Cyber Health Crisis: How to Manage the Risk

By Jennifer L. Rathburn, Christopher B. Evans, and Joseph S. Abrenio[1]

[1]The authors would like to thank Jennifer J. Hennessy, Rachel H. Bryers, Elizabeth R. Gebarski, and Samuel A. Magnuson of Quarles & Brady LLP for their work on this article.

I. Introduction

Cybersecurity is a rapidly growing concern for all organizations due to the increasing frequency of cyber attacks by cyber criminals, hacktivists, and nation-states. Almost weekly, the media reports a high-profile data breach. These attacks, previously perpetrated against financial institutions and the retail industry, have shifted their focus to the health care industry. In 2014, the Federal Bureau of Investigation (FBI) expressed concern that the health care industry was a prime target for increased cyber attacks by criminals.[2] Specifically, the FBI warned health care providers that their cybersecurity systems were not as robust as in other sectors, like the financial and retail industries, leaving them vulnerable to cyber intrusions.[3] The FBI further noted that electronic health records (EHR) are especially valuable on the black market and can be used to "file fraudulent insur-

[2]*Private Industry Notification: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

[3]*Private Industry Notification: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain.*

ance claims, obtain prescription medication, and advance identity theft."[4]

The FBI's concern is supported by recent Ponemon Institute studies, which found that cyber attacks were the number one cause of data breaches for the health care industry in both 2014 and 2015.[5] The number of health care organizations surveyed that reported experiencing a criminal attack[6] increased from 45% in 2014 to 50% in 2015.[7] Remarkably, between 2010 and 2015, cyber attacks on the health care industry spiked over 125%, with the average cost for a data breach per health care record rising to $398 in 2015.[8] Over the last two years, data breaches in the health care industry were the result of theft, hacking, or unauthorized disclosures of protected health information (PHI).[9] In 2016, ransomware, malware, and denial-of-service (DOS) attacks are the top cyber threats facing health care organizations.[10] Health care organizations must be aware that the cause of data breaches in the health care industry has shifted from accidental intrusions to intentional cyber attacks.[11]

The trend of intentional cyber attacks against the health care industry, however, is not just limited to cyber criminals.

---

[4]*Private Industry Notification: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain.*

[5]Ponemon Inst., Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data 1 (2016); Ponemon Inst., Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data 1 (2015).

[6]Ponemon Inst., Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data 1.

[7]Ponemon Inst., Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data 1 (2016); Ponemon Inst., Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data 1 (2015).

[8]Ponemon Inst., Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data 1 (2015); Ponemon Inst., 2015 Cost of Data Breach Study: United States 7 (2015).

[9]*Monthly Healthcare Data Breach Report: Aug 2015*, HIPAA Journal (Aug. 2015), http://www.hipaajournal.com/wp-content/uploads/2015/09/hipaajournal-healthcare-data-breach-report-august-20151.png.

[10]Ponemon Inst., Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data 2 (2016).

[11]Ponemon Inst., Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data 1 (2016).

The Community Health Systems data breach in 2014 marked the first state sponsored cyber attack against the health care industry.[12] Similar to state sponsored attacks seen in other industries, so too are cyber attacks against the health care industry aimed at the theft of intellectual property while also uniquely targeting patient health records.

The reason for the shift is simple: stolen health care information is lucrative. Security researchers found that health care data is far more valuable than stolen payment card information because banks are quicker to shut down compromised cards, decreasing the lifespan of stolen payment card credentials.[13] Health care information, however, can now be sold on the black market for $50 for a single record according to the FBI, compared to a single credit card account worth $1.[14] The discrepancy in value is due to the relative immutability of Social Security numbers and prescription information, as well as the health care industry's lack of methodology for minimizing damages caused by stolen health care records, in comparison to the banking sector's defined procedures for fixing fraudulent transactions.

The concern of cyber attacks have been amplified because health care organizations are relying more heavily on technology to collect and share health care data. From the adoption of EHRs and patient portals to the increased use of cloud solutions, telemedicine, mobile medical applications,[15] medical devices, and fitness trackers, the security of data is

---

[12]*Risks and Cyber Threats to the Healthcare Industry*, Infosec Inst. (Sept. 16, 2014), http://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry/.

[13]*Hackers Selling Healthcare Data in the Black Market*, Infosec Inst. (July 27, 2015) http://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/.

[14]Fahmida Rashid, *Why Hackers Want Your Health Care Data Most of All*, Infoworld (Sept. 14, 2015), http://www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html.

[15]The use of mobile apps in the health care field has skyrocketed in recent years as providers and health plans have recognized the benefit of this technology to improve health outcomes. The OCR has noticed this increase as well and has launched a new platform for health care mobile app developers and other parties interested in the interplay between health information technology and HIPAA privacy protection. The OCR will consider the input provided on this platform in developing its guid-

becoming even more essential to patient care and safety. As stated in a 2014 report from the Executive Office of the President, "[w]e live in a world of near-ubiquitous data collection."[16] The collection and use of health care data for research, product development, monetization, payment, health care operations, and treatment purposes is part of everyday operations for health care organizations. Such big data collection and the interconnectivity of health care devices and systems through health information exchanges/organizations (HIE/HIOs) by accountable care organizations (ACOs) to the Internet of things (IoT) only further underscores the need to implement cybersecurity measures to protect health care data.

The health care industry is also facing increasing legal and regulatory pressures to safeguard data. As discussed in the following sections, federal and state regulators are imposing significant penalties on health care organizations that fall victim to data breaches when such organizations have not implemented adequate security programs.

For all of these reasons, health care organizations must focus more heavily on preparing for and responding to cyber attacks as they are rich targets for cyber predators. While it may be impossible to prevent all cyber attacks, health care organizations must make every effort to implement reasonable measures to identify, protect, detect, respond, and recover from a data breach. The measures an organization takes to prepare and respond to a data breach will affect the public's perception of the organization and likely influence the potential penalties, fines, and costs that could result.

This article will provide health care organizations with the critical information to implement an effective cybersecurity program. The following sections will discuss (1) current health care industry threat actors; (2) how to build an effective cybersecurity program; (3) potential applicable security laws, frameworks, and guidance; (4) how to conduct a risk analysis; (5) how to handle a data security event and related

---

ance and technical assistance efforts, with the overall goal being to better protect the privacy and security of individuals' data used in these technologies. The platform is available here: http://hipaaqsportal.hhs.gov/.

[16] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big__data__privacy__report__may__1__2014.pdf.

practical considerations; (6) common pain points and cybersecurity best practices; (7) the value of table top exercises and penetration testing; (8) cyber threat information sharing; (9) health care board duties regarding cybersecurity; and (10) an overview of cyber-related potential penalties and enforcement actions.

II. Health Care Industry Threat Actors

As detailed above, the health care industry is being targeted by state sponsored actors, foreign intelligence services, cyber criminals, and negligent insiders. These cyber attacks were enabled by aging infrastructure. Below is a description of recent and notable breaches.

A. State Sponsored Attacks

- **Community Health Systems (CHS) Network Compromise/Malware:** A health care system, operating 207 hospitals in 29 states, suffered a data breach in August 2014, which exposed 4.5 million patient records and other sensitive personal information.[17] This cyber attack was attributed to a Chinese hacking team called Advanced Persistent Threat Gang (APT).[18] CHS described the attack as one involving "highly-sophisticated malware and technology"[19] in its Security and Exchange Commission 8-K filing.
- **Anthem, Inc. (Anthem) Spear Phishing:** The second-largest insurance provider in the United States suffered a data breach in 2015 that exposed the sensitive personal information of over 80 million customers and

[17]Bill Hardekopf, *The Big Data Breaches of 2014*, Forbes (Jan. 13, 2015), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

[18]Michael Mimoso, *APT Gang Branches Out to Medical Espionage in Community Health Breach*, Threat Post (Aug. 19, 2014), https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828/.

[19]Mimoso, *APT Gang Branches Out to Medical Espionage in Community Health Breach.*

employees.[20] Anthem discovered the breach on January 29, 2015,[21] but it is likely that the attack was initiated several months earlier in April 2014.[22] The attack has been attributed to a Chinese state sponsored hacking group named "Deep Panda."[23] Investigators believe that the group created a fake domain, "we11point.com," which resembled Anthem's domain "wellpoint.com" (the insurance provider changed its name from WellPoint to Anthem in late 2014) to steal employee credentials.[24] Then, Deep Panda used the fruits of its phishing operation to gain access to Anthem's systems and launched the attack.[25]

- **Premera Blue Cross Spear Phishing:** Another insurance provider experienced a data breach last year that compromised the PHI and financial data of 11 million people.[26] Although the breach was discovered in January 2015,[27] upon further investigation into the breach, it was revealed that the attackers infiltrated

---

[20]*Giant US Health Data Breach Could Lead to China*, Business Insider (Feb. 5, 2015), http://www.businessinsider.com/afp-giant-us-health-data-breach-could-lead-to-china-2015-2.

[21]Cynthia Larose & Kevin M. McGinty, *The Anthem Data Breach: The Fallout and What's Next*, Privacy & Security Matters (Feb. 10, 2015), http://www.privacyandsecuritymatters.com/2015/02/the-anthem-data-breach-the-fallout-and-whats-next/.

[22]*Anthem Breach May Have Started in April 2014*, Krebs On Security (Feb. 9, 2015), http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/.

[23]*Anthem Breach May Have Started in April 2014*.

[24]*Anthem Breach May Have Started in April 2014.*

[25]Brandon Bailey, *Anthem Hackers Tried To Breach System As Early As December*, Huffington Post (last updated Apr. 8, 2015), http://www.huffingtonpost.com/2015/02/06/anthem-hackers-december__n__6634440.html.

[26]Tara Seals, *Premera Slapped with 5 Lawsuits Over Data Breach*, Infosecurity Magazine (Apr. 3, 2015), http://www.infosecurity-magazine.com/news/premera-slapped-with-5-lawsuits/.

[27]Jose Pagliery, *Premera Health Insurance Hack Hits 11 Million People*, CNN (Mar. 17, 2015), http://money.cnn.com/2015/03/17/technology/security/premera-hack/index.html.

Premera's network in May 2014.[28] While it has not yet been definitively proven, security experts believe that the same group responsible for the Anthem attack is also responsible for the Premera attack.[29] Like the Anthem attack, a fake Web domain "prennera.com" was created to steal employee credentials.[30] Several weeks prior to the discovery of the breach, federal auditors warned Premera that its network-security procedures were inadequate.[31] In addition to the warning, officials provided Premera with 10 recommendations on how to improve their security procedure, which the insurance provider allegedly failed to implement.

B. Criminal Attacks

Criminal actors also increasingly target health care organizations for financial gain, and the following are examples of recent criminal cyber attacks against the health care industry using a variety of attack vectors.

- **UCLA Health Systems (UCLA) Lack of Preventative Measures/Network Compromise:** After noticing suspicious activities on one of its systems in October 2014, UCLA launched an investigation aided by the FBI.[32] On May 5, 2015, UCLA discovered that attackers had infiltrated its network, gaining access to unen-

---

[28]*Premera Blue Cross Breach Exposes Financial, Medical Records*, Krebs on Security (Mar. 17, 2015), https://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/.

[29]Jeremy Kirk, *Premera, Anthem Data Breaches Linked By Similar Hacking Tactics*, Computerworld (Mar. 18, 2015), http://www.computerworld.com/article/2898419/data-breach/premera-anthem-data-breaches-linked-by-similar-hacking-tactics.html.

[30]Kirk, *Premera, Anthem Data Breaches Linked By Similar Hacking Tactics.*

[31]Tara Seals, *Premera Slapped with 5 Lawsuits Over Data Breach*, Infosecurity Magazine (Apr. 3, 2015), http://www.infosecurity-magazine.com/news/premera-slapped-with-5-lawsuits/.

[32]Chad Terhune, *UCLA Health System Data Breach Affects 4.5 Million Patients*, Los Angeles Times (July 17, 2015), http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html.

crypted patient information.[33] The data breach, which was initiated in September 2014, exposed the sensitive personal information of 4.5 million patients.[34]

- **Medical Informatics Engineering Third-Party Breach:** On May 26, 2015, the medical software company discovered that attackers infiltrated its cloud service "nomoreclipboard" exposing the PHI and sensitive information of 3.9 million Americans.[35] The investigation into the data breach revealed that the attack was initiated 19 days earlier on May 7, 2015.[36]
- **Seton Healthcare Spear Phishing:** On February 26, 2015, the family of hospitals discovered that the PHI and sensitive information of 39,000 patients had been exposed in a data breach.[37] The attackers used a phishing operation to steal the credentials of hospital staff and infiltrate Seton's e-mail system.[38]

Due to the increase in cyber attacks, health care organizations recognize the inevitability of these threats and have begun to implement cybersecurity programs. The following sections will provide practical guidance to organizations on how to build an effective cybersecurity program that incorporates the HIPAA Security Rule and other relevant security frameworks and guidance.

III. Building an Effective Cybersecurity Program

To understand and defend against the threat, it is critical

---

[33]Terhune, *UCLA Health System Data Breach Affects 4.5 Million Patients.*

[34]Terhune, *UCLA Health System Data Breach Affects 4.5 Million Patients.*

[35]*Medical Informatics Engineering Hack Exposed Data on 3.9 Million People*, NBC News (Aug. 3, 2015), http://www.nbcnews.com/tech/security/medical-informatics-engineering-hack-exposed-data-3-9-million-people-n403351.

[36]*Medical Informatics Engineering Hack Exposed Data on 3.9 Million People.*

[37]*Seton Family of Hospitals Announces 39K HIPAA Breach*, HIPAA Journal (Apr. 26, 2015), http://www.hipaajournal.com/seton-family-of-hospitals-announces-39k-hipaa-breach-2353/.

[38]*Seton Family of Hospitals Announces 39K HIPAA Breach.*

to consider the most important and vulnerable "attack surfaces" of health care organizations. These include the transaction attack surface, intellectual property attack surface, supply chain attack surface, and people/mobile attack surfaces.[39] Moreover, the dramatic increase in the use of EHRs to store PHI, which is considered "data at rest," and the increase in connectivity between health care entities, from hospitals to primary care physicians (PCP) to pharmacies, payors, and others, considered "data in motion," have multiplied the access points a malicious actor may be able to exploit. This focus on interconnected technology to promote the continuum of care has resulted in the exponential increase of potential attack surfaces in the health care industry.

An effective cybersecurity program mitigates the risk from cyber incidents, focusing on the organization's threat surface and the types of attacks most effective against these threat surfaces. Such a program requires a commitment in two areas: Strategy and Operations. Moreover, a robust cybersecurity program requires resources. Remarkably, a recent study found that the health care industry allocates an average of just 14% a year of their IT budgets to cybersecurity.[40] Those organizations that do devote resources to cybersecurity often spend a significant amount of time in the Operations area, for example, implementing boundary defenses and monitoring an intrusion detection system, while neglecting the Strategy area. Organizations should consider a more balanced approach to mitigating cyber risk involving the following:

---

[39]Randy Hayes, *2014 Health Industry Threat Landscape Briefing*, Health Info. Trust Alliance (2014), https://hitrustalliance.net/content/uploads/2014/03/2014-Health-Industry-Threat-Landscape-Briefing.pdf.

[40]Harriet Taylor, *US Health Care Way Behind On Data Security, Says Forrester*, CNBC (Nov. 12, 2015), http://www.cnbc.com/2015/11/11/us-health-care-way-behind-on-data-security-says-forrester.html.

Strategic Efforts		Operational Efforts
● Define relevant, current, and emergent threats to business; ● Develop organization-wide security strategy or framework; ● Understand current security operations and process maturity; ● Define and implement needed levels of information asset protection; and ● Educate and inform executive/board level decision making.		● Organize people, process, and technology to meet threats; ● Conduct monitoring, detection, analysis, and response activities; ● Find and address vulnerabilities; ● Meet compliance and regulatory requirements and standards; and ● Perform audit functions.

As a starting point, an organization-wide security strategy should be identified through the selection and commitment to a cybersecurity "framework." This framework can help the organization understand the scope of activities it should perform as part of its security program, as well as conduct a risk/reward justification to determine the appropriate level of investment to meet risk mitigation goals.

Once a framework is selected, organizations should begin the cyber risk management process with a clear understanding of the goals and objectives for the security program. A "desired state" defines the level of desired risk mitigation and commitment of resources. The next step is to understand how the security program currently operates through use of a risk analysis. The analysis seeks to identify threats, vulnerabilities, and impacts, as well as the current state of security controls and operational maturity. Operational maturity is a measure of how effective the combination of people, processes, and technology are in preventing, detecting, and responding to cyber incidents. The difference between the desired state and the current state becomes the basis for a set of recommendations to tune the security approach within the organization.

The recommendations are a way to invest in, and reprioritize current investments in, cybersecurity practices within a health care organization. As indicated above, many organizations over-invest in certain security functions while underinvesting in others. For example, organizations may spend a significant amount of resources monitoring the boundary of its network yet ignore monitoring the internal network. A balanced approach is necessary for an effective cybersecurity program, and the plan of action should consider areas for increased focus or investment, as well as areas for decreased focus or investment.

As the recommendations are implemented, it is imperative for organizations to reassess the effectiveness (through conducting another risk analysis) and adjust the implementation strategy accordingly. This keeps the security strategy up to date, accounts for emergent risk, and continually ensures the investment in the cybersecurity program is appropriate.

