing cyber insurance are some of the obvious ones. Better enforcement of existing laws and increasing penalties to actually deter cyber criminals are other ways to begin to pull the reins in on cyber criminals. Finally, amending the HIPAA Security rule to mandate the current "addressable" standards and bring the technical requirements in line with the NIST standards, i.e. Cybersecurity Framework is mission critical in stopping the epidemic of data breaches in the healthcare industry. An amended HIPAA Security Rule may include safe harbors or mitigation of certain penalties for those organizations that encrypt their data and follow NIST standards. But ultimately an overall requirement to implement all standards, including the currently addressable is necessary to move providers to better protect ePHI.

[223] *Id.*
[224] *Id.*
[225] *Id.*

About the Author

Diane Doebele Koch (Hall) graduated from Fordham University School of Law in 1992 and practiced entertainment and corporate transactional law for twenty years in NYC and Florida prior to obtaining her RN license in February 2012 & BSN in May 2014. She will receive an LL.M. in healthcare law from Loyola University Chicago in May 2016. Her areas of interest are HIPAA/privacy, end of life ethics and quality issues in healthcare. Diane is licensed to practice law in New York and Florida and currently resides in the Clearwater, Florida area.

EXHIBIT A: 45 CFR Part 164, Subpart C, Appendix A to Subpart C of Part 164 - Security Standards: Matrix[226]

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	
		Risk Analysis (R); Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation

[226] Cornell University Law School, https://www.law.cornell.edu/cfr/text/45/part-164/subpart-C/appendix-A (last visited March 22, 2016).

		Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

EXHIBIT B: STATE PRIVACY LAWS[227]

State	Citation
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. § 36a-701b, 2015 S.B. 949, Public Act 15-142
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 *et seq.*
Idaho	Idaho Stat. §§ 28-51-104 to -107
Illinois	815 ILCS §§ 530/1 to 530/25
Indiana	Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 et seq.
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. §§ 51:3071 *et seq.*, 40:1300.111 to .116
Maine	Me. Rev. Stat. tit. 10 § 1347 *et seq.*
Maryland	Md. Code Com. Law §§ 14-3501 *et seq.*, Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass. Gen. Laws § 93H-1 *et seq.*
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -

[227] National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited March 28, 2016).

	C:21; 189:66
New Jersey	N.J. Stat. § 56:8-161, -163
New York	N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat §§ 75-61, 75-65
North Dakota	N.D. Cent. Code §§ 51-30-01 *et seq*., 51-59-34(4)(d)
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166
Oregon	Oregon Rev. Stat. § 646A.600 to .628, 2015 S.B. 601, Chap. 357
Pennsylvania	73 Pa. Stat. § 2301 *et seq.*
Rhode Island	R.I. Gen. Laws § 11-49.2-1 *et seq*., 2015 S.B. 134, Public Law 2015-138, 2015 H.B. 5220, Public Law 2015-148
South Carolina	S.C. Code § 39-1-90, 2013 H.B. 3248
Tennessee	Tenn. Code § 47-18-2107; § 8-4-119 (2015 S.B. 416, Chap. 42)
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053; Tex. Ed. Code § 37.007(b)(5); Tex. Pen. Code § 33.02
Utah	Utah Code §§ 13-44-101 *et seq.*; § 53A-13-301(6)
Vermont	Vt. Stat. tit. 9 § 2430, 2435
Virginia	Va. Code § 18.2-186.6, § 32.1-127.1:05, § 22.1-20.2
Washington	Wash. Rev. Code § 19.255.010, 42.56.590, 2015 H.B. 1078
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. § 40-12-501 *et seq.*
District of Columbia	D.C. Code § 28- 3851 *et seq.*
Guam	9 GCA § 48-10 et seq.
Puerto Rico	10 Laws of Puerto Rico § 4051 *et seq.*
Virgin Islands	V.I. Code tit. 14, § 2208