5-2018

A Comparative Analysis of HIPAA Security Risk Assessments for Two Small Dental Clinics

Scott Lisbon
St. Cloud State University

A Comparative Analysis of HIPAA Security Risk Assessments for Two Small Dental Clinics

By

Scott Lisbon

A Thesis

Submitted to the Graduate Faculty of

St. Cloud State University

In Partial Fulfillment of the Requirements

for the Degree of

Master of Science in Information Assurance

May 2018

Committee Members:
Dennis Guster, Chairperson
Balasubramanian Kasi
Erich Rice

Abstract

Cyber security risk assessments in the healthcare industry are legally required and demand an ongoing investment of time and resources. Small healthcare clinics are less likely to have streamlined processes in place to meet these requirements. This work presents two case studies featuring qualitative Health Insurance Portability and Accountability Act (HIPAA) security risk assessments of small dental clinics using the free Security Risk Assessment (SRA) tool provided by the US Department of Health and Human Services. One clinic used a cloud service provider to safeguard protected health information (PHI) while the other used an on-premises server. The data revealed detailed information relating to the cyber risk posture of each organization within the scope of the HIPAA Security Rule. Analysis included suggestions to mitigate the compliance gaps and vulnerabilities within the environment. Based on the data gathered, a comparative analysis of using the cloud vs. on-premises to manage PHI was conducted to provide insight into the need to balance security with other business requirements. This work provides greater context to the process of conducting HIPAA-compliant security risk assessments, including the responsibilities that small healthcare providers must own to protect their business reputation in the event of a major security incident.

Acknowledgements

I would like to extend my sincere gratitude to those who have nurtured my growth throughout this project. Dr. Erich Rice has been a terrific mentor who empowered me to own this work in the early stages. James Redman, CISA, CISSP provided useful early insight into the work as an experienced security auditor, which helped steer its focus. Dr. Dennis Guster, my thesis advisor, strongly supported the work throughout the process and was instrumental in helping me to understand the full context of cyber security, which includes a balance of management and technical skills.

Thanks to the Minnesota chapter of the Information Systems Security Association for providing premium professional development opportunities that are reflected in this work. I would especially like to call out Dr. Christophe Veltsos, Rebecca Herold, and Dr. Charlotte Tschider for their useful insights and leading-edge work in this area.

I would also like to offer special thanks to Dr. Susantha Herath for his support of the National Science Foundation STEM scholarship program. This program empowered me to grow with fellow peers and attend security conferences, which accelerated my growth as a professional in this field.

Table of Contents

Chapter Page

List of Figures

Chapter I: Introduction

Introduction

This work includes HIPAA security risk assessments of two small dental clinics using the SRA tool provided by the Department of Health and Human Services (HHS). One clinic used a cloud service provider (CSP) to safeguard PHI and the other housed PHI on-premises. A comparative analysis of the risks between the two clinics was conducted which included an evaluation of the pros and cons of housing PHI in the cloud. The final section includes an examination of key factors for small business owners to consider based on emerging cyber security trends.

Problem Statement

Periodic risk assessments for all healthcare entities which use electronic PHI are required under the HIPAA Security Rule as a subset of HIPAA compliance. Risk assessments are time-consuming activities which require expertise and significant attention to detail. These risks must then be managed and mitigated, as appropriate, in a continuous improvement process.

Nature and Significance of the Problem

Small healthcare clinics are often forgotten in the cyber security landscape and typically do not have significant resources to invest in their security program. Yet small businesses are a prime target for various cyberattacks which can compromise the confidentiality, integrity, and availability of PHI. This research contributes to addressing this resource problem by providing clear insight and direction into these competing

challenges that small business owners face in the healthcare space based on some of the most recent cyber security trends.

Objective of the Research

The objectives of this research are to help drive the HIPAA compliance conversation forward and assist small healthcare entities with developing their cyber security risk management programs.

Research Questions

- How much time and effort does it take to complete a HIPAA risk assessment using the SRA tool?
- What are the key cyber security responsibilities that healthcare providers must own to be HIPAA-compliant and maintain their reputation should a breach occur?
- What should healthcare providers consider when deciding whether to house PHI in the cloud or on-premises?

Limitations of the Research

The SRA tool is a guideline for risk assessments and its use does not guarantee compliance. The scope of the tool is limited to the HIPAA Security Rule, which is a subset of HIPAA compliance.

Definition of Terms

- **BAA**: Business associate agreement. Contract between two businesses for service provided, including liability and responsibilities should a breach or other security incident occur.
- **Clinic A**: Used a cloud service provider to house PHI.

- **Clinic B**: Housed PHI on-premises and included roughly six times more PHI records than Clinic A.
- **CSP**: Cloud service provider. Can be certified as HIPAA-compliant.
- **HHS**: Department of Health and Human Services. They own the SRA tool, provide guidance for HIPAA compliance, and administer HIPAA audits and fines.
- **HIPAA**: Health Insurance Portability and Accountability Act of 1996. This law governs compliance obligations for healthcare providers, which includes cyber security.
- **PHI**: Protected health information. Sensitive patient information protected by HIPAA law.
- **Small healthcare provider**: Less than 50 employees.
- **SRA tool**: Security Risk Assessment tool, provided by HHS as a guideline for HIPAA Security Rule compliance.

Summary

This research aims to provide small healthcare providers with clear guidance to fully own the cyber security risks in their clinical environment. The case studies and analysis provide examples of the level of detail and time commitment one should expect should they opt to use the SRA tool.

Chapter II: Background and Review of Literature

Introduction

This chapter provides greater context for the problem of conducting a HIPAA security risk assessment in compliance with the HIPAA Security Rule. Literature related to cyber risk management in healthcare is reviewed along with literature related to tools which enhance or automate cyber risk management processes.

Background Related to the Problem

Risk assessments are an important method of validating the current state of a cyber security program. Given that cyber security is regarded as an enterprise risk management function, risk assessments encapsulate all components of an organization's security posture. Within the healthcare industry, PHI is some of the most valuable data on the black market and the industry is highly regulated under HIPAA law. HIPAA compliance includes, but is not limited to, the HIPAA Security Rule, HIPAA Privacy Rule and HIPAA Enforcement Rule. Under the HIPAA Security Rule (HHS, 2003), healthcare entities are required to conduct periodic cyber security risk assessments which focus on the administrative, technical, and physical safeguards deployed within the enterprise. The HIPAA Privacy Rule relates to privacy regulations and the HIPAA Enforcement Rule relates to the enforcement of HIPAA provisions. Over the past several years, HHS has levied significant fines against healthcare providers that were noncompliant with HIPAA statutes.