IV. Potential Applicable Security Laws, Frameworks, and Guidance

A critical step health care organizations should take in developing a cybersecurity program is to determine the federal, state, or local laws or regulations that apply to them. For instance, most health care organizations are required to comply with the HIPAA Security Rule. Depending on the specific business and size of a health care organization, other

optional frameworks and guidance, such as the NIST Cybersecurity Framework, ISO 27001, and HITRUST Common Security Framework, may also be appropriate to consider. These frameworks can also help implement the requirements under the HIPAA Security Rule. In addition, health care organizations should be aware that the recent Cybersecurity Act of 2015 requires the Secretary of the Department of Health and Human Services (HHS) to develop voluntary cybersecurity guidance for the health care industry.[41]

Until we get further guidance from HHS, health care organizations should consider adopting other security frameworks and guidance depending on the specific services they provide. For example, entities that store, process, or transmit payment cardholder data must be aware of applicable Payment Card Industry Data Security Standard (PCI DSS) requirements. In addition, medical device manufacturers should evaluate whether to follow the Food and Drug Administration's (FDA) voluntary guidance regarding cybersecurity and medical devices, entitled "Content of Premarket Submissions for Management of Cybersecurity in

---

[41] Cybersecurity Act of 2015, H.R. 2029, 114th Cong. Division N § 405 (2015)

(The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that—

(A) serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) are consistent with—

(i) the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)(15));

(ii) the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note); and

(iii) the provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111-5), and the amendments made by such Act; and

(D) are updated on a regular basis and applicable to a range of health care organizations.)

Medical Devices" and "Postmarket Management of Cybersecurity in Medical Devices." Also, FDA regulated entities, with some exceptions, must be aware of the requirements set forth in 21 C.F.R. Part 11 regarding security controls for electronic records.[42] The following sections discuss some of these laws, frameworks, and guidance in further detail.

A. HIPAA Security Rule

The HIPAA Security Rule, set forth in 45 C.F.R. Part 164, subparts A and C, establishes standards to protect individuals' electronic protected health information (ePHI) that is created, received, maintained, or transmitted by a covered entity or business associate. The Security Rule requires that covered entities and business associates implement appropriate administrative, physical, and technical safeguards, documented in policies and procedures, to ensure the confidentiality, integrity, and security of ePHI. The administrative, physical, and technical safeguards are enumerated in 45 C.F.R. §§ 164.308, 164.310, and 164.312, respectively.

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 the HIPAA Security Rule.[43] In deciding which security measures to implement, the HIPAA Security Rule requires the covered entity or business associate to 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; and (iv) the probability and criticality of potential risks to ePHI.[44]

Each HIPAA Security Rule standard has implementation

---

[42]Generally, 21 C.F.R. Part 11 requires regulated entities to implement certain procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records. For further detail, refer to *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures—Scope and Application*, U.S. Dept. of Health & Human Servs. (Aug. 2003), http://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm125125.pdf.

[43]45 C.F.R. § 164.306(b)(1).

[44]45 C.F.R. § 164.306(b)(2).

specifications that are either "required" or "addressable." For example, the device and media controls standard contains two required implementation specifications (regarding disposal of ePHI and hardware and media reuse) and two addressable implementation specifications (regarding maintaining a record of the movements of hardware and electronic media and any person responsible for such media and data backup and storage).[45] When a standard includes required implementation specifications, the covered entity or business associate must implement the implementation specifications.

In contrast, when a standard includes addressable implementation specifications, a covered entity or business associate must assess whether each implementation specification is a reasonable and appropriate safeguard in its environment when analyzed with reference to the likely contribution to protecting ePHI. Importantly, "addressable" does not mean optional. If the implementation specification is reasonable and appropriate, the covered entity or business associate must implement the implementation specification. If implementing the implementation specification is not reasonable and appropriate, the covered entity or business associate must document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate.[46]

The HIPAA Security Rule standards or implementation specifications include, for example, encryption (which is addressable but highly recommended by OCR commentary),[47] security awareness training, security incident policies and procedures to identify and respond to suspected or known security incidents and mitigate harmful effects, audit controls to regularly review and record information system activity,

---

[45] 45 C.F.R. § 164.310(d).

[46] 45 C.F.R. § 164.306(d).

[47] *See, e.g.*, press release from Susan McAndrew, OCR's former Deputy Director of Health Information Privacy, stating, "Covered entities and business associates must understand that mobile device security is their obligation. Our message to these organizations is simple: encryption is your best defense against these incidents." *Stolen Laptops Lead to Important HIPAA Settlements*, HHS.Gov (April 22, 2014), https://wayback.archive-it.org/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422b.html.

access controls to ensure appropriate access to ePHI, authorization procedures to verify that the person or entity seeking access to ePHI is appropriate, and integrity controls to protect ePHI from improper alteration or destruction. One particularly important implementation standard, the risk analysis, is specifically discussed in detail in section V below.

B. NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) developed a cybersecurity framework, "Framework for Improving Critical Infrastructure" (CSF), to help organizations determine the level of investment in security needed to provide a defined level of maturity.[48] The NIST CSF is a voluntary, risk-based approach to manage cybersecurity risk in a cost-effective manner. The framework is not a regulation; therefore, there is no compliance requirement to it. However, the CSF provides a structured methodology for organizations to manage risk and determine an appropriate level of investment in security.[49]

The NIST CSF defines a set of activities that organizations can implement as part of their security program. The CSF organizes these activities around Functions, Categories, and Subcategories/Activities. The five NIST CSF functions are:

- Identify
- Protect
- Detect
- Respond

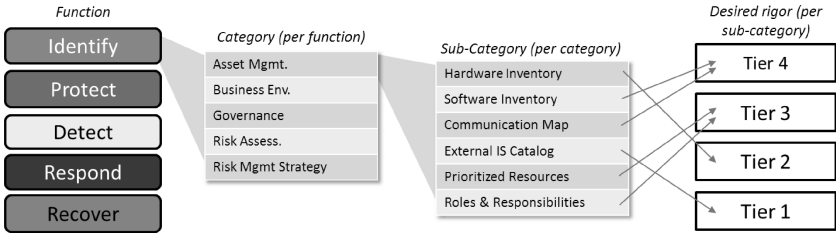
---

[48] *Framework for Improving Critical Infrastructure Cybersecurity*, Nat'l Inst. of Standards & Tech. (February 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[49] Please note the OCR recently released a mapping of the HIPAA Security Rule standards and implementation specifications to applicable NIST Cybersecurity Framework Subcategories. *See HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, Office for Civil Rights (Feb. 2016), http://www.hhs.gov/sites/default/files/NIST%20CSF%20to%20HIPAA%20Security%20Rule%20Crosswalk%2002-22-2016%20Final.pdf. Also, note that the Obama Administration endorsed the NIST CSF by basing the Precision Medicine Initiative's draft Data Security Framework on the NIST CSF. *Precision Medicine Initiative: Data Security Policy Principles and Framework*, White House (Feb. 25, 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/PMI__Security__Principles__and__Framework__FINAL__022516.pdf.

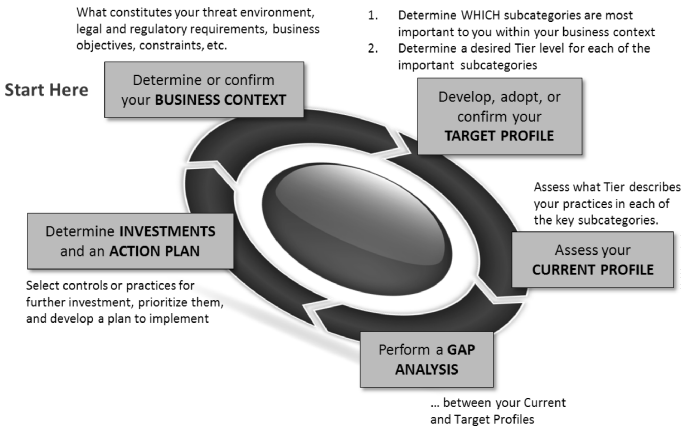
- Recover

Within each of the five functions, there are several categories, and each category has several activities associated with it, called subcategories. In the graphic below, for example, the Identify function has the categories of Asset Management, Business Environment, and Governance, among many other categories. The Asset Management category has several subcategories/activities, including Hardware Inventory, Software Inventory, and Communication Map, among others.



The NIST CSF becomes truly useful when organizations assign a desired rigor for each subcategory/activity. The tier rating specifies the level to which the organization desires a subcategory to be implemented and, by association, the resources it must expend to achieve that level of rigor.

A notional process for putting the NIST CSF into practice is shown in the figure below. It starts with understanding the business context for security, identifying security goals, and answering the question, "what do you need to protect your business from cyber risk?" The next two steps involve key components of the NIST CSF, the Target Profile and the Current Profile. A Target Profile defines where the organization needs to be from a security perspective and is based on the business context identified in the first step. The Current Profile defines how the organization currently does information security and is based on risk analyses. The Current Profile maps subcategories/activities to the tier (rigor) at which the activity is assessed. The Target Profile maps subcategories to the desired tier (rigor) for the activity. The difference between the Current Profile and Target Profile, as determined by the Gap Analysis in the next step, forms the basis for what the organization should implement for security. In the final step, the organization defines a plan of action regarding which controls to implement and the degree to which they should be implemented. At the end of the process, the organization has "fine-tuned" its security implementation to manage the desired level of risk.



C. ISO 27001

Formal information security frameworks provide a reasonable starting point for any cybersecurity program. Typically, frameworks range from all-encompassing (like ISO 27001) to more focused and less formal (e.g., CSC Top 20)—providing organizations several options for determining how much they want to "invest" in a security program.

ISO 27001 outlines an "Information Security Management System," or ISMS, which is comprised of policies, procedures, security controls, and the like.[50] A complete implementation of ISO 27001 requires organizations to prepare for and pass a certified audit of the standards. For large organizations, ISO 27001 as a framework may be more tenable than for smaller organizations. This is not a simple undertaking for any organization, and the benefits of being certified as ISO 27001 compliant should be weighed with the cost of the preparation and audit process.

ISO 27001 has 14 domains containing a number of controls for organizing an information security management system:

- **Information Security Policy**—are applicable policies defined, approved, published, and communicated to all staff?
- **Information Security Organization**—are roles and responsibilities for information security (e.g., operations, risk management, etc.) defined?
- **Human Resource Security**—do staff understand their responsibilities when it comes to information security?
- **Asset Management**—are information systems managed and controlled appropriately?
- **Access Control**—is access to facilities and information appropriately controlled and maintained?
- **Cryptography**—is information secured and encrypted with appropriate methods?
- **Physical and Environment Security**—are systems and facilities monitored and secured to prevent damage or disruption?
- **Operations Security**—are operating procedures like change management defined and implemented?

---

[50] *See ISO/IEC 27001-Information Security Management*, ISO.Org (last visited Nov. 30, 2015), http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

- **Communications Security**—are networks and services configured and operated in a secure manner?
- **System Acquisition, Development, and Maintenance**—is a life cycle for information systems defined and implemented?
- **Supplier Relationships**—are processes for identifying and managing risk from third-party suppliers defined and implemented?
- **Information Security Incident Management**—are processes defined and are incident response activities managed in a consistent manner?
- **Business Continuity Management**—is information security integrated into business continuity functions and processes?
- **Compliance**—are legal, regulatory, and contractual obligations identified and met within the organization?

Regardless of whether the organization seeks compliance with ISO 27001, the framework provides a comprehensive source of guidance, controls, and security strategies for the organization to consider for implementation. In this sense, the ISO 27001 framework provides a good reference for organizations looking for ideas on what to do from a security perspective.

D. HITRUST

The Health Information Trust Alliance (HITRUST) was formed by a group of health care organizations in 2007 with the common goal of improving patient care while lowering health care delivery cost by strengthening information security in the health care industry as a whole. With this fundamental mission, HITRUST collaborated with technology and information security experts to formulate the Common Security Framework (CSF), which is designed to be "used by any and all organizations that create, access, store or exchange" sensitive and/or regulated data.[51]

The CSF is founded upon the International Organization of Standards (ISO) and International Electrotechnical Commission (IEC) standards 27001:2005 and 27002:2005 and comprised of two key components: 1) the Information Secu-

[51] *About Us*, Health Information Trust Alliance, (last visited Nov. 27, 2015), https://hitrustalliance.net/about-us/.

rity Implementation Manual; and 2) the Standards and Regulations Mapping.

The Information and Security Implementation Manual includes 13 separate security categories, with 42 separate control objectives and 135 specifications focusing on security governance practices (e.g., organization, policy, etc.) and security control practices (e.g., people, process, and technology). The specific categories are as follows:

• Information Security Management Program • Access Control • Human Resources Security • Risk Management • Security Policy • Organization of Information Security • Compliance	• Asset Management • Physical and Environmental Security • Communications and Operations Management • Information Systems Acquisition, Development, and Maintenance • Information Security Incident Management • Business Continuity Management

The CSF harmonizes the above-identified Controls with the following Standards and Regulations:

• ISO/IEC 27002:2005 • ISO/IEC 27799:2005 • COBIT 5 • HIPAA Security Rule • HITECH Act • Stage 2 Meaningful Use Requirements • NIST SP 800-53 Revision 4 • NIST SP 800-66 • CMS ARS	• PCI DSS version 2.0 • FTC Red Flags Rule • 21 C.F.R. Part 11 • JCAHO IM • The CORE Security Requirements • 201 CMR 17.00 (State of Mass.) • NRS 603A (State of Nev.) • CSA Cloud Controls Matrix v. 1 • Texas House Bill 300

In 2015, HITRUST added privacy controls to the CSF by incorporating the HIPAA Privacy Rule and NIST SP 800-53 r4 FINAL Appendix J—Privacy Control Catalog into CSF v7. Critical to those "covered entities" governed by HIPAA, the CSF now addresses the privacy and security requirements set forth in HIPAA while further incorporating other

relevant health care related regulations and standards. Moreover, HITRUST offers a certification program providing an attestation process for those organizations needing to certify security compliance to third parties. In sum, the CSF is a risk-based approach to health care cybersecurity providing a scalable security baseline for health care organizations of all sizes.

E. PCI DSS for Payment Card Information

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded payment cards. The standard was first established in 2004 by the major payment card brands including Visa, MasterCard, American Express, Discover, and JCB. The standard includes 12 key requirements, each with a series of preventive and detective controls, for any merchant that stores, processes, or transmits payment cardholder data.[52] These requirements specify the framework for a secure payments environment to protect cardholder data.[53] Entities, including health care organizations, which store, process, or transmit credit card payments in any portion of their business model need to be concerned with PCI DSS compliance.

While the PCI Security Standards Council itself does not impose any sanctions for noncompliance, individual payment brands may have their own compliance requirements, including but not limited to contractual requirements and financial or operational consequences to certain businesses that are not compliant.

In April 2015, the PCI Security Standards Council published PCI DSS Version 3.1 and supporting guidance. While a majority of the revisions in this updated version are minor updates and clarifications, PCI DSS Version 3.1 addresses vulnerabilities within the Secure Sockets Layer (SSL) encryption protocol and early Transport Layer Secu-

---

[52] *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 3.1*, PCI Security Standards Council (Apr. 2015), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.

[53] *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 3.1.*

rity (TLS) that can put payment card data at risk. Essentially, SSL and TLS are encryption protocols designed to protect data in transit across networks. However, weaknesses were found within both, raising concerns about their acceptability for data protection. Therefore, SSL and early TLS implementations are no longer considered "strong cryptography."

Although Version 3.1 was originally published on April 15, 2015, PCI DSS Version 3.0 was not officially retired until June 30, 2015. A comprehensive summary of the changes from PCI DSS Version 3.0 to 3.1 is available at the PCI Security Standards Council's website.[54]

F. FDA Guidance for Medical Devices

The FDA is responsible for review, approval, and oversight of medical devices in the United States. In recent years, the FDA has expressed concern regarding the ability of hackers to access medical devices that contain embedded computer systems which can be susceptible to cybersecurity breaches and has identified numerous vulnerabilities that relate to inadequate security.[55] To date, many of the highly publicized security incidents involve technology-savvy consumers who "hack" into a medical device computer system to extract health information, sometimes for an off-label purpose.[56]

On October 2, 2014, the FDA issued voluntary final guidance regarding cybersecurity and medical devices, entitled "Content of Premarket Submissions for Management of

---

[54]Note that PCI DSS Version 3.2 was released on April 28, 2016. Version 3.1 will expire on October 31, 2016. However, all new requirements are best practices until February 1, 2018 to allow organizations an opportunity to prepare to implement these changes. For more information on PCI DSS requirements, please refer to the following link for the PCI Security Standards Council website, https://www.pcisecuritystandards.org/index.php.

[55]*Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication,* U.S. Food & Drug Admin. (June 13, 2013), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.

[56]*See, e.g.*, Kate Linebaugh, *Hackers Tinker With Medical Devices*, Wall St. J., Sept. 27-28, 2014, at A1.

Cybersecurity in Medical Devices".[57] The FDA suggests in the guidance that medical device security is a shared responsibility among stakeholders, including facilities, patients, providers, and manufacturers of these devices. Given the rapidly increasing use of wireless, Internet-connected, or network-connected devices, the guidance aims to provide recommendations stakeholders can use to manage and reduce the risk to patients that their devices may be compromised by insufficient cybersecurity.

The guidance urges manufacturers to build in the necessary cybersecurity safeguards on the front-end, during the design and development of a device, in order to provide more comprehensive protection for patients. Specifically, this privacy by design approach should involve a risk analysis, which includes an identification of the threats and vulnerabilities, an assessment of the impact of these threats and vulnerabilities, and an evaluation of how likely these areas are to be exploited. Manufacturers should submit documentation supporting this analysis to the FDA.

The FDA also recommends five "framework core functions" that manufacturers should use to manage potential cybersecurity risks: Identify, Protect, Detect, Respond, and Recover. This cybersecurity framework is taken directly from the NIST CSF. These five functions are aimed at setting baseline standards for an organization to manage its cybersecurity risks in an organized and efficient manner. Finally, the guidance advises manufacturers to include the following information relating to cybersecurity of their medical devices in premarket submissions:

- A listing of cybersecurity risks that were considered, as well as a listing and explanation of controls that have been established for the device;
- A matrix linking the risks and controls that were addressed;
- A plan for providing validated software updates and patches;
- A summary of controls in place to ensure device software will maintain its integrity; and

[57] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, U.S. Food & Drug Admin. (Oct. 2, 2014), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

- Instructions for use and specifications for the device relating to cybersecurity.