Maximum Possible Fines For HIPAA Violations

Violation	Fines Per Violation	Maximum Fine
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect – (Corrected)	$10,000 - $50,000	$1,500,000
Willful Neglect – (Uncorrected)	$50,000	$1,500,000

Figure 1. The Cost of HIPAA Non-Compliance. (HIPAA Journal, 2015)

As Figure 1 shows, violations can result in fines as high as $1.5 million. Each PHI record in a data breach is considered a violation, so this can add up very quickly for organizations with many records exposed. Figures 2 and 3 show the most recent breach data for 2016. In several cases, the fine exceeded $1.5 million which typically involved multiple breaches or a long history of noncompliance. The largest HIPAA fine to date was levied against Advocate Health Network for just over $5.5 million in August 2016. HHS has prosecuted violations against healthcare entities of all sizes.

Summary of 2016 HIPAA Settlements

Covered Entity	Date	Amount	Breach that triggered OCR investigation	Individuals impacted
University of Massachusetts Amherst (UMass)	November, 2016	$650,000	Malware infection	1,670
St. Joseph Health	October, 2016	$2,140,500	PHI made available through search engines	31,800
Care New England Health System	September, 2016	$400,000	Loss of two unencrypted backup tapes	14,000
Advocate Health Care Network	August, 2016	$5,550,000	Theft of desktop computers, loss of laptop, improper access of data at business associate	3,994,175 (combined total of three separate breaches)
University of Mississippi Medical Center	July, 2016	$2,750,000	Unprotected network drive	10,,000
Oregon Health & Science University	July, 2016	$2,700,000	Loss of unencrypted laptop / Storage on cloud server without BAA	4,361 (combined total of two breaches)
Catholic Health Care Services of the Archdiocese of Philadelphia	June, 2016	$650,000	Theft of mobile device	412 (Combined total)

Figure 2. Summary of 2016 HIPAA Settlements (Part 1). (HIPAA Journal, 2017)

New York Presbyterian Hospital	April, 2016	$2,200,000	Filming of patients by TV crew	Unconfirmed
Raleigh Orthopaedic Clinic, P.A. of North Carolina	April, 2016	$750,000	Improper disclosure to business associate	17,300
Feinstein Institute for Medical Research	March, 2016	$3,900,000	Improper disclosure of research participants' PHI	13,000
North Memorial Health Care of Minnesota	March, 2016	$1,550,000	Theft of laptop computer / Improper disclosure to business associate (discovered during investigation)	299,401
Complete P.T., Pool & Land Physical Therapy, Inc.	February, 2016	$25,000	Improper disclosure of PHI (website testimonials)	Unconfirmed
Lincare, Inc.	February, 2016*	$239,800	Improper disclosure (unprotected documents)	278

*Civil monetary penalty confirmed as lawful by an administrative law judge

Figure 3. Summary of 2016 HIPAA Settlements (Part 2). (HIPAA Journal, 2017)

Much of the attention with respect to cyber security in healthcare has gone to the mid-sized and large providers. These entities typically have more financial and human resources to devote to implementing security measures. With the overwhelming responsibilities that small businesses face in trying to meet the needs of the business, this work aims to address this well-known gap and demystify the cyber risk management process. The review of literature will consider various efforts undertaken by healthcare providers, with an emphasis on smaller providers, to improve their cyber risk posture.

Literature Related to the Problem

The federal government offers a few key resources to assist any small healthcare clinic with cyber risk management and HIPAA compliance. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2014) is the current broad industry standard used in both the public and private sectors. NIST also released a framework specifically geared for small businesses, including small healthcare clinics. (Paulsen & Toth, 2016) The Balridge Cybersecurity Excellence Builder (NIST, 2016) is a self-assessment tool provided by NIST which improves the ability of organizations to understand their cyber risk posture and take appropriate action. HHS provides information specific to HIPAA compliance, including the HIPAA Security Rule. (HHS, n.d.)

According to Morrissey (2017), "The demands of implementing an effective security risk assessment are the most difficult for smaller urban or rural practices, which typically have tight margins" (p. 39). Green, et al. (2015) specifically looked at managing PHI for low monetary resource healthcare providers. They found that these entities are critically lacking in in their ability to maintain a sound cyber risk posture and mentioned that, for many of these providers, “ongoing support will be needed…to remain viable” (p. 17). Blanke & McGrady (2016) created a detailed list of recommendations for security risk assessments based on the most recent data for healthcare data breaches. These recommendations can be foundational for small providers to move forward with their security programs.

Recent cyber risk management case studies have been administered in Canada

(Desouza & Valverde, 2016), Turkey (Namoɬlu & Ülgen, 2014), and Iran (Zarei & Sadoughi, 2016). Each of these cases involved medium or large healthcare organizations, which further suggests this to be an area of need for small healthcare providers in the United States. Lisbon & Rice (2017) used the SRA tool to assess a small dental clinic which utilized a cloud service provider. The methodology and data set from that work are core components of this expanded work.

Security education and awareness training is a key component of a healthcare security program. Fernandez-Aleman, et al. (2015) found a lack of security education and awareness training as well as communication of security expectations led to security lapses in healthcare organizations. He & Johnson (2015) examined how to better implement the lessons learned from security incidents compared with the typical healthcare organization. Bai, et al. (2014) offered a decision-making methodology to improve workflow processes and efficiencies related to cyber risk, attempting to tackle the low-resource problem on the process level in healthcare. Wei, Lin & Loho-Noya (2013) created a quantitative security risk assessment method with an emphasis on managing the risk of PHI.

Enterprise cyber security issues were previously relegated to the IT domain and budget. Andre (2017) makes clear that this outdated approach is untenable and requires a strategic risk management-based approach to address the distinct challenges in healthcare. Cascardo (2016) details numerous risk analysis and risk management steps that healthcare organizations can take to meet compliance obligations and reduce the likelihood of data breaches. Similar prescriptions are offered

by Blass & Miller (2015), with specific recommendations for the creation and maintenance of documentation, regular risk assessments, and appropriate training.

An important healthcare consideration is the inherent conflict of interest between protecting the patient and protecting their data. In certain crisis situations, protecting the patient may supersede protecting their data ethically and under the law. Kisekka (2016) explored this topic in depth by examining the resilience of healthcare IT personnel in their response to extreme healthcare events. She found that a well-prepared organization is more likely to protect the patient in these situations while also safeguarding their PHI, instead of having to make this compromise. This work should give confidence to healthcare providers that a proactive approach to cyber security will reap many benefits.

Continuous improvement is critical to building a resilient cyber security program. The emerging industry standard is maturity, which measures the strength of a security program at the business process level rather than simply checking the box for audit compliance. (Veltsos, 2016) Other recent work (Molnar & Großmann, 2017) proposed a maturity model which encapsulates four angles: tool support, risk assessment, testing, and compliance. Security programs would receive a maturity rating of level 1-5 in each of these areas, with 1 indicating little to no development and 5 indicating a significant level of business processes in place. This type of approach paints a more complete picture of the actual capabilities and processes of an organization’s program and ensures that the leadership of the organization is continuously focused on the next level of maturity that it aims to reach. For small clinics, this may involve just one or two

individuals and can help to better understand the context of their responsibilities.

Contracts are an emerging cyber security priority, particularly with respect to third-party vendors. Small organizations may have dozens of vendor relationships, while large organizations likely have thousands. Travis & Schwartz (2017) indicate several key areas to include in vendor contracts, including a notice and cooperation clause, a cyber security practices clause, and a cyber liability insurance or indemnification clause. Particularly if there is no insurance, they indicate indemnification clauses should be placed separately since the cost of a data breach far exceeds standard indemnification ceilings. Tschider (2016) recommends using standard language and strong contractual terms when negotiating cyber security contracts with cloud service providers. Business Associate Agreements (BAAs) are needed specifically for vendors that deal with PHI directly. (Healthcare Risk Management, 2017)

Literature Related to the Methodology

The SRA tool (ONC, 2016) is owned by HHS and was collaboratively developed by three of its sub-entities: The Office of the National Coordinator (ONC), Office for Civil Rights (OCR) and Office of the General Counsel (OGC). According to HIMSS (2016), the most recently updated version of the SRA tool streamlines the ability of small healthcare providers to comply with the HIPAA Security Rule. In its literature, the ONC makes clear that small healthcare providers are required to conduct HIPAA security risk assessments and that it must be done in a thorough and professional manner. (ONC, n.d.)

Other tools exist in private industry which can supplement the SRA tool functionality. The Health Information Trust Alliance (HITRUST) offers a free information sharing tool, Cyber Threat XChange (CTX), which offers automated threat management for organizations of all sizes. (HITRUST, 2017) This gives healthcare organizations the ability to strengthen their cyber risk posture irrespective of their maturity level. Organizations can also use a free tool to benchmark third-party vendor cyber risks. (CyberGRX, 2017) These results can then be fed into the SRA tool, which may be useful given the complexity of managing third-party cyber risks.

Summary

As the data in this chapter revealed, healthcare providers have a strong incentive to conduct risk assessments for the purposes of HIPAA compliance. Solutions for small healthcare entities have generally been overlooked in the body of knowledge. This allowed for the opportunity to conduct HIPAA security risk assessments using the SRA tool that were specifically geared for this demographic.

Chapter III: Methodology

Introduction

A qualitative risk assessment using the SRA tool was used. Information was gathered in a detailed manner and methodically analyzed with respect to the HIPAA Security Rule requirements

.Design of the Research

The research was conducted in a qualitative manner. While there were data points to reference in the SRA tool, such as risk level and likelihood, these factors were subjectively combined to determine whether the risk level is acceptable or must be mitigated. The HHS website and its guidance within the tool helped to define terms and provide context for what was needed.

Data Collection

Data was collected by interviewing the owner of each clinic to obtain detailed answers to each of the questions within the SRA tool. (ONC, 2016) An experienced security auditor was consulted early in the process to help guide it and ensure its accuracy with current industry trends. Data was entered directly into the tool which later produced a spreadsheet-based report with the fields of each question. Notes were also taken and later consolidated to form the overall picture which will be described in the Data Presentation & Analysis chapter.

Approximately 4-6 hours were spent with the owner of each clinic for the assessment; the first assessment took significantly longer due to it being the first time using the tool. The assessment included doing a physical walk-through of each site and

asking follow-up questions about its configuration. With practice, the entire process of gathering detailed, relevant data should take maybe 1-2 hours. Analyzing, integrating, and presenting the data should take additional time for the assessor.

Data Analysis

The SRA tool consisted of 156 detailed questions and was run as an executable file, which locally stored the data entries within the assessment data file. The context of each question was geared towards protecting PHI through administrative policies, physical access restrictions, or technical safeguards specific to the requirements laid out in the HIPAA Security Rule. Appendix A contains the full list of SRA tool questions for each of these areas.

The three types of questions were standard, required, and addressable. All entities must comply with the standard and required questions. Addressable questions would require an explanation for noncompliance along with documented alternative measures, if appropriate. (ONC, 2016)

For each question, there were fields to detail current efforts, suggest appropriate remediation steps, and mark the risk likelihood and impact. Questions could be flagged for further review at a later time, there was a section for additional notes, and there was a guidance area in the right pane to assist with answering the question. Figure 4 provides additional context.