Practically, it is important to note that while the guidance is considered to contain only "nonbinding" recommendations, the FDA has suggested that it may choose to delay or require changes to devices that come before it for approval if those devices do not meet the recommended security standards. However, manufacturers may elect to provide an alternative method or approach, with an appropriate justification, in lieu of the approaches recommended in the guidance. Regardless of how they do it, manufacturers are required to be vigilant about identifying risks and hazards associated with their medical devices and are responsible for mitigating those risks to address patient safety and device performance issues.

In January 2016, the FDA followed up on its premarket guidance with additional draft guidance entitled "Postmarket Management of Cybersecurity in Medical Devices."[58] The medical device industry anxiously awaited this guidance, which outlines recommended steps medical device manufacturers should take to continually monitor, identify and address cybersecurity vulnerabilities after devices enter the market. This guidance clarifies FDA's position on postmarket surveillance and demonstrates the FDA's efforts to continue to address cybersecurity at all stages of a medical device's lifecycle.

In addition to addressing the need for manufacturers to proactively plan for and to assess cybersecurity vulnerabilities, the guidance:

- addresses the importance of information sharing through participation in an Information Sharing Analysis Organization (ISAO), a collaborative group made up of public and private-sector members who share cybersecurity information; and
- recommends that manufacturers implement a comprehensive cybersecurity risk management program that includes application of the voluntary NIST CSF.

---

[58] Postmarket Management of Cybersecurity in Medical Devices, U.S. Food & Drug Admin. (January 22, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

The majority of postmarket remedial actions taken by device manufacturers to address cybersecurity vulnerabilities and exploits are considered "routine updates or patches" for which the FDA would not require advance notification or reporting. However, device manufacturers must be advised that for remedial actions relating to cybersecurity vulnerabilities that impact essential clinical device performance or present a reasonable probability of severe health consequences or death, device manufacturers must notify the FDA prior to making modifications to address such cybersecurity vulnerabilities.

An example of the FDA acting on concerns regarding specific medical devices was given on July 31, 2015, when the FDA issued a safety warning alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities associated with the infusion pump. The Symbiq Infusion System is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population. The infusion system has the ability to communicate with a hospital's information system via a wired or wireless connection over facility network infrastructures.

The FDA strongly encouraged health care facilities to discontinue the use of this pump and instead transition to alternative infusion systems after Hospira and an independent researcher confirmed that an unauthorized user could remotely access the Symbiq Infusion System through a hospital's network. This vulnerability could permit hackers who are connected to a health care facility's network to control the device and change the dosage delivered by the pump, causing a risk of an overdose or underdose to the patient.[59] Not only could hackers access a medical device to potentially harm patients, but they could also access a medical device in order to obtain entry to the health care provider's data systems to steal large amounts of records and information.[60] Therefore, health care providers need to be cognizant of the security of their medical devices, protect-

[59]To date, there is no evidence of any patient adverse events or unauthorized access of a Symbiq Infusion System in a health care setting.

[60]Mahmood Sher-Jan, *Medjacking: The Newest Healthcare Risk?*, Healthcare IT News (Sept. 24, 2015), http://www.healthcareitnews.com/news/medjacking-newest-healthcare-risk.

ing the data itself but also protecting "the doors to the data, including the potentially billions of back doors created by medical devices."[61]

V. How to Conduct a Risk Analysis of Your Organization's Security Posture

Many health care organizations struggle with how to conduct a risk analysis and how often to do it. Health care organizations are required by HIPAA to conduct a risk analysis. In fact, one of the most important HIPAA Security Rule implementation specifications is the risk analysis. The risk analysis implementation specification is found in the Security Rule's security management process standard, which requires covered entities and business associates to implement policies and procedures to prevent, detect, contain, and correct security violations. The security management process standard has four required implementation specifications that provide instructions to covered entities and business associates on how to implement the standard, one of which is the risk analysis.[62]

The risk analysis implementation specification mandates that covered entities and business associates conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity or business associate.[63] The findings from the risk analysis are essential in determining how to comply with many of the Security Rule standards and implementation specifications. The results of the risk analysis must be used to draft the remainder of the entity's HIPAA Security Rule policies and procedures. The results of the risk analysis are also critical in assessing whether an implementation specification or an equivalent alternative measure is reasonable and appropriate as discussed above.

In addition to being a requirement of the Security Rule, conducting a risk analysis is a core objective for providers seeking payment through the Meaningful Use Program. The

---

[61] Sher-Jan, *Medjacking: The Newest Healthcare Risk?*

[62] 45 C.F.R. § 164.308(a)(1)(i).

[63] 45 C.F.R. § 164.308(a)(1)(ii)(A).

Meaningful Use regulations require entities to protect ePHI created or maintained by the certified EHR technology adopted by the entity through the implementation of appropriate technical capabilities. To meet this objective, the entity is required to conduct or review a security risk analysis in accordance with the Security Rule's requirements, implement security updates as necessary, and correct identified security deficiencies as part of its risk management process.[64]

As noted above, the risk analysis is only one of the implementation specifications under the security management process standard. Another of the implementation specifications under this standard, the risk management implementation specification, requires covered entities and business associates to implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level.[65] This will include developing and implementing a risk management plan, implementing security measures, and evaluating and maintaining security measures.[66] The results of the risk analysis will be used in the covered entity or business associate's risk management.

The Office for Civil Rights (OCR) recognizes that there are numerous methods of performing a risk analysis, and there is no single method or "best practice" that guarantees compliance with the Security Rule. The OCR has released a few pieces of guidance to assist entities in conducting a risk analysis, which serve to provide insight into how the government expects covered entities and business associates to conduct a risk analysis. The Office of the National Coordinator (ONC) for Health Information Technology has developed a security

---

[64]*See, e.g.*, 42 C.F.R. § 495.6(d)(15); (j)(16), (1)(15); s*ee also Security Risk Analysis Tipsheet: Protect Patients' Health Information*, CMS (March 2016), https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/2016__SecurityRiskAnalysis.pdf;*Step 5: Achieve Meaningful Use Stage 1, Protect Electronic Health Information*, HealthIT.gov, https://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures/protect-electronic-health-information.

[65]45 C.F.R. § 164.308(a)(1)(ii)(B).

[66]*Basics of Risk Analysis and Risk Management*, HHS HIPAA Security Series (March 2007), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

risk analysis tool in collaboration with the OCR.[67] In addition, the OCR issued guidance to organizations on how to comply with the risk analysis requirement in the HIPAA Security Rule in 2010.[68] This OCR guidance provides the following specific elements that an organization must incorporate into its risk analysis.[69]

- **Scope of the Risk Analysis**: The risk analysis must include the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that an organization creates, receives, maintains, or transmits. This includes ePHI in all forms of electronic media, regardless of the particular electronic medium in which it is created, received, maintained, or transmitted or the source or location of the organization's ePHI.
- **Data Collection**: An organization must identify where its ePHI is created, received, maintained, or transmitted and document the results of this determination.
- **Identify and Document Potential Threats and Vulnerabilities**: Covered entities and business associates must identify and document reasonably anticipated threats to ePHI and vulnerabilities which, if triggered or exploited by a threat actor, would create a risk of inappropriate access to or disclosure of ePHI.
- **Assess Current Security Measures**: Covered entities and business associates must assess and document the security measures used to safeguard ePHI. The security measures implemented will vary among organizations, based on variables such as the size of the organization. For example, small organizations generally have more control within their operating environment and fewer variables (e.g., fewer workforce members and information systems) to consider when making decisions regarding how to safeguard ePHI.
- **Determine the Likelihood of Threat Occurrence**: Covered entities and business associates must take into

---

[67] *See Security Risk Assessment*, HealthIT.gov, https://www.healthit.gov/providers-professionals/security-risk-assessment.

[68] *Final Guidance on Risk Analysis*, OCR (July 14, 2010), http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html.

[69] *Final Guidance on Risk Analysis*.

account the probability of the potential risks to ePHI. The probability of the risk in combination with the initial list of threats will determine the threats that are "reasonably anticipated," meaning that the Security Rule requires covered entities and business associates to protect against the threats.

- **Determine the Potential Impact of Threat Occurrence**: Covered entities and business associates must consider the "criticality," or impact, of potential risks to confidentiality, integrity, and availability of ePHI. This will involve assessing, qualitatively and/or quantitatively, the magnitude of the potential impact that could result from a threat exploiting a vulnerability. The covered entity or business associate should ultimately document all potential impacts that could result.
- **Determine the Level of Risk**: Covered entities and business associates should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. This risk level determination may be determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence or by assigning a risk level based on the average of the assigned likelihood and impact levels. The covered entity or business associate should ultimately document the assigned risk levels and a list of corrective actions the organization will perform to mitigate each risk level.
- **Finalize Documentation**: The Security Rule requires the risk analysis to be documented but does not require a specific format for that documentation. The risk analysis documentation is a direct input to the risk management process.
- **Periodic Review and Updates to the Risk Analysis**: The Security Rule does not specify how often a covered entity or business associate needs to conduct a risk analysis, aside from requiring entities to update and document security measures "as needed." However, the OCR guidance states the process should be ongoing. The risk analysis should be updated as new technologies and business operations are planned (e.g., change in ownership, turnover in key staff, incorporation of new technologies). Performing the risk analysis and

adjusting risk management processes to address risks in a timely manner will allow covered entities and business associates to reduce the associated risks to reasonable and appropriate levels.

To emphasize the importance of completing and regularly updating the risk analysis, an organization should note that the OCR has a record of penalizing entities that the OCR determines have not completed a risk analysis during the OCR's investigation into those entities.[70] The OCR is also looking for completed risk analyses in the Phase Two HIPAA Audits that commenced in March 2016. In the Phase One audits, the OCR determined that two-thirds of the audited entities had not conducted a complete and accurate risk analysis.[71] Therefore, covered entities and business associates can expect the OCR to take a hard line on risk analyses during the Phase Two audits.

VI. How to Handle a Data Security Event and Related Practical Considerations

A. How to Handle a Data Breach

The prospect of dealing with a security breach can be a daunting task for any organization. When an organization discovers a security event has occurred, the first thing it must do is investigate whether the event rises to the level of a security incident or security breach in accordance with its security incident response plan. During the investigation stage, organizations should refrain from classifying an event as a "security incident" or "breach" until the investigation

---

[70] *See, e.g.*, *Resolution Agreement*, Department of Health and Human Services (August 2015), http://www.hhs.gov/sites/default/files/cancercare-racap.pdf (stating "[f]rom April 21, 2005, the compliance date of the Security Rule, until November 5, 2012, CCG failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by CCG"; CCH was issued a civil monetary penalty of $750,000 for that violation and others and had to complete a risk analysis and submit it to OCR for approval).

[71] *See, e.g.*, Linda Sanches, *HIPAA Privacy, Security and Breach Notification Audits, Program Overview & Initial Analysis*, Health Care Compliance Association (2013), http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf.

has been completed—even with internal personnel. Many factors go into the analysis of whether a security event constitutes a security incident or data breach under HIPAA and state law. Further, contractual notification requirements can differ depending on the specific facts and circumstances of a security event. Classifying an event as a "security breach" before doing a thorough investigation creates many issues for an organization—from managing internal personnel's understanding of the event to subsequent inquiries about the event. For these reasons, it is extremely important for an organization to complete its investigation, often with the assistance of third-party forensic investigators and outside counsel, before determining whether a security incident or data breach has occurred.

HIPAA specifically defines what constitutes a reportable data breach and security incident, and each has different notification obligations depending on whether the organization is a covered entity or a business associate. HIPAA defines "breach" as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.[72] The presumption under HIPAA is that acquisition, access, use, or disclosure of unsecured PHI that violates the Privacy Rule is a reportable breach. However, HIPAA provides certain exceptions to the definition of "breach." In addition, HIPAA permits organizations to walk through a risk assessment that may result in the organization not needing to provide notification of the breach. It is therefore important to walk through each step of the breach analysis step by step. The following sections outline each of those steps.

Step 1: Determine whether there has been an impermissible acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule.

For an acquisition, access, use, or disclosure to constitute a HIPAA breach, it must constitute a violation of the Privacy Rule. Violations of the Security Rule alone do not constitute a HIPAA breach. In addition, the incident must be an acquisition, access, use, or disclosure. Other violations of the Privacy Rule, such as a failure to provide an individual with a Notice of Privacy Practices, would not constitute a HIPAA breach.

---

[72] 45 C.F.R. § 164.402.

Step 2: Determine if the PHI is unsecured.

HIPAA's breach notification obligations apply to breaches of "unsecured PHI." Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HHS.[73] Generally, "secure" means encrypted or properly destroyed consistent with NIST guidelines. For more information, please see HHS' Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.[74] In addition, see the discussion of encryption at section VII(B) (Cybersecurity Best Practices) below.

Step 3: Evaluate whether the incident falls under one of the exceptions to the breach notification obligations.

HIPAA provides three exceptions to the definition of "breach." The first exception is that the definition of breach excludes any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule. Please note this would not exempt snooping employees or workforce members as an acquisition, access, or use in that case would not have been made in good faith or within the scope of the employee or workforce member's authority.

The second exception is that the definition of breach excludes any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate or organized health care arrangement in which the covered entity participates. This exception applies only if the information received as a result of such disclosure is not further used or disclosed in violation of the Privacy Rule.

---

[73] 45 C.F.R. § 164.402.

[74] *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

The third exception is that the definition of breach excludes a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.[75] This could occur, for example, when a covered entity or business associate hands the wrong medical records to a patient and immediately takes them back or when a covered entity or business associate sends an explanation of benefits (EOB) to the wrong individual, and the EOB is returned by post office, unopened, as undeliverable. In contrast, if the individual opened the EOB prior to returning it, this exception would not apply.

In addition, a use or disclosure of information that has been deidentified in accordance with HIPAA will not constitute a breach.[76]

Step 4: Conduct a risk assessment to determine whether the impermissible use or disclosure poses a low probability of compromise to the PHI.

Unless it fits into an exception discussed in Step 3, above, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the four factors provided by HIPAA. Those factors are as follows: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.[77] Each of those factors is addressed in detail below.

---

[75]45 C.F.R. § 164.402(1).

[76]78 Fed. Reg. 5566, 5642 n. 12 ("Information that has been deidentified in accordance with 45 C.F.R. 164.514(a) to (c) is not protected health information, and thus, any inadvertent or unauthorized use or disclosure of such information is not considered a breach for purposes of this rule.").

[77]45 C.F.R. § 164.402(2).

i. Nature and Extent of the PHI Involved

In considering the nature and extent of the PHI involved in the incident, the organization should evaluate the types of PHI involved. The risk to the PHI increases if sensitive financial information is involved (e.g., credit card information, Social Security number, bank information), given the risk for identity theft or financial fraud. The risk to the PHI also increases if the PHI contained sensitive clinical information (e.g., mental health, alcohol or other drug abuse treatment information, genetic information, etc.) or detailed clinical information (e.g., treatment plan, diagnosis, medication, medical history information, test results). Interestingly, HHS also stated that a use or disclosure of more than the minimum necessary PHI could constitute a breach.[78]

Another aspect to consider under this factor is the likelihood that the recipient can reidentify the PHI, based on the context and ability to link the PHI with other available information. For example, a list of patient names, addresses, and hospital ID numbers is clearly identifiable. However, a list of patient discharge dates and diagnoses may be less identifiable, depending on the specificity of the diagnosis, size of the community, and the likelihood the recipient could combine other information with the PHI to reidentify the PHI.

ii. Unauthorized Person Who Used the PHI or to Whom PHI Was Disclosed

The second factor requires covered entities and business associates to analyze who used or received the PHI. The organization should consider the recipient's obligation to protect the privacy and security of the PHI. Covered entities, business associates, and federal agencies would generally be required by law to protect the information. On the other hand, thieves and hackers would clearly not have any such obligation. On that note, HHS has stated that a use within a covered entity or business associate may be lower risk than disclosures outside the covered entity or business associate,

[78]78 Fed. Reg. 5566, 5644 to 5645.

since covered entity and business associate workforce members are obligated to protect the PHI.[79]

If the recipient has the ability to reidentify the information, that would also be relevant under this factor and weigh toward there being more than a low probability of compromise to the PHI. For example, an employer that receives dates of service and diagnosis information for certain employees may be able reidentify the PHI based on other information available to employer, such as dates of absence from work.

iii. Whether PHI was Acquired/Viewed vs. Simply Exposed

The third factor to consider is whether the PHI was actually acquired or viewed or whether there was only an opportunity for the information to be acquired or viewed. For example, if a laptop was lost or stolen and later recovered and a forensic analysis shows the PHI on the laptop was never accessed, an organization could possibly determine the PHI was not actually acquired or viewed.[80] However, if PHI is mailed to the wrong individual, who opens the envelope and calls the organization to report the error, the individual acquired/viewed the PHI.

iv. Extent the Risk was Mitigated

The fourth factor to consider is that quickly mitigating any risk to PHI that was improperly used or disclosed may lower the probability of compromise to the PHI. For example, if the covered entity or business associate can obtain assurances (e.g., a confidentiality agreement) from the recipient of the PHI that the PHI will be destroyed or will not be further used or disclosed, that could weigh toward a low probability of compromise under this factor. The covered entity or business associate must consider both the extent and efficacy of the mitigation, however, as assurances from employees, af-

---

[79]78 Fed. Reg. 5566, 5643.