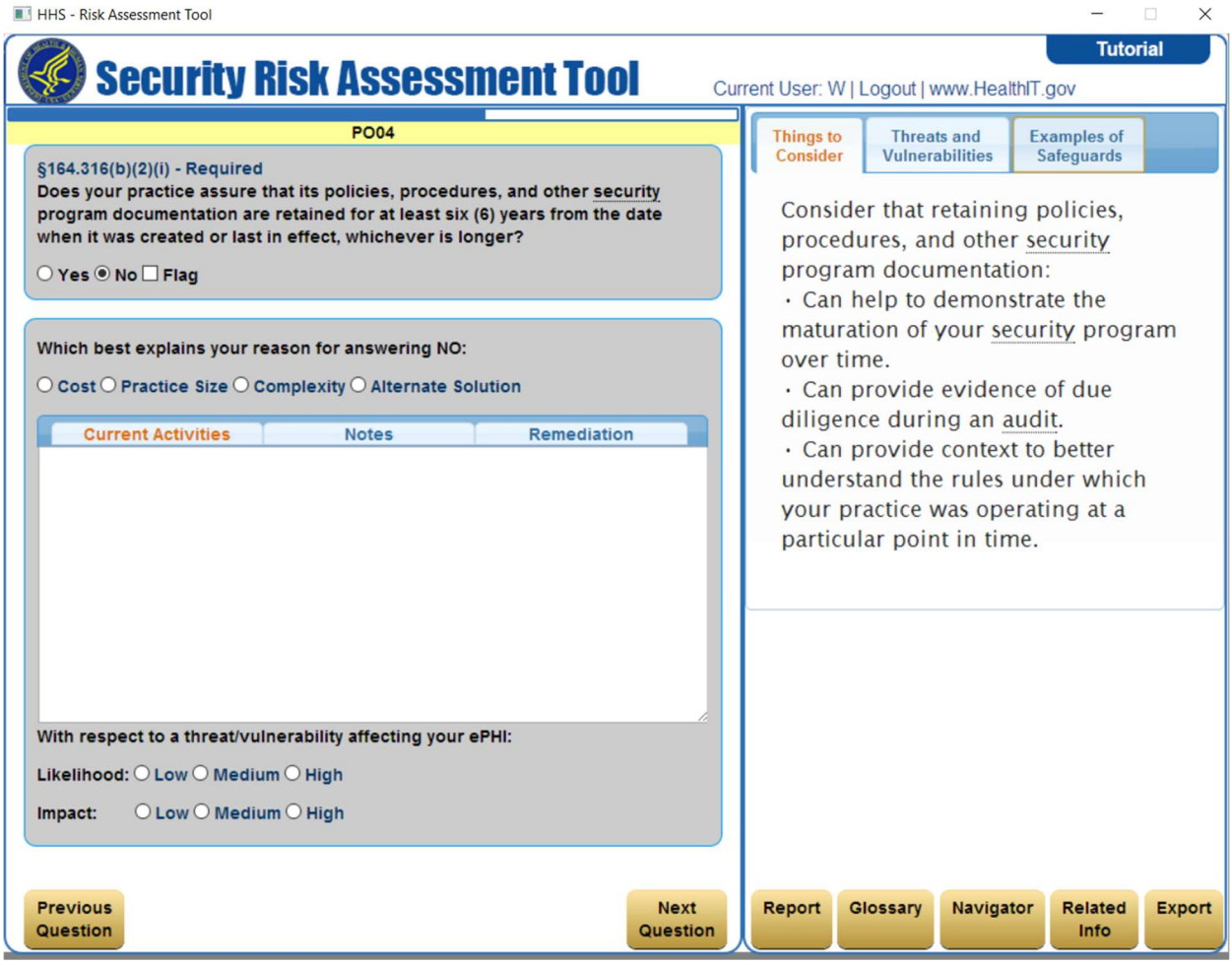

Figure 4. SRA Tool Question Sample

The questions were quite redundant throughout the assessment; it was determined that, out of 156 questions, roughly 100 needed to be answered for the small clinics in these cases. Small entities with one IT staff member, who may be the owner, do not require the granularity of all 156 questions. Each question was qualitatively addressed and compiled within the administrative, technical, and physical control categories to present a clear picture of the cyber risk posture for each case.

Summary

The SRA tool was adapted to fit the needs of these two cases. Overall, it served its purpose by providing a clear guideline for HIPAA Security Rule compliance.

Chapter IV: Data Presentation and Analysis

Introduction

Information was gathered from the two clinics using the SRA tool. Once collected, the information was synthesized and consolidated into a coherent set of data which is presented in this chapter. This chapter also features an analysis of the security gaps uncovered by each assessment as well as a comparative analysis between using the cloud to safeguard PHI vs. housing PHI on-premises.

Data Presentation

As data was entered into the SRA tool during each assessment, it saved the answers and later presented them as a spreadsheet report as shown in Figure 5 (use 2-2.5x zoom):

ID	Answer	Risk Level	Current Activities	Notes	Remediation	Reason	Last Edit
Question: Have you put any of your practice's workstations in public areas?							
PH24	Yes	Low	The receptionist machine is in the main area and there is free access to the 8 workstations in the facility.		Look to further lock down these workstations to avoid intrusions spreading to other devices. Consider implementing workstation monitoring to detect anomalies or problems.	N/A	[W]12/17/2016 8:04:33 pm
Question: Do your practice's policies and procedures require screening workforce members prior to enabling access to its facilities, information systems, and ePHI to verify that users are trustworthy?							
A27	Yes	Low	A thorough criminal background check occurs before anyone is hired; they only hire dental-certified individuals.	W: Speak with office manager regarding specific steps that are taken.		N/A	[W]1/6/2017 12:16:59 pm
Question: Does your practice know the authentication capabilities of its information systems and electronic devices to assure that a uniquely identified user is the one claimed?							
T35	Yes	Low	They use unique accounts and are meeting bare minimum requirements of single-factor authentication.			N/A	[W]1/6/2017 11:35:34 am

Figure 5. SRA Tool Spreadsheet Report

To protect anonymity and preserve space, only samples of the actual data in the SRA tool report are presented in this example. The full data sets will be revealed in this section. Clinic A was initially assessed by Lisbon & Rice (2017); its data presentation is paraphrased in the subsequent sub-section.

It should be noted that Clinic A demonstrated a significantly more mature risk posture than Clinic B. For this reason, the presentation of the data for each clinic varies. Clinic A features more granular detail that correlates more closely to the specific questions of the SRA tool while Clinic B gives a clear picture with some specificity of its relevant cyber security activities. The data analysis will more closely analyze the gaps within Clinic B which reveal its lack of maturity. The concept of maturity in cyber security will be analyzed further in the Discussion chapter.

Case Study: Clinic A. Clinic A employed five people and used eight stationary computing devices. It was responsible for roughly 1,600 patient PHI records. The owner remotely managed the computing environment as needed using a virtual private network (VPN) from home; they had no dedicated IT personnel, so the owner took on all IT and security-related responsibilities. Clinic A used a CSP to safeguard PHI, which effectively transferred a large portion of risk to the CSP for managing it. The clinic owner reported that the cloud architecture itself was HIPAA-compliant, as was the BAA between the entities. It was found that the owner of Clinic A was quite organized with respect to many of the responsibilities outlined in the SRA tool, which will now be detailed according to what the owner reported during the assessment.

Clinic A took many actions in the area of administrative controls. The clinic clearly stated the name of its security point-of-contact in its BAAs related to accessing PHI and handled PHI in a similar manner to financial records such that a reasonable level of security of PHI was maintained. A list of all BAAs was maintained, and they had

an attorney review and sign off on the language of all BAAs. The BAA between the clinic and CSP included termination procedures as well as the handling of PHI.

With regards to employee hiring procedures, Clinic A would only hire dental-certified individuals after performing a thorough criminal background check. When an employee was terminated, they would promptly disable the user's logon access and delete the employee's physical access codes to the building. Their employee handbook served as a guideline for job descriptions in the practice. The handbook included language which explicitly forbade violation of the office PHI policy, which would result in employee termination. Employees also performed cleaning duties.

Clinic A performed segregation of duties with its PHI processes, where possible, including with the processing of cash payments. The clinic owner implemented various levels of access control within the local computing environment as well as the CSP environment with an emphasis on implementing role-based access and least privilege. The owner had full administrative access while the office manager had access to most administrative functions, except for adding and removing users. Other clinical personnel had strictly role-based access for their jobs, including clinical notes and health histories but no other PHI. It is notable that there existed billing codes within the CSP database that abstracted unnecessary PHI details based on access level, which effectively accounted for an additional layer of access control in the day-to-day functioning of the business.