[80]Please note, however, that a covered entity or business associate cannot wait for the laptop to be found or returned to conduct its breach analysis. The OCR has expressly stated, "if a computer is lost or stolen, we do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered." 78 Fed. Reg. 5566, 5646.

filiated entities, covered entities, or business associates will provide more protection than assurances received from other third parties.[81]

The covered entity or business associate must analyze these four factors, plus any other relevant factors, to evaluate the overall probability that the PHI has been compromised. The risk assessment must be thorough, completed in good faith, and conclusions must be reasonable. The risk assessment must be documented in writing if the covered entity or business associate ultimately determines that notification of the breach is not required based on a determination of a low probability of compromise to the PHI. The covered entity or business associate is required to notify affected individuals, the OCR, and potentially the media if the risk assessment fails to show a low probability that the PHI has been compromised. These notification requirements are addressed in Step 5 below. Importantly, the covered entity or business associate has the burden of proof for showing why breach notification was not required.

Readers may notice that this risk assessment is different than it was historically. That is because the risk assessment requirements changed in 2013 with the Omnibus HIPAA Final Rule. Prior to the release of those rules, the risk assessment was subjective, and notification was required if an acquisition, access, use, or disclosure of PHI created a significant risk of financial, reputational, or other harm to the individual. However, in 2013, the risk assessment changed to the more objective standard used today.

Some organizations have inquired into why HHS even permits covered entities and business associates to conduct a risk assessment. HHS recognizes that the risk assessment prevents individuals from being flooded with breach notifications for inconsequential events, which could lead to unnecessary anxiety and eventually lead to apathy among individuals. As an example of when a covered entity or business associate could demonstrate that the incident created only a low probability of compromise to the PHI, HHS provided the example where a covered entity misdirects a fax containing PHI to the wrong physician practice. Upon receipt, the receiving physician practice notifies the sending

[81]78 Fed. Reg. 5566, 5642 to 5643.

covered entity and destroys the fax. HHS concluded that the covered entity might be able to demonstrate low probability that the PHI was compromised since the recipient was a covered entity (required to protect the PHI under HIPAA) that promptly destroyed the information upon receipt.[82] That is the type of situation where individual notification is not necessary or beneficial.

Often health care organizations will need to hire consultants to assist in the investigation of and the response to a breach. For example, organizations often need to hire forensic investigators, statisticians, public relations firms, call centers, and mailing houses. To the extent practical, organizations should have their outside counsel contract with the investigative consultants, such as forensic firms and statisticians (instead of the organization entering into a direct contract with the consultant), or at least have outside counsel involved in the process, in an effort to have the consultant's investigation and findings covered by attorney-client privilege and/or work product protection. That approach was successful in a recent ruling involving the Target data breach.[83] Plaintiffs argued that Target was required to release certain documents relating to a group called the Data Breach Task Force. Critical here, Target established this Task Force after its well-publicized breach, at the request of in-house and outside counsel to educate Target attorneys about the breach so that counsel could provide Target with informed legal advice. This Data Breach Task Force was separate from Target's ordinary course investigation.

After an in-camera review of selected documents, the court generally agreed that the documents were privileged and protected, finding that the work of the Task Force was focused on informing Target and its in-house and outside counsel about the breach so that it could provide Target with legal advice and prepare to defend the company in litigation, not on remediation of the breach. Although the court's decision did not explicitly depend on the presence of outside counsel, the decision clearly demonstrated that outside counsel's involvement was helpful in clearly delineating the

[82]78 Fed. Reg. 5566, 5646.

[83]*See* In re Target Corp. Customer Data Sec. Breach Litig., No. 14-2522, 2015 U.S. Dist. LEXIS 151974 (D. Minn. Oct. 23, 2015).

two tracks (i.e., legal advice versus breach remediation) and thus creating the protection.

Step 5: Provide notifications, if risk assessment shows more than a low probability of compromise to the PHI.

If the risk assessment demonstrates there is more than a low probability of compromise to the PHI, the covered entity will be required to provide written notice to the affected individuals, the OCR, and the media (in certain situations). Each of these notification obligations is discussed in detail below. Note that although HIPAA places these notification obligations on the covered entity, covered entities can delegate the responsibility to a business associate where appropriate.

In addition, if the entity conducting the assessment is a business associate, HIPAA requires the business associate to notify the applicable covered entity of the breach if the business associate's risk assessment demonstrates there is more than a low probability of compromise to the PHI. Importantly, the business associate agreement between the covered entity and business associate may require the business associate to report even suspected breaches although this is not required by HIPAA.[84] The business associate agreement will also likely specify a time frame that the business associate must comply with in making reports to the covered entity, which is usually much shorter than the 60 days HIPAA gives the business associate to report the breach to the covered entity. Thus, business associates should promptly review its applicable business associate agreement(s) in the event of a potential breach.

i. Individual Notifications

A covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of the breach. The covered entity must provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a

[84] 45 C.F.R. § 164.410.

breach.[85] A breach is treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity or by exercising reasonable diligence would have been known to the covered entity.[86] A covered entity is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).[87] Importantly, if a business associate is functioning as an agent of a covered entity, the covered entity is deemed to discover the breach when the business associate discovers the breach. Generally speaking, a business associate is functioning as an agent of a covered entity if the covered entity has the ability to control the business associate's conduct.[88]

HIPAA requires the individual notifications be made in writing by first class mail at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.[89] The regulations contain specifics regarding the content of the notifications and requirements for substitute

---

[85]Law enforcement can delay the notifications to individuals, HHS, and the media. *See* 45 C.F.R. § 164.412, stating if a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate must (a) if the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) if the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

[86]The time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach. 78 Fed. Reg. 5566, 5648.

[87]45 C.F.R. § 164.404.

[88]*See* 78 Fed. Reg. 5566, 5580 to 5582.

[89]45 C.F.R. § 164.404(c).

notification if there is insufficient or out-of-date contact information for the individual.[90]

ii. OCR Notification

A covered entity must notify HHS following the discovery of a breach of unsecured PHI. For breaches of unsecured PHI involving 500 or more individuals, the covered entity must notify HHS contemporaneously with the individual notifications. For breaches of unsecured PHI involving less than 500 individuals, the covered entity must maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide notification to HHS for breaches discovered during the preceding calendar year.[91] Notifications to HHS are submitted via online portal on HHS' website.[92]

iii. Media Notification

For a breach of unsecured PHI involving more than 500 residents of a single state or jurisdiction,[93] a covered entity must notify prominent media outlets serving the state or jurisdiction, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.[94] For example, if a breach affected 510 residents of the State of Arizona, the covered entity would have to notify prominent media outlets serving the State of Arizona. However, if the breach involved 200 residents of Arizona, 200 residents of New Mexico, and 200 residents of Texas, HIPAA would not require the covered entity to notify the media.

B. Security Incidents Not Rising to the Level of a Breach

If the risk assessment demonstrates there is only a low

---

[90] 45 C.F.R. § 164.404(d).

[91] 45 C.F.R. § 164.408.

[92] *Submitting Notice of a Breach to the Secretary*, Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

[93] A "jurisdiction" is a geographic area smaller than a state, such as a county, city, or town. 78 Fed. Reg. 5566, 5653.

[94] 45 C.F.R. § 164.406.

probability of compromise to the PHI and thus it is not a reportable breach, covered entities should determine if the incident constitutes a security incident. HIPAA defines "security incident" as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[95] Covered entities do not need to report security incidents to any other party under HIPAA and should handle the incident in accordance with their internal security incident response plan. In contrast, even if the risk assessment demonstrates there is only a low probability of compromise to the PHI, a business associate will still have to report the incident to the applicable covered entity if the incident constitutes a security incident and/or a use or disclosure in violation of the applicable business associate agreement.[96] The business associate will need to review its applicable business associate agreement(s) to determine the reporting requirements and time frames.

C. Other Considerations

In addition to HIPAA's requirements, there may be other laws to consider when handling a security breach. HIPAA does not preempt all state breach notification laws; as a result, in addition to the breach notification obligations under HIPAA, organizations will also need to check if there are any additional notification requirements under state breach laws. Moreover, for breaches involving payment card data, organizations will also have to comply with the Payment Card Industry Data Security Standards (PCI DSS) contractual breach reporting obligations. In September 2015, the PCI Security Standards Council issued incident management guidance aimed to help organizations respond to data breaches.[97] For breaches affecting non-U.S. operations or involving data received from or transmitted to other countries, organizations will also need to investigate whether international breach laws apply.

---

[95] 45 C.F.R. § 164.304.

[96] *See* 45 C.F.R. § 164.314(a)(2)(i)(C); 45 C.F.R. § 164.504(e)(2)(ii)(C).

[97] *Responding to a Data Breach: A How-to Guide for Incident Management, PCI Security Standards Council*, PCI Security Standards Council LLC, https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf.

In addition, the Federal Trade Commission (FTC) enforces its own breach law that applies to vendors of personal health records (PHRs), PHR-related entities, and third-party service providers for vendors of PHRs or PHR-related entities.[98] Per the FTC, a business is a PHR-related entity "if it interacts with a vendor of personal health records either by offering products or services through the vendor's website—even if the site is covered by HIPAA—or by accessing information in a personal health record or sending information to a personal health record . . . [unless the PHR-related entity is] already covered by HIPAA."[99] The FTC's data breach law requires that entities subject to the law provide notice to affected individuals, the FTC, and the media in certain instances when there has been an unauthorized acquisition of PHR-identifiable health information that is unsecured and in a PHR. Third-party service providers must notify the applicable PHR or PHR-related entity. The notification time frames are similar to those under HIPAA.

In addition to considering other laws, various government agencies have issued guidance regarding certain types of data breaches or incidents. For example, the FTC has issued guidance for health care providers and health plans on preventing and responding to medical identity theft.[100] In addition, the Department of Justice (DOJ) has released guidance on best practices for preparing a cyber incident response plan, preparing to respond to a cyber incident, and actions to avoid after a cyber incident.[101] The DOJ's Cybersecurity Unit issued the guidance, taking "lessons learned" from federal prosecutors about cyber criminals' tactics as well as information gathered from companies that have dealt with cyber

---

[98] 16 C.F.R. Part 318.

[99] *Complying with the FTC's Health Breach Notification Rule*, Federal Trade Commission (April 2010), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

[100] *Medical Identity Theft: FAQs for Health Care Providers and Health Plans,* Federal Trade Commission (January 2011), https://www.ftc.gov/tips-advice/business-center/guidance/medical-identity-theft-faqs-health-care-providers-health-plans.

[101] *Best Practices for Victim Response and Reporting of Cyber Incidents*, Department of Justice (April 2015), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

incidents. The list is primarily aimed at smaller organizations with limited resources, but the DOJ says larger organizations might benefit from its findings as well.[102]

The DOJ recommends preparing for a potential cyber incident by identifying the organization's "crown jewels," putting in place an actionable cyber incident plan, implementing appropriate technology, obtaining any necessary authorizations to permit network monitoring before a cyber incident occurs, and ensuring organizational policies align with the cyber incident response plan. The DOJ also recommends establishing relationships with cyber information sharing organizations to obtain access to information about new or commonly exploited vulnerabilities and engaging with law enforcement before an incident actually occurs. Lastly, the DOJ states organizations should ensure legal counsel understand the organization's technology and cyber incident management. The guidance notes that "[h]aving ready access to advice from lawyers well acquainted with cyber incident response can speed an organization's decision making and help ensure that a victim organization's incident response activities remain on firm legal footing."[103]

During an intrusion, the guidance recommends that organizations immediately assess the problem, implement measures to minimize continuing damage, record information about the attack, and then notify the appropriate people, including management, law enforcement, the Department of Homeland Security, and other potential victims. Before notifying outside third parties, however, an organization should work with its legal counsel to implement a security incident response plan that defines a process to determine when it is appropriate to notify such third parties. After the intrusion, the guidance states organizations should not use the compromised system to communicate and hack into or damage another network (i.e., "hack back"). Organizations should also remain vigilant and guard against intruders trying to regain access to networks they previously compromised.

---

[102] *Best Practices for Victim Response and Reporting of Cyber Incidents.* at 1.

[103] *Best Practices for Victim Response and Reporting of Cyber Incidents.* at 4.

After reading this section on handling data breaches, health care organizations will likely be interested in additional information on how to *prevent* data breaches in the first place. Although it might not be possible to prevent all data breaches, organizations can take steps to protect the privacy and security of data to minimize the likelihood or scope of breaches. The next sections provide practical guidance for organizations on how to best prepare for a data breach, including lessons learned and cybersecurity best practices.

VII. Common Pain Points & Cybersecurity Best Practices

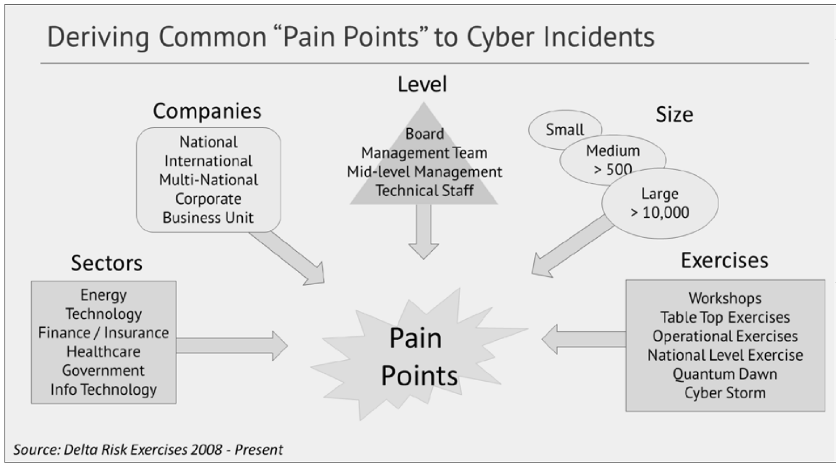
History reveals both the good and bad when it comes to organizations dealing with cybersecurity issues. The following section proposes a set of trends, categorized as "pain points" for issues organizations grapple with when responding to incidents and "best practices" for actions organizations can implement to help secure their network, mitigate risk, and limit disruption from cyber attacks. This section also provides information on exercises and penetration testing, which are methods that organizations can use to address the pain points.

A. Common Pain Points

The common pain points listed below are derived from a series of cyber exercises conducted by Delta Risk LLC[104] over the past seven years. The exercises were both discussion-based (table top) and functional in nature and involved companies of varying sizes (small to large) from different sectors (health care, technology, financial services, government, manufacturing, etc.). Organizations were presented with a cyber scenario and asked to respond in a manner consistent with their current capabilities and processes. The common pain points, below, stem from Delta Risk LLC's own observations during these exercises of the issues that affect most companies when presented with a cyber incident.

---

[104]Delta Risk LLC (www.delta-risk.net) specializes in strategic cyber security consulting, cyber exercises, assessments, and training.


Deriving Common "Pain Points" to Cyber Incidents
Level
Companies
National
International
Multi-National
Corporate
Business Unit
Board
Management Team
Mid-level Management
Technical Staff
Size
Small
Medium
> 500
Large
> 10,000
Sectors
Energy
Technology
Finance / Insurance
Healthcare
Government
Info Technology
Pain
Points
Exercises
Workshops
Table Top Exercises
Operational Exercises
National Level Exercise
Quantum Dawn
Cyber Storm
Source: Delta Risk Exercises 2008 - Present

The common pain points are listed in no particular order:

- **No established cross-functional incident "commander" to coordinate response:** Large organizations (especially those with multiple business units or disparate functions) were challenged by the lack of a coordination point—a quarterback who could coordinate a response effort across multiple functions within the organization. Organizations that appoint a person with visibility into business-wide impacts, and authority to make decisions across business units, (typically, a CISO or global IT or security lead), were found to be more successful during incident response scenarios.
- **No cross-organizational considerations or buy-in on incident response plan:** Organizations typically have an incident response plan, but the plans are frequently developed from a centralized perspective, and do not address the considerations of business units or multiple functions needed to coordinate and operate together during a response. Organizations that have integrated incident response plans, which account for the differences in the way business units respond (for example, authorities, operating procedures, decision making, impacts) or who have standardized incident response across their functions are more successful during incident response scenarios.
- **No established data classification to guide response activities and determine severity:** Many organizations have data classification guidance, but it is typically limited to defining classification types (e.g., confidential, sensitive, etc.) and does not track where in the organization the most critical information resides. Organizations that invest in understanding where types of information reside, and place a rating of importance on the information, are able to more rapidly make decisions, implement mitigations, and determine potential impacts when a certain type of data is compromised.
- **Missing processes or "use cases" for responding to high impact scenarios:** Organizations should "prethink" their response to cyber incident scenarios that may have a high impact on business operations. This allows the organization to respond in a rapid and consistent manner, having thought through the consider-

ations and major decisions that would typically need to be made during a response effort. For example, organizations that have previously discussed how they would respond to a data breach are better prepared to respond.

- **Cross-functional response procedures, including contact lists, are unavailable:** Many organizations focus on incident response as an IT or security function, but a typical response may require input and action from multiple functions within the organization including HR, legal, C-Suite, and communications. Procedures need not be detailed; a "memory jogger" of things to consider and who to contact can help cross-functional response be more rapid and effective.
- **Unknown business impact:**Organizations wrestle with understanding the impact of a cyber incident, frequently waiting until the impact occurs or until a decision on a course of action is made before understanding the extent of the impact. Organizations that have a good understanding of what actions cause certain impacts, or have ready access to staff which understand the impacts during an incident, are better able to make informed mitigation decisions.
- **Undefined event and incident terms:** Some organizations mix terminology during an incident response effort, causing confusion among responders and decision makers. In particular, terms like "event," "incident," or "breach" are used interchangeably when in reality they have specific meanings. Organizations that standardize, publish, and consistently use the same terminology are more effective at responding as intent and meaning are immediately clear.
- **No detailed event and incident thresholds defined:** Organizations are unclear on when an event escalates into an incident and lack thresholds for determining when to trigger certain response actions such as communicating with senior management or involving law enforcement. For the most part, organizations realized after the fact that their thresholds were too lax and many senior executives stated they would want to be involved earlier in the response, even if it was just from an informational standpoint. Organizations that define thresholds for key "use cases" or high impact scenarios, and understand when to escalate activity, are able to

rapidly make decisions and not get stuck in "analysis paralysis" with regard to what actions to take and when.