The owner proactively managed both environments in consultation with the CSP to maximize functionality while ensuring there were appropriate access controls on all

electronic devices to maintain the confidentiality and integrity of PHI. Within the clinic environment, this included system reviews, multiple firewalls, operating system updates to all devices, and regular password resets.

Many of the HIPAA Security Rule requirements for technical controls were implemented within the CSP interface. The CSP interface encrypted PHI data at rest and in transit. It had an auto-logoff policy for idle users, which paired with the clinic's auto-logoff policy of 4-6 hours to meet this requirement. The owner followed the CSP's recommendations for security settings within the CSP interface and paired these with practical technical controls in the local environment. The CSP performed regular data backups and maintained an extremely high availability of the service. This meant a service outage was unlikely and the clinic owner determined this was an acceptable business risk. Clinic A did not use shared accounts for any business function and maintained a secure list of authorized users and passwords.

Overall, Clinic A effectively complied with physical security requirements. They used an internal security system which included motion alarms and locks. The system was periodically tested to confirm it was in working order. A third-party security firm managed the protection of the facilities and equipment; the clinic had a BAA with this entity. Clinic employees had free access to the facility during employment. If a breach occurred after hours when the doors were locked, a security team would be promptly dispatched in response.

The owner proactively maintained a Facility User Access List which included active employees as well as accountants who had 1099 form access, but no facility

access. The facility itself was designed to avoid scenarios where a casual passerby could view PHI on clinic devices and the front desk computer was always monitored by staff personnel. Clinic A also maintained an inventory of devices containing PHI and ensured that any physical security measures implemented occurred with minimal impact to the business.

Case Study: Clinic B. Clinic B employed 12 people and used 15 stationary devices. It was responsible for protecting roughly 10,000 PHI records. These records were housed on a desktop device running Windows 7 through the Patterson EagleSoft user interface. Although the device ran a desktop version of Windows, it is otherwise referenced as a server in this work since it provided PHI services for the clinic. The clinic owner was the only individual with logon access to the device and managed it by remotely connecting to it over a VPN as needed. A previous IT contractor set up the entire system which served as a single point of failure for the entire clinic. The clinic owner estimated a daily loss of $8,000 per day if the device stopped working. The owner was unaware of how the device was set up and has consulted EagleSoft, as needed, to keep it running. The owner ran two sets of regular data backups from the device: one went to a cloud backup provider and the other to an external hard drive stored in the office. Clinic personnel were able to send secure HIPAA-compliant email containing PHI out of the EagleSoft interface using a specific version of Microsoft Office. Clinic devices had web browsers installed with free internet access.

Clinic B had an employee handbook, employee termination policies, and BAAs with some, but not all, of its key vendors. They implemented segregation of duties

through receipt of cash payments. Employees were granted role-based access within EagleSoft to only what they needed for their job and clinic devices were managed by the owner with least privilege in mind. A couple of examples of this were that most clinic devices did not have rights to print and employee system access was terminated before they received official termination notice. The clinic owner periodically reviewed and scanned the devices for vulnerabilities to see if there was anything obvious to eliminate from them. The clinic did not use shared accounts and auto-logoff policies existed both within the EagleSoft interface as well as on each clinic device. This ensured that free access to PHI did not exist if a device was left unmonitored.

The clinic contracted with a security company to respond to security alarms after hours. Its internal security system featuring motion alarms and locks had been tested. The facility allowed free access which included the use of open bays. These bays allowed for limited viewing of PHI on a nearby device if another patient was in the area. Other clinic devices were not out in the open or clearly visible to patients walking by. The clinic did not use mobile devices.

Data Analysis

Based on the answers from the assessment and current cyber security knowledge, various gaps were identified and are qualitatively analyzed further in the Gaps Analysis sub-section. The Comparative Analysis sub-section examines some of the critical factors for each clinic to consider as well as the pros and cons of a cloud-based approach to protecting PHI. Similar to the previous section, the gaps analysis involving Clinic A is paraphrased. (Lisbon & Rice, 2017)

Gaps Analysis. During the assessments, various gaps in the security posture of both clinics emerged. Most prominently was the lack of documentation in numerous areas where the respective owners attested compliance as well as numerous other areas of noncompliance.

Documentation is a critical area that HHS demands for HIPAA compliance. If a security incident occurs and there is no documentation to validate an existing process, HHS will regard the entity to be noncompliant. For both clinics, nearly 40% of the questions answered within the SRA tool indicated documentation shortcomings. Both clinic owners performed most of the cyber security processes on an ad hoc basis without proper documentation. The creation and maintenance of documentation is needed in the three HIPAA Security Rule areas of administrative, technical, and physical controls. The following paragraphs spell out an exhaustive list of documentation needs for both healthcare entities.

With regards to administrative documentation, both clinic owners must formally document a security plan and the results from this risk assessment. They should formally document a program to mitigate threats and vulnerabilities to PHI that were mentioned in this risk assessment and classify the risks as high, moderate, or low. Each clinic owner should document their full list of duties as the security point-of-contact.

Each clinic needs to create policies and procedures to assess and manage risk to PHI. In these policies, each practice must describe how its risk management program prevents PHI exposure. Both clinics will need a written policy which explains how they grant role-based access to clinical personnel and business associates. There must be a

policy to explicitly grant access to PHI to those who need it and deny access to others. Within the employee handbook, they should ensure it uses formal termination language, review the termination language for misusing PHI, and include an Acceptable Use section with language about devices being monitored and tracked. Both clinics should create security training documentation that includes sanction policies, how malware can get into systems, and good practices to follow to protect PHI.

Both clinics need to put together a Disaster Recovery Plan (DRP) and Contingency Plan (CP) for emergency situations that may arise. The CP should include how PHI will be handled should a local server or CSP failure occur. Each owner should evaluate when it would be practical to test the CP and document these tests. This includes identifying and assessing the criticality of information systems applications and how PHI would be accessed and stored during the implementation of the CP.

Each clinic should perform several administrative tasks on at least an annual basis. Periodic employee training regarding information security threats to PHI and periodic review of risk assessment policies and procedures should occur. BAA contract language should be reviewed to affirm HIPAA compliance, the CP should be tested, and the employee handbook should be updated as appropriate.

Technical documentation needs to be created by both clinics. They must document their identity verification procedures for an individual who seeks access to PHI as well as their definition of emergencies that are the most likely and have the greatest business impact. These emergency scenarios will drive the DRP and CP documents. Both clinics must also maintain an inventory and location record of all

workstation devices; document employee facility and workstation access; and document the regular review and update of physical security and environmental vulnerabilities.

Physical documentation must include each owner's use of remote access to the facility computing environment, how the positioning of workstations limits unauthorized viewing of PHI, and security procedures for the secure storage and destruction of PHI data. It must also include procedures for the protection of keys, combinations, and other physical access controls. Any modifications or repairs to physical security features must also be documented.

Multiple technical gaps exist within each clinic and will now be addressed in further detail. Both clinics should implement a USB restriction policy on clinic devices. Given that individuals have free facility access during business hours, such a policy should be carefully considered along with its business impact on the appropriate devices. To avoid internet-based threats, both clinics should consider implementing IP whitelisting on clinic machines to avoid web application-based attacks from Internet surfing. Group Policy implementation, web filtering, or virtual machine deployment could also accomplish or supplement efforts towards this goal. Another option is to look at setting up virtual local area networks (VLANs) on the local clinic network where each device would be segregated. This would deter an internet-based intrusion on one device from affecting other devices.

Given that both clinics use network print-fax devices which commonly receive faxed PHI over plain old telephone service (POTS), each print-fax device is vulnerable to physical memory intrusions and internet-based intrusions. Cable locks on these

devices can help prevent this memory from being stolen and VLANs can segment these devices to prevent a compromise should an attacker gain control of another internet-connected office device.

Gaps: Clinic A. The most obvious gap for Clinic A was its use of single-factor authentication over the internet when connecting to the CSP to access PHI records. Most responsible healthcare providers have already moved to multifactor authentication, and Clinic A should initiate conversations with the CSP to make this happen. Passwords are considered weak security over the internet, and this action would likely decrease the liability for the clinic should a breach occur.

Clinic A also had a process gap when it received emails containing PHI. In these situations, they should take special measures to record the information while not retransmitting it over the internet. Replies to emails contain metadata which could allow an unauthorized third party to reconstruct PHI data that was deleted from the message. The clinic should implement a policy where users must not reply directly to any received emails containing PHI. Clinic personnel should create a new email message with no PHI in it to send and ensure that all outgoing messages have a legal disclaimer at the bottom of the email that absolves the clinic of liability for any PHI received. The clinic should also implement an email retention policy based on the knowledge that client PHI may exist in a mailbox folder and should be deleted within a set timeframe.

Clinic A must conduct due diligence to understand and document how the CSP is handling PHI. While these risks were transferred to the CSP for its day-to-day management, it is still the responsibility of the clinic to ensure the CSP is compliant with

HIPAA requirements on a periodic basis. They should verify the existence of any security certification the CSP holds i.e. a service organization controls (SOC) standard. Such certifications clearly communicate the standards of compliance that exist in the CSP environment. They should also check with the CSP regarding specific security measures that are in place, including encryption procedures, backup procedures, and which business associates have access to PHI. Encryption includes data at rest and in transit. Each of these answers should be documented and periodically re-checked by the clinic during annual reviews or risk assessments.

Gaps: Clinic B. There were many gaps within Clinic B that were of a more serious nature than the ones identified within Clinic A. Clinic B lacked a competent management approach which protected the security of PHI. The lone server which ran EagleSoft was a low-maintenance option to keep the business running, but it was a single point of failure that would be costly for the business when it inevitably fails. Its location at the front of the office under the desk was in too open of an area. Additionally, the external hard drive used to back up PHI was located on the front desk near the server for convenience. Securing the external hard drive and moving the server to a more secure location are critical steps that need to occur in short order.

Encrypting data at rest was another critical gap in Clinic B. While EagleSoft had an encryption feature in its current version for data stored on the server, this was not manually implemented by the owner. EagleSoft encrypts its communications between its client program and server calls over the internet. PHI data backed up to the cloud and the external hard drive were not encrypted at rest. The owner used a VPN to

transfer the data, which implies it was encrypted in transit. The owner originally used two backup sources because of the perceived unreliability of the cloud when first deploying the solution several years ago. The cloud backup provider was not HIPAA-compliant, so they need to either choose an appropriate HIPAA-compliant solution with that provider or find a new provider. The owner stayed with this backup provider because it was a free solution. Off-site backups had not been tested and the owner did not have a process in place for maintaining PHI based on HIPAA requirements.

The BAAs with EagleSoft, the cloud backup provider, and other vendors with PHI access need to be reviewed, and in certain cases remediated, to comply with HIPAA requirements. A contingency plan and disaster recovery plan need to be created which address the single point of failure gap for the server containing PHI.

Another gap was logon monitoring. Clinic B did not monitor logons on its devices and the owner did not know to what extent EagleSoft monitored the logons within its interface. This is an area to follow up and document accordingly with the vendor.

The remediation of each of these gaps needs to be documented clearly so that the next iteration of risk assessment for Clinic B can focus more granularly on other core items within the SRA tool.

Comparative Analysis: Cloud vs. On-Premises. By operating in a Software-as-a-Service (SaaS) model, Clinic A transferred the risks of managing PHI encryption, backups, and server redundancy to the CSP. Should a healthcare provider have an interest in managing their own HIPAA-compliant on-premises IT environment, there are several focal points to consider. The advantages of an on-premises setup may include

greater autonomy, lower costs, and a lack of reliance on the internet to do business. Rural areas without high-speed internet may benefit less from the cloud services model. More time will be required to manage an on-premises environment due to the added complexity; this could also be transferred to an IT contractor or managed services provider, which would add to the cost.

The advantages of using the cloud option are greater simplicity and less overhead for the small business. Particularly for non-tech-savvy small business owners, this may be the ideal option. In spite of these benefits, businesses still must conduct due diligence on the CSP for HIPAA compliance, manage the local IT environment effectively, and understand that their business depends on a reliable internet connection. Poor security practices will negate many of the benefits that the cloud provides and potentially result in HIPAA fines.

An additional option to consider is a hybrid cloud deployment, using Clinic B as an example. In one scenario, Clinic B continues to run its primary systems in a modified HIPAA-compliant setup that uses the cloud for failover purposes. The second scenario uses the cloud for primary business functionality and Clinic B maintains its current infrastructure while making appropriate improvements in the event of a cloud or internet failure. The latter might be the most cost-effective option with the costs of operating in a HIPAA-compliant cloud being fairly reasonable. One of the key considerations to this equation is that the clinic owner has a reasonable base of IT knowledge which can be leveraged in a hybrid solution to improve business margins, should there ever be an internet or cloud outage. This is an important distinction compared with someone who

has little knowledge or interest in IT and outsources the IT-related tasks to a contractor. Another way to frame this is that it is a time vs. money trade-off, with a central question being to what degree a business has an interest in investing time in its IT infrastructure.

Summary

This chapter extensively covered the data collected from each case study, analyzed the security gaps within each clinic, and offered a comparative analysis of IT deployment options based on the risk assessment results.