- **Lack of precanned external communications responses:** Internal and external communication is critical during incident response and most organizations have some type of communication plan which addresses when to communicate and the general tenor of the communication. However, most organizations stop there and do not create holding statements or other predefined communication templates, resulting in missed communication opportunities, or worse, wrong or conflicting information being released from multiple points. Organizations that have a clear media and communication policy, coordinated by a central function, using templated communications have a good handle on crisis communications during a cyber incident.
- **Train and exercise the most likely, or highest risk, scenarios:** Many organizations are good at responding to events that occur often, having had the opportunity to refine the response process during the events. However, many organizations do not "practice" for their highest risk scenarios, nor their most likely scenarios, which results in organizations reacting to a major incident for the first time, as it is actually occurring. Through exercising and training to the most likely or highest risk scenarios, organizations build muscle memory in their response and are able to respond in a manner that benefits from having thought through the response.

B. Cybersecurity Best Practices

The following are a set of best practices that are either required or recommended specifically for health care organizations. While there are certain actions required by HIPAA or recommended by HHS, the OCR, the FDA, the FTC, or others, it is commonly accepted that just complying with the HIPAA Security Rule only provides a modicum of security and should not be construed as complete security. For a more comprehensive approach, organizations should consider the various security frameworks (like ISO or NIST) or implement the best practices outlined by authoritative sources, such as the Center for Internet Security (CIS),

formerly known as SANs Top 20, and the Australian Signals Directorate (ASD) 35. The following section discusses general cybersecurity practices specific to health care organizations and then provides an overview of the CIS and ASD recommended best practices.

- **Encryption:** HHS/OCR strongly suggests that organizations secure PHI by making it unusable, unreadable, or indecipherable to unauthorized individuals, in particular to prevent reportable breaches.[105] Generally speaking, this requirement necessitates encryption of PHI data at rest (e.g., stored on file servers, in databases, on desktops, on laptops, paper copies, etc.) and while in transit (e.g., sending via e-mail, website upload, or syncing service like Dropbox). The HIPAA Security Rule requires that an algorithmic process must be used to transform the data with a confidential process or key that is stored in a different location from the data being encrypted.[106] For data at rest, an encryption process consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices must be used. Further, for data in motion, a process which complies with NIST Special Publication 800-52, Guide for the Selection and Use of Transport Layer Security (TLS) Implementation; SP 800-77, Guide to IPSec VPNs; or SP 800-113, Guide to SSL VPNs or others which are validated to the Federal Information Processing Standards (FIPS) 140-2 guidance must be used. If the guidance is followed and an event occurs, the event will not constitute a breach under HIPAA.[107]
- **Data destruction**: Also in accordance with HHS/OCR guidance, the media on which PHI is stored must be destroyed in a specific manner. For paper, film, or other hard copy materials, it must be shredded or destroyed such that the PHI is not readable or recoverable. Redaction is specifically noted as an invalid method of data

---

[105]*Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, HHS.Gov (last visited Dec. 29, 2015), http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

[106]See definition of encryption at 45 C.F.R. § 164.304.

[107]*Guidance to Render Unsecured Protected Health Information Unusable*.

destruction. Electronic copies of data must be handled in accordance with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI is unreadable and unrecoverable (e.g., with forensic tools). Like encryption, if these methods are used, then an event involving the "destroyed media" will not constitute a breach under HIPAA.[108]

- **Risk analysis**. As discussed in a previous section, risk analyses are required by the HIPAA Security Rule, and provide organizations with a method of understanding the threats, vulnerabilities, and impacts from cyber events, as well as identifying potential mitigation strategies. As part of this process, organizations will decide what risks to mitigate and what risks to accept due to various factors like time to implement, impact to operations, or resource availability. It is important to document the decision and rationale for mitigating risk and accepting risk and periodically review the decisions to ensure relevance.
- **Deidentifying data.** While there is no specific requirement to do so, deidentifying data in accordance with HIPAA's requirements[109] will mitigate the impact of a data breach and eliminate reporting requirements. The process of deidentifying data removes any "individually identifiable" markers from the data set—for example, Social Security numbers, names, and other information required by HIPAA. By removing unnecessary information, or storing it separately, a compromise of one data source would result in information that is not tied to a person, making it unusable by a data thief unless it was combined with another data set. In the age of big data, organizations should consider their intended current and future uses of data and evaluate whether their business and strategic goals would be met if such data is maintained in a deidentified data set.
- **Incident response plans**. An incident response plan guides an organization's activities in response to a cyber attack. A plan typically contains a description of the re-

[108] *Guidance to Render Unsecured Protected Health Information Unusable*.

[109] 45 C.F.R. § 164.514(a) to (c).

sources available for response by outlining roles and responsibilities and identifies the assets to be protected or covered by the plan, as well as some prioritization of those assets. Plans should include escalation thresholds, for example, when to escalate from an event to an incident or when to escalate the incident to senior management. Further, plans should include call trees or notification lists and have pointers to the most up-to-date contact information for people who should be involved in the response. The plan may also offer some type of guidance on conducting impact analysis to help responders triage and identify "how bad is it?" This is typically drawn from the organization's own information classification guidance if the organization has it. The plan should list the steps required in a response in as much detail as needed by the organization. For example, a response to a high criticality system may require a detailed, step-by-step checklist to guide the responders. However, for a low impact system, the plan may only need to provide "memory joggers" or a list of "things to consider" for the responders. A key part of incident response is to document the incident itself, how it was handled, and any lessons learned. In addition, the incident response plan should outline what is required for documentation and a process for identifying and implementing lessons learned stemming from response activities.

- **Network segmentation**. Segmenting a network is the concept of structuring the network in such a manner to separate different parts of the network from each other. Network segmentation can be done on a functional or data basis. Functional segmentation separates the network according to function or job role. For example, a functionally segmented network would place all of the human relations systems in one segment as distinct from all of the patient diagnostic systems, which would be in another segment. Data segmentation separates the network according to the location of data or asset criticality. In this case, public or nonsensitive data and systems used to access that data would be segmented in one part of the network, distinct and separate from sensitive data, like patient records or employee health information. In addition, network segmentation often

leads to an architecture that provides additional monitoring and logging points within the internal network and allows an organization's security functions to monitor internal activity within the network, not just that which crosses the external boundaries. Network segmentation, when done physically, involves planning and work to restructure the network but provides a solid architecture from which to conduct security monitoring and logging. Network segmentation, when done virtually, through use of Virtual Local Access Networks (VLANs), offers a quicker implementation, at the expense of adding logging and monitoring points.

- **Logging**. A significant number of organizations have the infrastructure to log security related events, but many either do not have it turned on or lack the monitoring functions to interpret the data from those logs. Logging functions are present on most network infrastructure devices like routers and switches, as well as end-user devices (e.g., laptops), servers, and security appliances (e.g., web proxies). Similar to the way performance monitoring data is examined by IT staff to determine the health of the network, an organization's security functions can examine the data from logging sources, correlate it, and derive an understanding of the security issues. In many cases, this data can be examined in real time to provide immediate alerting of incidents and can be analyzed after the fact to determine extent or scope of a compromise. However, to be effective, this data must be collected and stored through a logging function so that it can be analyzed. The storage size and time requirements are guided by organizational size, response times, and the type of information being logged—but it should be noted that data storage is relatively inexpensive, and at least a week of logging information for small to mid-sized organizations can be stored easily and inexpensively. Organizations should seek to collect as much security logging information that can be processed in a timely manner and have provisions for archiving the information for a set period of time (e.g., months) to assist in forensic analysis. Logging and monitoring solutions vary widely—and the right choice for an organization will depend on its size as well as the composition and capability of the security

team. For small to mid-size organizations, an outsourced security provider may be a good option. There are many vendors which provide security logging, monitoring, response, and remediation services. The right vendor for an organization is dependent on many factors like services offered, guaranteed service levels, cost, and reporting products.

- **Two factor authentication**. Username and password combinations have proven to be insufficient for controlling access to sensitive systems, applications, and data. Attackers have proven time and again that they are able to compromise usernames and passwords of users through phishing or other attacks. To address this vulnerability, two factor authentication adds security to the username and password combination by introducing another "item" into the authentication process to prove the user is who they say they are. Multifactor authentication involves: 1) something you know (e.g., a password); 2) something you have (e.g., a code received via SMS); and 3) something you are (e.g., fingerprint scan). Two factor authentication combines two of these (typically password and a code received via text message) to strengthen the identification and authorization process. Two factor authentication forces attackers to compromise not only the username and password but also the out-of-band identification method (e.g., sending SMS messages to users). Organizations should seek to add two factor authentication where feasible for users accessing sensitive systems or data. Doing so will significantly raise the bar for an attacker as they must compromise both methods in order to access the system or data; one method by itself is not sufficient.
- **Privacy and security by design**. A significant number of network and online implementations are done in such a manner that the focus is on getting things up and running first and then securing them later. This has proven to be a poor strategy, with many security functions tacked on after the fact being unable to provide an adequate level of protection. By considering the security and privacy implications of a system during its design, a comprehensive approach can be implemented with a corresponding reduction in risk from attackers.

- **Vendor management.**Organizations should consider implementing a vendor management program to identify and evaluate their vendors. HIPAA requires a covered entity to enter into a HIPAA-compliant Business Associate Agreement (BAA) with its vendors/business associates who create, receive, maintain, or transmit PHI on the covered entity's behalf.[110] Further, HIPAA requires a business associate to pass down the requirements in its BAAs to its vendors/subcontractors through a Subcontractor BAA between the business associate and subcontractor.[111] Organizations should ensure that their business associates and subcontractors have implemented administrative, physical, and technical safeguards in accordance with the HIPAA Security Rule. Further, organizations should require vendors to encrypt and destroy data, as appropriate, in accordance with the HHS/OCR guidance discussed above. Organizations should also consider how to mitigate the risk of a data breach in their BAAs and Subcontractor BAAs through breach notification obligations, indemnification language, etc. The success of an organization's cybersecurity program is highly dependent on its vendors and their subcontractor's security programs.
- **Cyber liability insurance**. Most general liability and commercial property policies specifically exclude losses to electronic data and losses incurred because of the Internet. A good cyber liability policy (or policies) can go a long way towards plugging these "gaps" in coverage. Cyber liability insurance is still fairly new, and there is a lot of variation among policies and therefore a lot of room for negotiation. Fundamentally, evaluating cyber coverage, like any other type of coverage, involves assessing the potential risks for which coverage is needed and comparing that risk with the coverage being offered. Coverage for damage to electronic data, liability for causing such losses to others, and professional liability coverage for IT related businesses are commonly offered coverages. Beyond this, critical thought should be given

[110]45 C.F.R. § 164.502(e)(1)(i).

[111]45 C.F.R. § 164.502(e)(1)(ii).

as to the likely costs that should be shifted to insurance. For example, some policies will pay for the costs and expenses associated with identifying who must be notified of a breach and providing required notices but stop short of providing funds for business interruption or hiring a public relations firm to repair reputational damage in the wake of a breach.

In addition to these recommendations, we also advise health care organizations to look to other organizations for guidance on "what to do now" to increase security. Several organizations have published "best practices" lists for security controls and protective measures. Some lists are more helpful than others by providing guidance along with implementation ideas. The Center for Internet Security (CIS) and the Australian Signals Directorate (ASD) publish excellent examples of these best practices and are discussed below.

The CIS list[112] was formerly known as the SANS Top 20.[113] Prior to Version 6, the list was published by SANS and the Council on Cyber Security. The list originated through consensus of community experts on what should be done to increase security. Despite the ownership changes, the list provides 20 controls organizations can implement immediately. The list provides guidance on the control, recommended tools, and implementation ideas. It should be noted that for each of the controls, several have "sub-controls," making the list a little larger than just 20 steps. Of the Top 20, the following five are identified as "Quick Wins" and recommended to be implemented first to provide an immediate increase in security.

---

[112]The current CIS list is available for download at *CIS Controls for Effective Cyber Defense Version 6.0*, Center for Internet Security, http://www.cisecurity.org/critical-controls/.

[113]The California Attorney General recently endorsed the CIS Controls as the minimum level of reasonable security standards under California law. *See* Cal. Civ. Code § 1798.81.5(b) (requiring businesses that collect personal information of California residents to use "reasonable security procedures and practices" to protect that information). The California Attorney General stated in a 2016 Data Breach Report that "failure to implement all the [CIS] Controls that apply to an organization's environment constitutes a lack of reasonable security." Kamala D. Harris, Attorney General, *California Data Breach Report*, California Department of Justice (Feb. 2016), https://oag.ca.gov/breachreport2016.

- Application whitelisting
- Standard secure configurations
- Patch applications software within 48 hours
- Patch system software within 48 hours
- Reduced number of users with administrative privileges

The ASD list contains 35 controls.[114] These controls were determined to be effective in mitigating 85% of the attacks the ASD was seeing and responding to. The list provides the mitigation, rationale, and implementation guidance for each control. Further, the list defines the following Top 4 controls, for which it provides detailed implementation guidance, as well as an implementation guide for project managers, on its site.

- Application whitelisting
- Patch application
- Patch OS
- Restrict administrative privileges

Organizations looking for ideas on how to improve their security should consult both the CIS Top 20 and the ASD Top 35 lists for recommendations, specifically focusing on the respective Top 5 and Top 4 controls. Given the overlap in controls between the two lists, organizations can take the implementation guidance provided by each organization and combine it to determine the most appropriate implementation.

VIII. Table Top Exercises and Penetration Testing

Table top exercises and penetration testing provide health care organizations with a method of end-to-end examination and testing of their security capabilities. Each construct provides an organization with a different view into how their security capabilities operate, and each has its own pros and cons in an organization's security strategy.

Table top exercises are a construct used to discuss how a

[114] *Strategies to Mitigate Targeted Cyber Intrusions-Mitigation Details*, Australian Signals Directorate (Feb. 2014), http://www.asd.gov.au/publications/Mitigation__Strategies__2014__Details.pdf?&v1.

health care organization would respond to a given cyber crisis in an informal, nonimpact generating, manner. During a table top exercise, participants are presented with a hypothetical situation and must discuss how they would respond. Specifically, participants are asked to demonstrate decision making (i.e., who is making the tough decisions) and coordination (i.e., who is talking to who) and determine actions they would take if the scenario were to occur. Table top exercises are discussion-based, meaning participants only discuss actions they would take—they do not actually perform the actions—resulting in zero impact to ongoing operations. Participants are welcome to refer to guidance or documentation as needed during the exercises—they may go so far as to call other people to discuss ideas or solutions—but the point of the table top exercise construct is to minimize risk to operations by keeping the exercise at the discussion-only level.

Generally, there are four levers which can be adjusted to customize a table top exercise for an organization:

1. **Length**: the length of time allocated for the exercise; generally ranges from one hour to multiday.
2. **Depth**: the level of realism in the presented scenario; generally ranges from "off-the-shelf" precanned exercise to fully customized exercise scenario tailored to the organization's specific risk concerns.
3. **Participants**: the organizations involved in the exercises; generally ranges from single organization to cross-functional participation from multiple business units.
4. **Level**: the level of the participants; generally ranges from technical staff to C-Suite executives.

Table top exercises can range from one hour discussions on a very specific topic or risk concern all the way to multiday exercises with involvement from senior, mid, and line level management and technical staff. As an example, a simple table top exercise might be a two hour discussion on how the organization would respond to a public breach of PHI for 10,000 customers from a communications/messaging perspective. A more complex table top exercise might be a two-day discussion starting at the technical staff and line management level, who identify issues outside their scope of authority that must be escalated to senior executives. The exercise would then break from the technical staff, and the

senior executives would become participants to discuss actions and needed decisions before pushing the results of the decision making session back to the technical staff and line management. The exercise would then continue with the technical staff interpreting the decisions from senior executives and discussing how to implement the decisions before concluding.

Table top exercises can provide a wide spectrum of opportunities for health care organizations to identify procedural gaps, organizational shortfalls, and even technical vulnerabilities as they react to a given situation.

In contrast, penetration testing is focused almost exclusively on the technical aspects of a health care organization's security. In a typical penetration test, the intent is to find a way to gain access to sensitive information or systems from a "hacker" perspective. Penetration testing helps an organization identify where it can be exploited, across its people, processes, and technology. A penetration tester may be able to find technical ways of remotely accessing internal systems, or they may find that the organization is highly susceptible to phishing messages and is able to get access to systems through the user population. Penetration testing can come in many forms and take many different routes in determining where the weaknesses are in the organization.

A "white box" penetration test is conducted with advance knowledge of the health care organization and the systems being tested. The team may have network architecture diagrams, system names, and/or knowledge of security procedures and systems from the organization. The team should use this information to customize the testing approach to focus on the risks it is concerned about as an organization. A "black box" test in contrast is conducted with no knowledge of the organization. It is up to the penetration team to find information on the organization, its network, and how to navigate its internal systems to conduct the test. This type of test most closely represents what a typical hacker would do when targeting an organization. Penetration testing is usually done within a set time frame, and as such, the penetration testing team has to determine appropriate courses of action and conduct its activities. By using a white box approach, the penetration testing team can spend more time on conducting its activities instead of chart-

ing the network and systems and establishing courses of action. With a black box approach, the team will spend a portion of its time determining courses of action and less time on conducting activities as compared to a white box test. White box tests are most appropriate when an organization is concerned about specific risks and can focus the testing team on specific areas. Black box tests are most appropriate when an organization is unsure of where to begin its security efforts or is looking for a broad test of its capabilities.

Due to the highly variable quality of penetration testing teams and the wide range of potential activities, it is imperative to work with a professional penetration testing team (if the organization does not have an internal testing team) to establish the scope of the test up front. The organization should determine which systems are in play and those that are off limits to the penetration testers. In addition, the organization should identify and document, in writing, how far it wants the team to go in accessing information, and it should set limits on what the team is allowed to do based on its risk appetite and the risks it wants to evaluate. Further, if using an external team, the organization should review samples of deliverables and reports to make sure the team is going to be able to provide the organization with the results in the necessary format.

IX. Cyber Threat Information Sharing/ Cybersecurity Collaboration

As the health care industry faces increasing cyber threats, the industry as a whole must stay informed about the types of attack methods. A method for doing so is sharing threat information and indicators throughout the industry. Threat information sharing is not a new concept, and in fact, the United States government has been promoting a public-private information sharing concept for some time. However, this public-private sharing concept has faced significant challenges because the private companies are often asked to share that they have been a victim of a cyber attack and the information related to any such attack. Understandably, private companies are concerned that by sharing this information, they may expose themselves to civil liability and, just as concerning, brand damage. In addition, current infor-

mation sharing guidelines are limited and confusing. In sum, there is currently not much incentive for private companies, including those in the health care industry, to meaningfully engage in threat information sharing.

In an apparent effort to address these liability concerns, while promoting a public-private threat information sharing program, President Obama signed the Cybersecurity Act of 2015 into law on December 18, 2015.[115] What many privacy advocates may view as controversial, the Cybersecurity Act of 2015 shelters companies that voluntarily share "cyber threat indicators" and "defensive measures" with other private entities or a federal agency from liability as long as any personal information of an individual known at the time of sharing is removed. The Act's provisions will sunset in 10 years.

The Cybersecurity Act of 2015 also addresses the need to improve cybersecurity in the health care industry by expressly requiring HHS to, among other things, convene a task force to address cybersecurity issues unique to the health care industry.[116] The membership of this task force was announced on March 16, 2016 and the inaugural meeting was held April 21, 2016.[117] Under the Cybersecurity Act of 2015, the HHS task force is required to:

A. analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;
B. analyze challenges and barriers private entities (excluding any state, tribal, or local government) in the health care industry face securing themselves against cyber attacks;
C. review challenges that covered entities and business

---

[115]Cybersecurity Act of 2015, H.R. 2029, 114th Cong. Division N §§ 101 to 111 (2015).

[116]Cybersecurity Act of 2015, H.R. 2029, 114th Cong. Division N § 405 (2015).

[117]*Health Care Industry Cybersecurity Task Force*, Pub. Health Emergency (last reviewed Apr. 12, 2016), http://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx; *Health Care Industry Cybersecurity Task Force Inaugural Meeting*, Pub. Health Emergency (last reviewed Apr. 20, 2016), http://www.phe.gov/Preparedness/planning/cip/Pages/HCICTaskforce.aspx.

associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

D. provide [HHS] with information to disseminate to health care industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

E. establish a plan for implementing [the Cybersecurity Information Sharing Act of 2015], so that the federal government and health care industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

F. report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).[118]

Notwithstanding the above, the health care industry has access to threat information through dedicated Information Sharing and Analysis Centers (ISAC). ISACs are centers established by Critical Infrastructure Key Resource (CI/KR) owners and operators for the purpose of providing private and government industries with relevant cyber threat information and other critical resources such as risk mitigation, incident response, alert, and information sharing. The National Health ISAC (NH-ISAC) is the nation's Information Sharing and Analysis Center (ISAC) for health care and public health critical infrastructure. NH-ISAC is a nonprofit and membership-sustained ISAC with a mission to provide threat information sharing and coordinated threat response to the health care industry.

In addition to the NH-ISAC, a private collaboration of health care, business, technology, and information security leaders, known as HITRUST, developed the HITRUST Cyber Threat Intelligence and Incident Coordination Center (C3), which provides cyber threat warning and threat intelligence services to participating health care organizations. Participating members can also benefit from the HITRUST Cyber Threat XChange (CTX), a component of (C3). CTX was created with the focus of accelerating the detection and response

[118]Cybersecurity Act of 2015.

to cyber threats by automating the threat collection and analysis process.

X. Health Care Boards and Cybersecurity Oversight

Boards of Directors (Boards) owe fiduciary duties to the health care organizations they govern. Generally, these include the duty to monitor and oversee corporate risk,[119] including cybersecurity risks. Therefore, it is important that Boards mandate that their organizations implement a cybersecurity program to ensure their fiduciary duties are met. Now more than ever, it is imperative that Boards take cybersecurity oversight seriously. As discussed in the introduction, the health care industry is vulnerable to cybersecurity attacks because of the value of health information and the industry's less than robust cybersecurity systems.[120] Furthermore, the potential for an OCR audit and breach notification laws make it even more critical that health care organizations take appropriate measures to protect against a cybersecurity attack.

Boards must ensure their health care organizations are taking proactive steps to secure and protect data. The Board should be protected by the business judgment rule for decisions it makes regarding cybersecurity threats if it makes such decisions on an informed basis, in good faith, and in the honest belief that the action is taken in the best interest of the health care organization.[121] However, failure to monitor cybersecurity risks (i.e., inaction) could also lead to an allegation of bad faith conduct in breach of the duty of

---

[119]This is the law in Delaware, and it is very likely that companies and organizations in other jurisdictions could see so-called *Caremark*-derivative claims in the wake of a data breach. *See* In re Caremark Int'l Derivative Litig., 698 A.2d 959 (Del. Ch. 1996).

[120]*See* section I of this article.

[121]*See* Comm. on Nonprofit Corporations., Am. Bar Ass'n, Guidebook for Directors of Nonprofit Corporations 38–39 (Willard L. Boyd III & Jeannie Carmedelle Frey eds., 3d ed. 2012). While the Business Judgment Rule is more established in case law involving for-profit corporations, the concept has also been recognized in the nonprofit context as the standards used by courts in nonprofit cases are often derived from corporate case law. Guidebook for Directors of Nonprofit Corporations at 39 n.21.

loyalty.[122] Therefore, it is not enough to just respond effectively to a breach, but rather it is important that Boards take preemptive measures to monitor cybersecurity risks to their organizations. If a breach does occur, Boards can still protect themselves from liability if they take proactive steps to address the breach and minimize exposure.[123] In addition to having HIPAA security policies and procedures, Boards should also consider implementing the NIST Framework for cybersecurity protection[124] as this will enable them to demonstrate that their organizations use prudent practices and due care in line with nationally recognized standards.

Once an organization's cybersecurity program is implemented, the Board should continually assess and evaluate it. While the Board's role is to provide high-level oversight, it should consider having an audit or risk management committee that scrutinizes the quality of the cybersecurity planning done by the organization's executive management and IT leadership. The Board should also ensure the health care organization's management has developed a data breach response plan consistent with best practices in the industry. Furthermore, given the FBI's recent warning discussed in the introduction, the Board and senior leadership within the organization could consider reaching out to leaders in other industries, like the financial and retail industries, to better

---

[122]*See Caremark*, 698 A.2d at 968–69; *see also* Stone ex rel. AmSouth Bancorporation v. Ritter, 911 A.2d 362, 369–70 (Del. 2006) (clarifying that the fiduciary duty violated for failing to monitor corporate risk in bad faith is the duty of loyalty).

[123]*See* Palkon v. Holmes, No. 2:14-CV-01234(SRC), 2014 WL 5341880, at *7 (D.N.J. Oct. 20, 2014) (dismissing a *Caremark* derivative suit brought against the Wyndham Worldwide Corporation (WWC) Board of Directors arising out of three data breaches that occurred within the company). The district court in *Palkon* noted that the plaintiff conceded that security measures existed when the first breach occurred. 2014 WL 5341880 at *6 n.1 Furthermore, the court recognized that the WWC Board took proactive steps after each breach to remedy the situation and minimize exposure by holding multiple board meetings to discuss the breaches, having its Audit Committee review the breaches, hiring technology firms to investigate the breaches, and by implementing the technology firms' recommendations to enhance cyber security. Palkon, 2014 WL 5341880, at *2.

[124]NIST is the National Institute of Standards and Technology. The NIST Framework was released on February 12, 2014. *See Framework for Improving Critical Infrastructure Cybersecurity*.

understand the cybersecurity programs that have been deemed more successful and how they can most efficiently maximize their resources to achieve success in preventing cyber attacks.

Boards must also be constantly aware of the current cybersecurity risks to their organizations. In a recent survey of board members conducted by the National Association of Corporate Directors (NACD), "health care" directors admitted to having the least knowledge of cybersecurity risks.[125] As a result, it is necessary for Boards to increase their knowledge of the cybersecurity threats to their organizations. In engaging in this process, Boards and their organizational leadership should consider the following questions:

- What information and systems warrant the very highest safeguards (e.g., what are your crown jewels)?
- How do existing safeguards compare with emerging best practices?
- Are critical risks receiving appropriate management attention and director oversight?
- Does the organization have a chief information officer (CISO) or other security oversight management personnel that report to the Board?
- Are external and internal cyber risks adequately communicated across the organization?
- Are appropriate measures in place to ensure sensitive data is adequately protected if relying on third-party IT service providers for services that involve such data or have access to the organization's information systems?
- Does the organization have a robust, written incident response plan?
- Is there a response team in place that has clear responsibilities and authority?
- Does the organization have appropriate resources (e.g., an insurance policy) to make it more resilient if a data breach occurs?

In considering these questions, it is important to recognize that each Board must tailor its oversight and monitoring of its organization's cybersecurity risks to the specific needs of

[125]Kim S. Nash, *Boards Struggle With Cybersecurity, Especially in Health Care*, WSJ.com (July 1, 2015), http://blogs.wsj.com/cio/2015/07/01/boards-struggle-with-cybersecurity-especially-in-health-care/.

its organization. Board oversight encompasses a variety of governance approaches, including ad hoc review of specific issues, annual risk analyses, and continual education of cybersecurity awareness. Boards must invest the time and resources in working with their organization's leadership teams to view cybersecurity as an "enterprise-wide" risk issue, not just as an IT issue.[126]

XI. Overview of Cyber-related Potential Penalties and Enforcement Actions

There are various penalties and enforcement actions that can be imposed as a result of a cyber incident. Specifically, this section discusses the potential penalties imposed by the OCR, the FTC, and State Attorneys General/Consumer Protection Agencies. This section also discusses the general types of potential civil liability and other litigation associated with a data breach.

This section does not address the entire scope of potential liability related to a data breach, which, depending on the type and scope of the data breach, may include other actions brought by other federal and state regulators. Furthermore, there are additional expenses related to data breaches and violations of HIPAA that are not addressed in this section but may be covered under relevant insurance policies. For example, there are costs related to breach notification, maintaining call centers, legal, forensic investigations, and administrative expenses or lost business costs, such as reputational losses, diminished goodwill, abnormal turnover, renegotiation of contracts, etc. Lastly, depending on the circumstances of a breach, an organization's potential liability may be offset by its vendors' obligations.

A. OCR Enforcement

Both covered entities and business associates are subject to civil monetary penalties and criminal penalties under

---

[126] *Cybersecurity: What the Board of Directors Needs to Ask*, Inst. of Internal Auditors Research Found, at 8 (2014), http://www.theiia.org/bookstore/downloads/freetoall/5036.dl__GRC%20Cyber%20Security%20Research%20Report.pdf (citing the National Association of Corporate Directors (NACD) Principle #1); *see also Cyber-Risk Oversight in the Boardroom*, Nat'l Ass'n of Corp. Directors, http://www.nacdonline.org/files/Cyber-Risk%20Oversight%20in%20the%20Boardroom.pdf.

HIPAA. The OCR is charged with enforcing HIPAA and may begin an investigation or take other actions it deems appropriate upon learning of a suspected violation through its complaint process or through a compliance review.[127]

In the case of a breach affecting 500 or more individuals, the OCR will open a compliance review of the covered entity or business associate, or both, as applicable. The OCR is also required to do a compliance review when a preliminary review of the facts of a complaint indicate a possible HIPAA violation due to willful neglect. The OCR also has the authority to conduct compliance reviews to determine if a covered entity or business associate is generally in compliance with HIPAA. If the OCR determines that a serious violation has occurred and the matter is not resolved by informal means, then it may impose an appropriate civil monetary penalty or pursue criminal penalties.

Under HIPAA, civil monetary penalties are tiered based on intent and generally range from $100 to $1.5 million.[128] When an entity did not know and, by exercising *reasonable diligence*, would not have known that the entity violated HIPAA, the penalties range from $100 to $50,000 per violation.[129] Where the violation was due to *reasonable cause* and not *willful neglect*, the penalties range from $1,000 to $50,000 per violation. Where the violation was due to *willful neglect* and corrected within 30 days after discovery, the penalties range from $10,000 to $50,000 per violation. Where the violation was due to *willful neglect* and *not* corrected within 30 days after discovery, the penalty is $50,000 per violation. The possible total penalty for identical violations in a calendar year is $1.5 million.

When calculating the amount of a civil monetary penalty, the following factors will be taken into consideration: (1) the nature of the violation (e.g., the number of individuals af-

---

[127]For a detailed description of OCR's complaint and enforcement process, please refer to the OCR website, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html.

[128]Please note that these civil monetary penalties are for violations occurring on or after February 18, 2009. For violations occurring prior to February 18, 2009, the OCR may not impose a civil monetary penalty in an amount more than $100 for each violation or in excess of $25,000 for identical violations during a calendar year. 45 C.F.R. § 160.404(b)(1).

[129]45 C.F.R. § 160.404(b)(2).

fected and time period in which the violation occurred); (2) the nature and extent of the harm resulting from the violation (e.g., whether physical, financial, or reputational harm occurred or whether it hindered the individual's ability to receive health care); (3) the entity's history of prior compliance with HIPAA; (4) the financial condition of the entity; and (5) other matters as justice may require.[130] For further detail on how civil monetary penalties are calculated, mitigating and aggravating factors the OCR takes into consideration and affirmative defenses, refer to Attachment A.

The OCR may also agree to enter into a resolution agreement with a covered entity or business associate. A resolution agreement is a contract between HHS/OCR and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations (e.g., staff training, completing a security risk analysis, and fixing vulnerabilities) and make reports to HHS/OCR generally for a period of three years. During such period, HHS/OCR monitors the covered entity's or business associate's compliance with its obligations set forth in the resolution agreement. These agreements also generally include the payment of a resolution amount. Typically, resolution agreements are reserved to settle investigations involving more significant violations. When HHS/OCR has not been able to reach a satisfactory resolution through the covered entity's or business associate's demonstrated compliance or corrective action through other informal means, civil monetary penalties may be imposed for noncompliance against a covered entity or business associate. This article discusses the resolutions related to security violations of electronic PHI on Attachment B.

The OCR also works in conjunction with the Department of Justice to refer possible criminal violations of HIPAA. When a person knowingly obtains or discloses PHI in violation of HIPAA, the criminal penalty is up to $50,000 and one year in prison.[131] If this wrongful conduct involved false pretenses, the penalty is up to $100,000 and five years in prison. If the wrongful conduct involved the intent to sell,

[130]45 C.F.R. § 160.408.

[131]42 U.S.C. § 1320d-6.

transfer, or use the PHI for commercial advantage, personal gain, or malicious harm, the penalty is up to $250,000 and 10 years in prison.

There is no private right of action under HIPAA. This means that affected individuals may not sue a covered entity or business associate for a breach of HIPAA. Individuals can file a complaint against a covered entity or business associate with the OCR. State Attorneys General can also bring a civil action to enjoin further actions or obtain damages.

In addition, the OCR commenced Phase Two of the HIPAA audits in March 2016.[132] Phase One of these audits was conducted as a pilot program in 2011 and 2012 on 115 covered entities.[133] In Phase One, audited covered entities were required to provide documentation of their privacy and security compliance efforts. In addition, every audit included a site visit where the OCR interviewed covered entity personnel and observed the covered entity's processes and operations to determine if the covered entity was in compliance with HIPAA's requirements.

The Phase Two audits are focused on monitoring compliance with the HIPAA Privacy, Security, and Breach Notification Standards as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Phase Two audits will be guided by findings and observations from the Phase One audits that indicated areas of concern in relation to privacy of PHI or security breaches. Audited entities can expect that although some on-site audits may be conducted, the majority of audits in Phase Two will be desk audits involving paper review only. Notably, Phase Two audits will cover both covered entities and business associates.

The OCR officially began the Phase Two audits in March 2016 by sending emails to certain covered entities to verify their contact information. Once the covered entity has responded to the OCR in a timely manner, the OCR will send a pre-audit questionnaire to gather data about the size,

---

[132] *OCR Launches Phase 2 of HIPAA Audit Program*, U.S. Dept. of Health & Human Servs. (Mar. 21, 2016), http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/.

[133] For more information on the OCR audit process, *see* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.

type, and operations of the organization. The pre-audit questionnaire will also ask covered entities to identify their business associates. Business associates will then also receive the pre-audit questionnaire from the OCR. The OCR has also made it clear that if a covered entity or business associate fails to respond to the information requests, the OCR will use publically available information about these entities to create the audit pool, meaning they still may be selected for an audit. The OCR will then use the information collected from the pre-audit questionnaires to create the Phase Two audit pool.[134]

Covered entities and business associates should focus now on preparation for these audits, as the OCR expects an auditee to respond to all requests for documentation during the desk audit phase within 10 business days of the request. For example, covered entities and business associates should enter into business associate agreements where needed; update existing agreements for compliance with the Omnibus HIPAA Final Rule; and ensure policies and procedures comply with HIPAA, that workforce members have been trained on those policies and procedures, and this training is documented. Covered entities should also review their Notice of Privacy Practices for compliance.

In addition, both covered entities and business associates should conduct a thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity or business associate. It is important to note that in the Phase One audits, 60% of the findings and observations were based on the Security Rule, and 58 out of 59 audited health care providers had at least one Security Rule finding or observation. Furthermore, the audits revealed that two-thirds of the audited entities had not conducted a complete and accurate risk analysis.