Chapter V: Discussion, Future Work, and Conclusion

Introduction

This chapter includes a discussion of recent cyberattack data involving small businesses, the evolving regulatory landscape, contract caveats, and a further analysis of maturity in the HIPAA context. Numerous areas are identified where future work can build upon the current body of knowledge. It concludes with a summary of the contributions of this work and a final comment on the use of the cloud vs. on-premises solutions.

Discussion

Recent data suggests that only one in four small businesses are well-prepared for a cyberattack (William, 2017) and that 43% of attacks targeted small businesses in 2015, up 25% from 2011. (Sophy, 2016) Furthermore, 60% of small businesses that suffer cyberattacks go out of business within six months. (Miller, 2016) This suggests that currently there is significant opportunity to assist small businesses with improving their security posture and mitigating risks. While these numbers may not be precisely mirrored in the healthcare sector, it is not far-fetched to think that many small healthcare organizations would be crippled by a targeted attack and generally need greater attention placed on their security program.

From a regulatory perspective, the financial incentives continue to shift towards compliance. Growing HIPAA fines, usually after breaches, continue to receive widespread attention. Morrissey (2017) noted that the Medicare Access and Children's Health Insurance Program Reauthorization Act of 2015 added an additional layer of

financial incentives for healthcare providers to prioritize security. Providers who are audited and cannot show documentation of security risk assessments now face a resultant 25% reduction in Medicare reimbursements; if providers are found to have lied about compliance, they are liable to incur at least a five-figure fine. A 25% Medicare reimbursement reduction is a significant incentive for providers who are heavily reliant on these payments. If this requirement continues to be enforced on a broader scale, it may create a larger shift in the approaches of healthcare organizations towards more resilient cyber security practices.

Contract liability is an additional point of emphasis for both clinics. HIPAA-compliant BAAs need to be put in place with new or existing vendors that deal directly with PHI, and periodic audits of BAAs are needed. Healthcare Risk Management (2017) advised that using BAAs for vendors that do not deal with PHI introduces ambiguity with regards to HIPAA regulations. They indicate that it is worth spending time and possibly consulting with an attorney to ensure appropriate BAAs include provisions which are reasonable or favorable. Note that an industry standard that is universally amenable for both parties has yet to emerge. This implies that third-party risk could be a business backbreaker and needs to be given high priority within the security plan.

The maturity of a security program is important to consider when determining how to interpret the results of a risk assessment, with the understanding that risk assessments are an iterative process. It may not be realistic for a small clinic to make a significant jump in its security posture after the first assessment. The signals from HHS are that it wants to see commitment and progress in this realm. If a healthcare provider

can demonstrate that it has taken definitive steps forward with its security program, this can help to avoid or reduce fines that would result from a breach or random audit. Clinic B is on a very basic level of maturity and would need to approach its next iteration quite differently than Clinic A, which is perhaps a level or two higher on the 1-5 maturity scale (Veltsos, 2016).

Future Work

There are many areas where future work can occur. A closer evaluation of the factors from a security standpoint that distinguish small from medium-sized practices would help streamline the learning curve for healthcare providers and empower small providers to maintain a growth mindset with respect to these compliance obligations. An important component to note about this work is that the SRA tool is geared specifically for HIPAA Security Rule compliance, which is a subset of HIPAA compliance. Future work could integrate this risk assessment process within the HIPAA Security Rule with other HIPAA compliance requirements i.e. the HIPAA Privacy Rule. Many of these requirements are less complex than what has been undertaken in this work, yet a holistic overall solution would be most beneficial and practical for healthcare providers to further streamline their compliance processes.

Exploring the knowledge and priority gaps between small healthcare providers could also provide valuable insight into the thinking behind what exists in practice. A well-formulated query of providers could further elicit their needs without causing undue risk about sharing what is likely a weak cyber risk posture in many cases.

Another angle for future consideration is how to improve the experience of using

the SRA tool. The SRA tool is essentially a spreadsheet that does nothing to intelligently automate the output. Integrating the SRA tool with an orchestration technology would give the data more value in an automated workflow. Alternately, the SRA tool could integrate with machine learning technology to take the input from a healthcare provider directly and return output which is relevant and actionable for the business.

The HITRUST CTX partnership with Trend Micro is an important opportunity for healthcare providers to improve the maturity of their threat intelligence capabilities. (HITRUST, 2017) This information sharing opportunity is free to join and future work could deploy this functionality in a small clinical setting to demonstrate the value of the evolving information sharing capabilities for small healthcare providers as a complementary component of a resilient security program.

Contract liability seems to be an area of great opportunities and challenges. Future work could emphasize a deep dive into the dynamics of all perspectives involved in the third-party contractor risk problem and offer targeted analysis which can drive forward a solution that works for all parties. Such work would give small healthcare providers greater clarity and confidence to negotiate BAAs that maintain the resilience of their cyber risk posture.

Conclusion

While not a one-size-fits-all solution, the SRA tool effectively provided an overarching context to conduct HIPAA security risk assessments. The data from both case studies reveals the depth and breadth of knowledge required to effectively assess the cyber risk posture of these organizations. Risk assessments are a serious

undertaking and require a full commitment from the organization to meet HIPAA requirements. Even small healthcare providers are required to safeguard the confidentiality, integrity, and availability of PHI data. Regardless of who contracts with them as a service provider, these organizations own the requirements for HIPAA compliance. Therefore, it is critical that appropriate documentation and BAAs be in place to protect from this growing avenue of risk. Common sense cyber security measures must be followed for other efforts, such as safeguarding PHI using a CSP, to succeed.

Clinic A showed a higher level of maturity than Clinic B by reporting answers that had a high degree of compliance. However, both clinics must add significant documentation to demonstrate compliance in many areas identified by the SRA tool questionnaire. Clinic B had several critical areas to remediate in short order, or else it risks getting caught flat-footed when a breach or other disaster occurs.

The data also provided a window into the two approaches used by these clinics: housing PHI in the cloud vs. on-premises. The cloud is an ideal solution in many ways, and it is cost-effective for businesses that have access to high-speed internet. An on-premises solution is preferable for entities who prefer a more hands-on approach, or perhaps do not want their business to rely on an internet connection. A hybrid cloud option may be preferable in many cases, which can offer the best of both worlds with a modest level of time investment from the business. This ultimately makes whether, and to what degree, to use the cloud a subjective question.

References

Andre, T. (2017). Cybersecurity: An enterprise risk issue. *HFM (Healthcare Financial Management)*, 1-6.

Bai, X., Gopal, R., Nunez, M., & Zhdanov, D. (2014). A decision methodology for managing operational efficiency and information disclosure risk in healthcare processes. *Decision Support Systems*, *57,* 406-416. doi:10.1016/j.dss.2012.10.046

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management*, (1), 14. doi:10.1002/jhrm.21230

Blass, G., & Miller, S.A. (2015). The top ten things your organization should be doing to pass an audit and reduce risk of a breach. *Journal of Healthcare Information Management*, 10-13.