B. FTC

In addition to OCR oversight, health care organizations may also be regulated by the FTC. The FTC has broad pow-

---

[134] *HIPAA Privacy, Security, and Breach Notification Audit Program*, U.S. Dept. of Health & Human Servs., http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.

ers to regulate privacy and security under section 5 of the Federal Trade Commission Act, codified at 15 U.S.C. § 45. The FTC is tasked with "prevent[ing] persons, partnerships, or corporations . . . from using unfair methods of competition . . . and unfair or deceptive acts or practices in or affecting commerce."[135] The FTC construes this to mean that when a company fails to adhere to its own stated privacy policies, the company's policy is deceptive.[136] In addition, failure to reasonably safeguard consumer data can be construed as unfair practices affecting commerce.[137] However, pinning down what constitutes "reasonable safeguards" is difficult. Two recent cases help define the FTC's authority. One, the *FTC v. Wyndham*[138] case affirmed the FTC's broad authority to regulate data security while also giving concrete examples of what constitutes "reasonable safeguards" whereas the other, the *FTC v. LabMD, Inc.*[139] case, reigned in some of this authority.

The first to challenge the FTC's authority to ensure that companies take reasonable and appropriate measures to protect consumers' personal data was Wyndham Worldwide Corporation (Wyndham).[140] Wyndham suffered three hacks between 2008 and 2009. In June 2012, the FTC filed suit

---

[135]15 U.S.C. § 45(a)(2).

[136]*See, e.g.*, *2014 Privacy & Data Security Update*, Fed. Trade Comm'n (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate__2014.pdf.

[137]*2014 Privacy & Data Security Update*.

[138]*See generally* Fed. Trade Comm'n v. Wyndham Worldwide Corp., et al., 10 F. Supp. 3d 602, 610 (D.N.J. 2014) (order denying motion to dismiss), *aff'd*, 799 F.3d 236 (3d Cir. 2015). For the full procedural history, *see Wyndham Worldwide Corporation*, FTC File No. 102-3142, *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation.

[139]*See generally* LabMD, Inc. v. Fed. Trade Comm'n, 776 F.3d 1275 (11th Cir. 2015). For the full administrative procedural history *see In the Matter of LabMD, Inc.*, FTC File No. 102-3099, *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[140]*See generally* Fed. Trade Comm'n v. Wyndham Worldwide Corp., et al., 10 F. Supp. 3d 602, 610 (D.N.J. 2014) (order denying motion to dismiss), aff'd, 799 F.3d 236 (3d Cir. 2015). For the full procedural history, *see Wyndham Worldwide Corporation*, FTC File No. 102-3142, *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation.

against Wyndham alleging that Wyndham's conduct was an unfair practice, in part, because Wyndham allegedly permitted easily guessed passwords, hotel property management systems and third-party vendors to connect to Wyndham's network without taking appropriate cybersecurity precautions, and payment card information to be stored in clear readable text. Further, the FTC's complaint alleged that Wyndham's conduct was unfair because it failed to use firewalls, failed to employ reasonable measures to detect and prevent unauthorized access to its network, and did not follow "proper incident response procedures" or conduct security investigations. Also, the FTC alleged that Wyndham's privacy policy was deceptive because it stated Wyndham used encryption, firewalls, and other appropriate safeguards when Wyndham, allegedly, did not.

Wyndham challenged, arguing that the FTC lacked statutory authority to regulate security practices. Unfortunately for Wyndham, the courts have upheld the FTC action, confirming the FTC's broad authority, by indicating that any other holding would carve out "a data-security exception to the FTC's authority."[141] Moreover, the courts have held that the FTC does not need to formally publish rules and regulations defining what it means by "reasonable security measures." However, on December 11, 2015, in the FTC's settlement with Wyndham, the FTC gave some guidance on what it believes constitutes reasonable security measures. For example, in the FTC settlement, Wyndham agreed, among other things, to adhere to the PCI DSS, to conduct regular risk assessments, to create barriers (e.g., firewalls) between corporate servers and those of its franchisees, and to have a third-party assess annually whether Wyndham meets PCI DSS or other approved standards for the next 20 years.

Although these safeguards are specific to Wyndham in this instance, health care organizations should consider adopting these security measures as well. For example, health care organizations need to conduct risk assessments as required by HIPAA and should comply with PCI DSS if they store, process, or transmit credit card payments. Health

[141]Fed. Trade Comm'n v. Wyndham Worldwide Corp., et al., 10 F. Supp. 3d 602, 610 (D. N.J. 2014) (order denying motion to dismiss), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

care organizations also should evaluate third-party access to their networks and the safeguards they have in place to restrict inappropriate access. Lastly, they should consider having a third-party periodically assess whether they are in compliance with applicable standards.

LabMD also challenged the FTC's authority to regulate data security.[142] Without going in-depth on the procedural history, LabMD, a medical testing laboratory, was under FTC investigation for an alleged 2008 data breach of consumer information. Notably, the FTC rather than the OCR took the lead in investigating the alleged breach by LabMD. Specifically, the FTC issued Civil Investigative Demands (CIDs) to investigate LabMD's use of peer-to-peer file sharing (LimeWire), which was the alleged cause of the breach due to the lack of appropriate security measures. In August 2013, the FTC filed an administrative complaint against LabMD alleging that LabMD engaged in an "unfair" act by failing to prevent unauthorized access of patient information. LabMD challenged the FTC's authority to issue these CIDs and the complaint and, essentially, the FTC's power to regulate data privacy and security.

The case has taken several iterations. At each step, LabMD argued that the FTC had no authority to address the data security practices of private companies. The courts have confirmed that "the facially broad reach of Section 5's prohibition" includes regulation of data security practices, largely, because it was Congress' intent to grant the FTC " 'broad discretionary authority . . . to define unfair practices on a flexible, incremental basis.' "[143] However, in a November 2015 ruling by the Administrative Law Judge, the administrative case against LabMD was dismissed because the FTC failed to prove that LabMD's actions caused or were likely to cause substantial probable injury to

---

[142] *See generally* LabMD, Inc. v. Fed. Trade Comm'n, 776 F.3d 1275 (11th Cir. 2015). For the full administrative procedural history *see In the Matter of LabMD, Inc.*, FTC File No. 102-3099, *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[143] In re LabMD, Inc., No. 9357, 2014 WL 235518, at *3, 4 (F.T.C. Jan. 16, 2014) (citation omitted).

consumers.[144] This ruling could have significant implications because the FTC may become less eager to investigate companies, and likewise, companies will be less willing to agree to FTC consent decrees where there is no evidence that actual or probable harm exists or is likely to exist. However, because this decision was appealed by the FTC on November 23, 2015 and oral arguments were heard in early March 2016,[145] the impact of it is still unclear.

C. State Attorneys General/Consumer Protection Agencies

State Attorneys General have the authority to bring civil actions on behalf of state residents for violations of HIPAA and state law. In certain instances, HIPAA permits State Attorneys General to obtain damages on behalf of state residents or to enjoin further violations of HIPAA.[146] In addition to HIPAA, state data breach law may also be implicated in a breach scenario depending on the circumstances. There are 47 states that have data breach laws, including the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. Only Alabama, New Mexico, and South Dakota do not have data breach laws. Typically, the State Attorneys General enforce state data breach laws. Unlike HIPAA, many state data breach laws provide a private right of action for violations.

For the most part, organizations governed under HIPAA are often excluded from complying with state data breach laws, but it depends upon the state law and the data at issue. In order to assess whether state data breach laws are triggered, organizations need to determine the types of information affected, the location of the data at issue, residency of individuals affected, if any exclusions apply, among other factors. Even if an organization is excluded from complying

---

[144]In re LabMD, Inc., No. 9357, 2015 WL 7575033 (F.T.C. Nov. 13, 2015).

[145]Complaint Counsel's Notice of Appeal re FTC File No. 102-3099 (Nov. 24, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[146]For more information on HIPAA enforcement requirements related to State Attorneys General's ability to bring suits, please refer to the following link on the OCR website, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html.

with state data breach laws, in certain situations, it may be advisable to meet state law requirements when the law is not clear and to notify State Attorneys General to provide transparency regarding the situation. The facts and circumstances of every data breach are unique and need to be evaluated individually under each applicable state law.

D. Civil Liability and Other Litigation

There is also a possibility of class action suits or other lawsuits being brought against a covered entity or business associate as a result of a data breach. Many class action suits have been dismissed based on lack of standing due to the fact there has was no harm as a result of the data breach. However, this is an area that is quickly evolving.

Within two months of news reports regarding Target's data breach, approximately 70 civil lawsuits had been filed against Target. Within two days of Anthem's public announcement of its data breach, at least six consumer class actions were filed against Anthem. Such statistics confirm that while the possibility of civil liability may be more remote than regulatory action for data breaches, civil litigation is likely to follow public disclosure of any breach—and follow disclosure immediately. This trend is growing, not shrinking, in the wake of the recent court decisions. We are seeing litigation in three areas: (1) consumer class actions; (2) shareholder derivative suits; and (3) third-party business suits.

The first category, consumer class actions, proceed on dozens of theories of liability including common law negligence in handling the data, breach of contract, breach of implied contract, unjust enrichment, violations of state consumer protection statutes, and violations of state data breach statutes authorizing private causes of action. Until recently, these suits were often dismissed at the pleadings stage on the basis that plaintiffs lacked standing to sue for speculative injuries and could not, in good faith, allege specific, identifiable damages caused by the breach. However, courts have recently denied defendants' motions to dismiss the claims on standing grounds, finding plaintiffs' damages allegations sufficient to confer standing. These decisions have encouraged plaintiff's counsel to continue to vigorously pursue such claims and result in substantial increased costs

of defense and, perhaps, settlement amounts paid to resolve consumer class actions. Further, these decisions confirm the need for organizations facing consumer claims to provide credit monitoring and related support to affected individuals to address and diffuse at least in part the allegation of damages, proactively establishing the basis for the litigation defense that the consumers have not suffered direct, concrete injury and, therefore, lack standing.

The second category, shareholder derivative suits (which may or may not be filed on a class basis), also proceed on various theories of liability, including that the directors, officers, and board members of the organization breached their fiduciary duties and wasted corporate assets by failing to protect customer information and failing to timely disclose the data breach. Such suits may be more susceptible to dismissal than consumer class actions because of the protections the business judgment rule affords the organization in refusing to pursue such suits on its own provided the organization takes appropriate procedural steps to ensure the business judgment rule applies when faced with a shareholder demand.

The third category, third-party business suits, typically are brought against an organization by clients, financial institutions, or other entities with which the organization has contractual relationships and proceed on negligence and contract theories of liability, including that the organization failed to exercise reasonable care and/or implement contractually required measures to protect the third party's data. For example, business associate agreements, payment card related agreements, service agreements, and any other relevant agreements could come into play.

XII. Summary

As demonstrated in this article, the health care industry is under cyber attack by advanced persistent threats, such as sophisticated cyber criminals and even nation-states. The reasons are simple: PHI is valuable, and the industry is currently unprepared. For these reasons, health care organizations should implement a cybersecurity program with the capabilities to identify, protect, detect, respond, and recover from a data breach. Moreover, these cybersecurity programs must be continuously evolving by implementing risk manage-

ment processes to evaluate new threats and vulnerabilities. Now, more than ever, health care organizations must recognize that how they prepare for and respond to a data breach will affect how patients, regulators, business partners, and investors perceive them going forward.

While the focus of this article has been about cybersecurity best practices and effective methods for organizations to protect themselves from risk, organizations should not lose sight of their patients who entrust them with their most personal information. This is best summarized by Dan Munro in *Forbes*, "[t]he value of health data also transcends the technical means used to manage and protect it."[147] Munro adds, "[p]rivacy may well be dead, but trust isn't and [patient] trust is finite. Medical data is lifelong and has serious clinical consequences—along with financial ones."[148]

Attachment A
Civil Monetary Penalties

The following provides further detail on how civil monetary penalties are calculated under HIPAA specific to violations by a covered entity.[149]

Penalty Calculation Based on When the Violation Occurred

For violations occurring prior to February 18, 2009, the OCR may not impose a civil monetary penalty in an amount more than $100 for each violation or in excess of $25,000 for identical violations during a calendar year.[150]

---

[147]Dan Munro, *Healthcare Moves to the Cloud But Is The Cloud Ready for Healthcare?*, Forbes (July 6, 2015), http://www.forbes.com/sites/danmunro/2015/07/06/healthcare-moves-to-the-cloud-but-is-the-cloud-ready-for-healthcare/.

[148]*Healthcare Moves to the Cloud But Is The Cloud Ready for Healthcare?*

[149]Note that business associates are also subject to HIPAA penalties.

[150]45 C.F.R. § 160.404.

For violations occurring on or after February 18, 2009, amounts for civil penalties are based on the culpability or "state of mind" of the violator as follows:[151]

- *No Knowledge*. Where a covered entity does not know, and by exercising reasonable diligence[152] would not have known, that the covered entity violated HIPAA's administrative simplification provisions, the penalty range is $100 to $50,000 for each violation of an identical requirement or prohibition within the same year. The maximum penalty is capped at $1.5 million for violations of an identical requirement or prohibition within the same calendar year.
- *Reasonable Cause*. Where a violation is due to "reasonable cause"[153] and not "willful neglect," the penalty range is $1,000 to $50,000 per violation, with a cap of $1.5 million for violations of an identical requirement or prohibition within the same calendar year.
- *Willful Neglect*[154] *(but Corrected)*. Where a violation is due to "willful neglect," but was corrected during the 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, the penalty range is $10,000 to $50,000 per violation, with a cap of $1.5 million for violations of an identical requirement or prohibition within the same calendar year.
- *Willful Neglect (but Not Corrected)*. Where a violation is due to "willful neglect," but was not corrected during the 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising rea-

---

[151]45 C.F.R. § 160.404.

[152]Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. 45 C.F.R. § 160.401.

[153]Reasonable cause means an act or omission in which a covered entity knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision but in which the covered entity did not act with willful neglect. 45 C.F.R. § 160.401.

[154]Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. 45 C.F.R. § 160.401.

sonable diligence, would have known that the violation occurred, the minimum penalty is $50,000 per violation; there is no maximum per violation, and the total penalty is capped at $1.5 million for violations of an identical requirement or prohibition within the same calendar year.

OCR Discretion

In response to concerns that the degree of discretion granted to OCR in determining the number of identical violations could result in inconsistent penalties, OCR makes the following points in the preamble to the HIPAA final rules:[155]

- OCR will determine the penalty amounts on a case-by-case basis, taking into account the mitigating and aggravating factors discussed below;
- A covered entity or business associate may avoid (or reduce) many penalties by self-correcting violations;
- OCR has discretion to waive certain penalties even if they are not self-corrected in a timely manner;
- OCR has discretion to compromise civil monetary penalties; and
- Entities can appeal penalties to administrative law judges.

These factors do not seem to provide much comfort in response to concerns about excessive discretion since three of the five factors emphasize (rather than circumscribe) the amount of discretion.

Mitigating and Aggravating Factors that OCR Takes into Consideration

HIPAA also provides that OCR has significant leeway in determining the amount of the penalties by taking into account the following factors that may increase or decrease the amount of the penalty:[156]

- The nature and extent of the violation, considering, among other things, the number of individuals affected and the time period during which the violation occurred;
- The nature and extent of the harm resulting from the

[155]78 Fed. Reg. 5565, 5582 to 5586.

[156]45 C.F.R. § 160.408.

violation, consideration of which may include, but is not limited to, whether the violation caused physical, financial, or reputational harm, or hindered an individual's ability to obtain health care;
- The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity, consideration of which may include whether the current violation is the same as or similar to previous indications of noncompliance, whether and to what extent the covered entity has attempted to correct previous indications of noncompliance, how the covered entity has responded to technical assistance from OCR provided in the context of a compliance effort, and how the covered entity has responded to prior complaints;
- Financial condition of the covered entity, including whether the covered entity had financial difficulties that affected its ability to comply; whether the imposition of a civil monetary penalty would jeopardize the ability of the covered entity to continue to provide, or to pay for, health care; and the size of the covered entity; and
- Other matters as justice may require.

Please note the factors that may be considered in determining the amount of a civil monetary penalty are not specifically labeled as aggravating or mitigating. Instead, whether they are aggravating or mitigating will depend on the circumstances.

Affirmative Defenses

There are also affirmative defenses that exist for HIPAA violations. The specific defenses noted in HIPAA are as follows:[157]

- OCR is not permitted to impose a civil monetary penalty if a covered entity establishes that the violation in question is punishable as a criminal offense and that a penalty has been imposed under the HIPAA criminal liability provisions.
- For violations occurring prior to February 18, 2009, the OCR may not impose a civil money penalty on a covered

[157] 45 C.F.R. § 160.410.

entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:

(1) The covered entity establishes, to the satisfaction of OCR, that it did not have knowledge of the violation, determined in accordance with the federal common law of agency, and by exercising reasonable diligence would not have known that the violation occurred; or

(2) The violation is:

(i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated and is not due to willful neglect; and

(ii) Corrected during either:

(A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or

(B) Such additional period as OCR determines to be appropriate based on the nature and extent of the failure to comply.

- For violations occurring on or after February 18, 2009, the OCR may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of OCR that the violation is:

(1) Not due to willful neglect; and

(2) Corrected during either:

(i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or

(ii) Such additional period as OCR determines to be appropriate based on the nature and extent of the failure to comply.

The OCR also treats the statute of limitations as an affirmative defense even though it is not listed as an affirmative

defense in HIPAA. The OCR has a period of six years from the date of the occurrence of a violation to commence a civil monetary penalty action for that violation, and OCR's interpretation of this defense requires an entity to affirmatively raise the issue if the entity believes the violation occurred more than six years before the civil monetary penalty action was commenced.

Attachment B
Past Resolution Agreements Related to Security Violations of Electronic PHI[158] Security Flaws

1. *University of Washington (UW), December 14, 2015:* UW, which designates its health care components as a single affiliated covered entity, collectively referred to as UW Medicine (UWM), entered into a resolution agreement in the amount of $750,000 as a result of a breach of unsecured ePHI. UWM reported to OCR in November, 2013 that ePHI of approximately 90,000 individuals was accessed after an employee downloaded an e-mail attachment that contained malicious malware. OCR's investigation found that UWM had failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. As a result of the settlement, UW has agreed to enter into a Corrective Action Plan.
2. *Triple-S Management Corporation (Triple-S), November 30, 2015:* Triple-S, an insurance holding company based in San Juan, Puerto Rico, entered into a resolution agreement on behalf it its wholly owned subsidiaries in the amount of $3.5 million after OCR received multiple breach notifications from Triple-S involving unsecured PHI. OCR's investigation indicated wide-spread noncompliance throughout Triple-S's various subsidiaries offering Medicare Advantage Plans. Some of these

[158]Each of these summarized OCR resolution agreements can be found on the U.S. Department of Health & Human Services, Office for Civil Rights website. *See Resolution Agreements*, HHS.Gov (last visited Apr. 25, 2015), http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html. Please note that Attachment B does not discuss all of OCR's resolution agreements.

breach incidents affected fewer than 500 individuals, and some affected more than 500 individuals. OCR determined that Triple-S subsidiaries (1) failed to implement procedures for terminating access to ePHI when workforce members' employment terminates; (2) impermissibly disclosed its beneficiaries PHI to an outside vendor with which it did not have a business associate agreement; (3) disclosed more PHI than was necessary to accomplish the purpose for which it hired the outside vendor; (4) failed to implement appropriate safeguards to protect its beneficiaries' PHI; (5) failed to implement security measures sufficient to reduce the risks and vulnerabilities of ePHI to a reasonable and appropriate level; (6) failed to conduct a risk analysis of all IT equipment, applications, and data systems utilizing ePHI; and (7) impermissibly disclosed the PHI of its Medicare Advantage beneficiaries in multiple breach incidents. As a result of the settlement, Triple-S has agreed to establish a comprehensive compliance program, and has entered into a Corrective Action Plan.

3. *Anchorage Community Mental Health Services, December 2, 2014:* Anchorage Community Mental Health Services (ACMHS), a five-facility mental health nonprofit, reported a breach of unsecured ePHI affecting 2,743 individuals. This breach involved malware "compromising the security of its information technology resources." ACMHS paid a resolution amount of $150,000 and entered into a Corrective Action Plan. The ACMHS matter involved ongoing HIPAA violations dating back to 2005. In OCR's investigation, it determined the following: (1) that ACMHS had failed to conduct a security risk analysis since 2005; (2) that ACMHS had adopted "sample" security policies and procedures in 2005, but through March 2012, did not follow these procedures; and (3) that ACMHS failed to implement technical security measures such as ensuring a firewall was in place or that IT resources were supported and updated with security patches.
4. *New York and Presbyterian Hospital and Columbia University, May 7, 2014:* The New York and Presbyterian (NYP) Hospital and Columbia University (Columbia) resolution agreement involves two separate entities. These entities participate in a joint arrangement involv-

ing Columbia faculty members serving as attending physicians at NYP. Through this joint arrangement, NYP and Columbia operate a shared data network and shared network firewall administered by employees of both entities, linking to NYP patient information systems containing ePHI. The entities reported a breach affecting 6,800individuals to OCR in September 2010 and settled for a total of $4.8 million, with NYP paying $3.3 million and Columbia paying $1.5 million. The entities also entered into a Corrective Action Plan. The breach resulted from a Columbia physician attempting to deactivate a personally owned computer server on the network containing ePHI. However, this deactivation resulted in ePHI becoming publicly accessible on the internet, and the breach was discovered by a now deceased patient's partner on the internet. OCR investigated the matter and determined that: (1) NYP impermissibly disclosed the ePHI to Google and other internet search engines when a server was "errantly reconfigured"; (2) the entities failed to conduct an accurate and complete risk analysis that identified all systems (IT equipment, applications, and data systems) that accessed the ePHI; and (3) both entities failed to develop a risk management plan that addressed the potential threats and hazards to the security of the ePHI which assessed and monitored all systems linked to PHI or reduced the risk of the PHI. OCR also concluded that (4) NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies and procedures on information access management.

5. *Skagit County, Washington, March 7, 2014:* Skagit County, Washington, is the first settlement with a county government and involves a December 2011 breach involving the PHI of 1,581 patients of Skagit County. Skagit County notified OCR of a breach involving money receipts with ePHI thought to only involve seven individuals. This ePHI was accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the County. Upon OCR's investigation, it was determined that the breach was significantly larger than the seven individuals. Skagit County paid a resolution amount of

$215,000 and entered into a Corrective Action Plan. In OCR's investigation, it reached five conclusions: (1) For a two-week period in September 2011, Skagit County disclosed the ePHI of 1,581 individuals through its public web server; (2) since November 28, 2011, Skagit County failed to provide notification to all such individuals whose PHI had been compromised as a result of the breach; (3) since April 2005, Skagit County failed to implement sufficient policies and procedures, to "prevent, detect, contain, and correct security violations"; (4) from April 20, 2005, to June 1, 2012, Skagit County failed to implement and maintain security policies and procedures; and (5) Skagit County failed to provide appropriate training to its workforce, including its information security workforce, regarding HIPAA security.

6. *WellPoint, Inc., July 11, 2013*: WellPoint, Inc., an Indiana corporation, submitted a report to OCR regarding security weaknesses in an online application database allowing the ePHI of 612,402 individuals to be accessible to unauthorized individuals over the internet. WellPoint paid a resolution amount of $1.7 million related to this breach. OCR's investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule. OCR reported that WellPoint failed to (1) adequately implement policies and procedures for authorizing access to the on-line application database; (2) perform an appropriate technical evaluation in response to a software upgrade to its information systems, which affected the security of ePHI maintained in its web-based application database; and (3) have technical safeguards in place to verify the person or entity seeking access to ePHI maintained in its application database. This impermissible disclosure was from October 23, 2009, to March 7, 2010.
7. *Idaho State University, May 21, 2013*: The Idaho State University (ISU) matter involves the breach of the ePHI of approximately 17,500 patients at an outpatient clinic. ISU reported the breach to OCR on August 9, 2011. The ePHI at issue was unsecured for a period of at least 10 months due to disabling of firewall protections at servers maintained by ISU. As a result of this matter, ISU paid a resolution amount of $400,000 and entered

into a Corrective Action Plan. OCR's investigation determined that (1) ISU did not conduct a security risk analysis as part of its security management process from April 1, 2007, until November 26, 2012; (2) ISU did not adequately implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level for the same five-year period; and (3) ISU did not adequately implement procedures to regularly review records of information system activity to determine if any ePHI was used or disclosed in an inappropriate manner for the same five-year period.

8. *Phoenix Cardiac Surgery, P.C. (PCS), April 13, 2012:* In this case, a provider impermissibly posted ePHI on a publicly accessible internet calendar. OCR also found that the provider failed to (1) have adequate policies and procedures to safeguard PHI; (2) train its workforce on HIPAA; (3) appoint a security officer; (4) conduct an accurate and thorough risk analysis; or (5) enter into a business associate agreement with its Internet-based calendar and e-mail vendors. PCS agreed to pay a resolution amount of $100,000 and enter into a Corrective Action Plan. This case signaled a change in OCR's position on conduits (*i.e.*, entities that merely transport or transmit information but do not regularly access it).

Stolen, Lost, or Otherwise Inappropriately Accessed Unsecured Electronic Media

1. *Feinstein Institute for Medical Research, March 17, 2016*: Feinstein Institute for Medical Research (FIMR), a biomedical research institute in New York, reported that a laptop containing the ePHI of approximately 13,000 patients and research participants was stolen from an employee's car. OCR investigated the matter and found that FIMR (1) failed to conduct an accurate and thorough risk analysis; (2) failed to implement policies and procedures for granting access to ePHI by its employees; (3) failed to implement physical safeguards for a laptop that contained ePHI to restrict access to unauthorized users; (4) failed to implement policies and procedures that govern receipt and removal of hardware and electronic media and contain

ePHI in and out of the facility; and (5) failed to implement a mechanism to encrypt ePHI or document why encryption was not reasonable. FIRM agreed to pay a settlement amount of $3,900,000 and enter into a Corrective Action Plan.

2. *North Memorial Health Care of Minnesota (North Memorial), March 16, 2016*: North Memorial agreed to settle in an amount of $1,550,000 for the hospital's failure to implement a business associate agreement ("BAA") with a contractor and failure to conduct an organization-wide risk analysis. From March, 2011 to October, 2011, North Memorial permitted Accretive Health ("Accretive") to access the hospital's patient database to perform certain activities as a business associate without first entering into a BAA, as required under the HIPAA Privacy and Security Rules. During this time period when a BAA was not in place, an unencrypted password-protected laptop was stolen from an Accretive workforce member's locked vehicle, which contained the electronic protected health information ("ePHI") of 9,497 individuals. In addition to the monetary settlement, North Memorial was required to enter into a Corrective Action Plan, which among other things, requires North Memorial to develop policies and procedures related to business associate relationships, and then train its workforce members. North Memorial also must modify its existing risk analysis process and develop and implement an organization-wide risk management plan.
3. *Lahey Clinic Hospital, Inc. (Lahey), November 25, 2015:* Lahey, a nonprofit teaching hospital in Massachusetts, reported that a laptop, which had been connected to a computerized tomography (CT) scanner, was stolen from an unlocked treatment room (workstation). Lahey notified OCR that the laptop contained ePHI of 599 individuals. OCR investigated the matter and concluded that Lahey: (1) failed to conduct a thorough risk analysis of all of its ePHI; (2) failed to implement reasonable and appropriate physical safeguards for a workstation that accessed ePHI; (3) failed to implement policies and procedures with respect to the workstation that govern the movement of hardware and electronic media that contain ePHI in

and out of the facility; (4) failed to assign a unique user name for identifying and tracking user identity with respect to the workstation; (5) failed to record and examine the activity of the workstation; and (6) impermissibly disclosed ePHI of the affected individuals. Lahey paid a resolution amount of $850,000 and entered into a Corrective Action Plan. This case emphasized that entities must appropriately protect the workstations associated with medical devices in conformity with HIPAA standards.

4. *Cancer Care Group, P.C., August 31, 2015*: Cancer Care Group, P.C., a radiation oncology private physician practice, reported a breach of unsecured ePHI after a laptop bag containing an employee's computer and unencrypted backup media with personal information of 55,000 current and former Cancer Care patients was stolen from the employee's car. Cancer Care paid a resolution amount of $750,000 and adopted a Corrective Action Plan. During the OCR's investigation, it found that Cancer Care: (1) failed to conduct an enterprise-wide risk analysis prior to the breach; and (2) did not have a written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities, which was a common occurrence within the organization.
5. *St. Elizabeth's Medical Center, July 8, 2015*: St. Elizabeth's Medical Center (SEMC), a tertiary care hospital, agreed to settle in the amount of $218,400, for both the noncompliance with HIPAA by SEMC workforce members, affecting at least 498 individuals, and a separate breach incident of unsecured ePHI on a former SEMC workforce member's personal laptop and USB drive, affecting 595 individuals. As part of the settlement, SEMC agreed to enter into a Corrective Action Plan. OCR first received the complaint alleging that SEMC workforce members used an internet-based document sharing application to store documents that contained ePHI. OCR determined during the investigation that SEMC did not take appropriate steps to identify and respond to the security incident. OCR later learned from SEMC about the breach of unsecured ePHI stored on the former workforce member's personal computer.

6. *Concentra Health Services, April 22, 2014*: On December 28, 2011, Concentra notified OCR that an unencrypted laptop was stolen a month earlier from one of its physical therapy centers located in Springfield, Missouri. The number of affected individuals was not mentioned as part of the resolution agreement, but Concentra paid a resolution amount of $1,975,220 and entered into a Corrective Action Plan. OCR investigated the matter and determined two main issues: (1) Concentra failed to adequately "remediate and manage" its identified lack of encryption, or in the alternative, document why encryption was not reasonable and appropriate, and implement an equivalent option to encryption. This failure was ongoing from October 27, 2008, to June 22, 2012, when a complete inventory assessment was completed, and Concentra began the process to encrypt all unencrypted devices (previously some but not all devices had been encrypted); and (2) Concentra did not sufficiently implement policies and procedures to prevent, detect, contain, and correct security violations when it "failed to adequately execute risk management measures to reduce its identified lack of encryption to a reasonable and appropriate level" for the period between October 27, 2008, and June 22, 2012.
7. *QCA Health Plan, Inc., April 22, 2014*: QCA Health Plan, Inc. (QCA) is another matter involving a stolen laptop affecting 148 individuals on October 8, 2011. QCA paid a resolution amount of $250,000 and entered into a Corrective Action Plan. OCR determined that (1) QCA did not implement adequate policies and procedures to prevent, detect, contain, and correct security violations, including the failure to conduct a risk analysis of the potential risks and vulnerabilities to ePHI, and failure to implement appropriate security measures to reduce those risks; (2) QCA failed to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users; and (3) QCA impermissibly disclosed the ePHI of the affected individuals.
8. *Adult & Pediatric Dermatology, P.C., December 20, 2013*: The Adult & Pediatric Dermatology, P.C. (APD) matter involved a report by APD in October 2011 that

an unencrypted thumb drive containing the electronic protected health information (ePHI) of approximately 2,200 individuals was stolen from a vehicle of one of its staff members. The thumb drive was never recovered. APD notified its patients of the theft of the thumb drive within 30 days of the theft and also provided media notice. The APD matter is the first settlement with OCR for not having policies and procedures in place to address the breach notification provisions of HITECH. APD paid a resolution amount of $150,000 and entered into a Corrective Action Plan. In OCR's investigation, it determined that (1) APD did not conduct an accurate or thorough risk analysis of the potential risks and vulnerabilities related to ePHI until October 1, 2012; (2) APD did not fully comply with the administrative requirements of the Breach Notification Rule to have written policies and procedures and to train members of its workforce regarding breach notification until February 7, 2012; and (3) APD impermissibly disclosed the ePHI of up to 2,200 individuals for a purpose not permitted under HIPAA and did not reasonably safeguard an unencrypted thumb drive.

9. *Affinity Health Plan, Inc., August 14, 2013*: The Affinity Health Plan (Affinity) matter involves a nonprofit managed care plan in the New York City area that had previously leased a photocopier currently owned by CBS Evening News. CBS Evening News informed Affinity that the photocopier contained ePHI on the hard drive. This breach was reported to OCR on April 15, 2010, and involved the ePHI of 344,579 individuals. As a result of the breach, Affinity paid a resolution amount of $1,215,780 and entered into a Corrective Action Plan. In OCR's investigation, it determined that (1) Affinity impermissibly disclosed ePHI of up to 344,579 individuals when it failed to properly erase the hard drives of the photocopiers prior to sending them back to a leasing company; (2) Affinity failed to assess and identify the potential security risks and vulnerabilities of the ePHI stored in the hard drives; and (3) Affinity failed to implement its policies for the disposal of ePHI with respect to the hard drives.
10. *Hospice of North Idaho (HONI), December 31, 2012*:

The case involved the theft of a laptop containing the ePHI of 441 individuals. OCR's investigation determined that there was a failure by HONI to conduct an accurate and thorough risk analysis and to adequately adopt or implement security measures to ensure the confidentiality of ePHI with respect to portable devices. HONI paid a resolution amount of $50,000 and entered into a Corrective Action Plan. The case was significant in that it was the first settlement for a breach affecting fewer than 500 individuals.

11. *Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (MEEI), September 17, 2012*: The case involved a breach of the unsecured ePHI of about 3,500 individuals due to the theft of an unencrypted laptop. The investigation by OCR uncovered MEEI's failure to (1) conduct a thorough risk analysis; (2) to maintain sufficient security measures to ensure the confidentiality of ePHI with respect to mobile devices; (3) to implement policies and procedures (a) to address security incident identification, reporting, and response, (b) to restrict access to authorized users for portable devices that access ePHI, (c) governing the receipt and removal of portable devices; and (4) to adopt technical policies and procedures to allow access to ePHI using portable devices only to authorized persons or programs. MEEI paid a resolution amount totaling $1.5 million (in three installments), and entered into a Corrective Action Plan.
12. *Alaska Department of Health and Human Services (DHHS), June 26, 2012*: In this case, a portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of a DHHS employee. Over the course of the investigation, OCR found that DHHS did not have adequate policies and procedures in place to safeguard ePHI. Further, DHHS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule. DHHS agreed to pay a resolution amount of $1.7 million and enter into a Corrective Action Plan.

11. *BlueCross BlueShield of Tennessee (BCBST), March 13, 2012*: This case involved the theft of 57 hard drives containing encoded PHI. The data consisted of over 300,000 video recordings and over 1 million audio recordings. According to OCR, the insurer had not adequately protected PHI, had failed to update its security risk analysis in response to operational changes, and had failed to implement appropriate physical safeguards. BCBST agreed to pay a resolution amount of $1.5 million and to enter into a Corrective Action Plan.
13. *Providence Health & Services, July 16, 2008*: On several occasions between September 2005 and March 2006, backup tapes, optical disks, and laptops, all containing unencrypted electronic protected health information, were removed from the Providence premises and were left unattended. The media and laptops were subsequently lost or stolen, compromising the protected health information of over 386,000 patients. OCR received over 30 complaints about the stolen tapes and disks, submitted after Providence alerted patients to the theft, pursuant to state notification laws; Providence also reported the stolen media to HHS. As a result of the investigation, Providence agreed to pay a $100,000 resolution amount and enter into a Corrective Action Plan.