Cascardo, D. (2016). Compliance challenges facing healthcare providers in 2016. *Journal of Medical Practice Management*, *31*(5), 276-279.

CyberGRX. (1). CyberGRX Launches Free Tool to Help Companies Benchmark Third-Party Cyber Risk. *Business Wire (English)*.

Desouza, E., & Valverde, R. (2016). Reducing security incidents in a Canadian PHIPA regulated environment with an employee-based risk management strategy. *Journal of Theoretical & Applied Information Technology*, *90*(2), 197.

Fernández-Alemán, J., Sánchez-Henarejos, A., Toval, A., Sánchez-García, A., Hernández-Hernández, I., & Fernandez-Luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International Journal Of Medical Informatics*, doi:10.1016/j.ijmedinf.2015.01.010

Green, L. A., Potworowski, G., Day, A., May-Gentile, R., Vibbert, D., Maki, B., & Kiesel, L. (2015). Sustaining 'meaningful use' of health information technology in low-resource practices. *Annals of Family Medicine*, *13*(1), 17-22. doi:10.1370/afm.1740

He, Y., & Johnson, C. (2015). Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template. *International Journal of Medical Informatics*, *84,* 941-949. doi:10.1016/j.ijmedinf.2015.08.010

HHS. (2003). Health insurance reform: Security standards; final rule. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

HHS. (n.d.). HIPAA for Professionals. Retrieved from https://www.hhs.gov/hipaa/for-professionals

HIPAA Journal. (2015). The Cost of HIPAA Non-Compliance. Retrieved from http://www.hipaajournal.com/the-cost-of-hipaa-non-compliance-2843/

HIPAA Journal. (2017). Summary of 2016 HIPAA Settlements. Retrieved from https://www.hipaajournal.com/ocr-hipaa-enforcement-summary-2016-hipaa-settlements-8646/

HITRUST. (2017). HITRUST and Trend Micro Advance the State of Cyber Threat Information Sharing to Cyber Threat Management. *Business Wire (English)*.

Kisekka, V. (2016). Managing information technology extreme events in healthcare organizations: An investigation of individual resilience, performance, and information assurance. *Dissertation Abstracts International Section A*, *77*.

Lisbon, S., & Rice, E. (2017, April 7-8). *Case Study: Information Security Risk Assessment for a Small Healthcare Clinic Using the Security Risk Assessment Tool Provided by HealthIT.gov*. Paper presented at the Midwest Instruction and Computing Symposium, La Crosse, WI.

Miller, G. (2016). 60% of small companies that suffer a cyber attack are out of business within six months. *The Denver Post*. Retrieved from https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

Molnar, A., & Großmann, J. (2017). CRSTIP - An Assessment Scheme for Security Assessment Processes. doi:10.1109/ISSREW.2014.16

Morrissey, J. (2017). Mips Raises the Bar on Security: Risk assessment requirement could cut into reimbursement. *Health Data Management*, *25*(4), 1.

Namoɬlu, N., & Ülgen, Y. (2014). Network security vulnerabilities and personal privacy issues in healthcare information systems: A case study in a private hospital. Paper presented at the *2014 18th National Biomedical Engineering Meeting, BIYOMUT 2014,* doi:10.1109/BIYOMUT.2014.7026385

NIST. (2014). Framework for improving critical infrastructure cybersecurity. Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NIST. (2016). Balridge cybersecurity excellence builder. Retrieved from https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf

ONC for Health Information Technology. (2016). Security risk assessment tool. Retrieved from https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

ONC for Health Information Technology. (n.d.). Top 10 Myths of Security Risk Analysis. Retrieved from https://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis

Paulsen, C., & Toth, P. (2016). Small business information security: The fundamentals. *NIST*. Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

Sophy, J. (2016). 43 Percent of Cyber Attacks Target Small Business. *Small Business Trends*. Retrieved from https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html

Tschider, C. (2016). Storing Data in the Cloud & Crafting Your Contract Carefully. *C-Level Magazine*. Retrieved from http://digital.ipcprintservices.com/publication/?i=346226&article_id=2608602&view=articleBrowser&ver=html5#{%22issue_id%22:346226,%22view%22:%22articleBrowser%22,%22article_id%22:%222608602%22}

Travis, F., & Schwartz, M. (2017, May). Using contracts to curb cyberrisks. *Risk Management*, *64*(4), 16+.

Veltsos, C. (2016). Maturity Assessment, Profile, and Plan: A MAPP to Clearer Information Security. Retrieved from http://trustsds.com/downloads/white-papers/MAPP-Information-Security.pdf

What You Think You Know About HIPAA Might Be Wrong. (2017). *Healthcare Risk Management*, *39*(6), 1-3.

Wei, J., Lin, B., & Meiga, L. (2013). Development of an e-healthcare information security risk assessment method. *Journal of Database Management*, *24*(1), 36-57. doi:10.4018/jdm.2013010103

William, D. (2017). Only 1 in 4 Small Businesses Well Prepared for Cyber Attack. *Small Business Trends*. Retrieved from https://smallbiztrends.com/2017/07/prepared-for-a-cyber-attack-small-business.html

Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. *Risk Management and Healthcare Policy*, *9,* 75-85. doi:10.2147/RMHP.S99908

Appendix: SRA Tool Questions

Administrative Safeguards

- **A1 - §164.308(a)(1)(i) Standard** Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its electronic protected health information (ePHI)?
- **A2 - §164.308(a)(1)(i) Standard** Does your practice have a process for periodically reviewing its risk analysis policies and procedures and making updates as necessary?
- **A3 - §164.308(a)(1)(ii)(A) Required** Does your practice categorize its information systems based on the potential impact to your practice should they become unavailable?
- **A4 - §164.308(a)(1)(ii)(A) Required** Does your practice periodically complete an accurate and thorough risk analysis, such as upon occurrence of a significant event or change in your business organization or environment?
- **A5 - §164.308(a)(1)(ii)(B) Required** Does your practice have a formal documented program to mitigate the threats and vulnerabilities to ePHI identified through the risk analysis?
- **A6 - §164.308(a)(1)(ii)(B) Required** Does your practice assure that its risk management program prevents against the impermissible use and disclosure of ePHI?
- **A7 - §164.308(a)(1)(ii)(B) Required** Does your practice document the results of its risk analysis and assure the results are distributed to appropriate members of

the workforce who are responsible for mitigating the threats and vulnerabilities to ePHI identified through the risk analysis?

- **A8 - §164.308(a)(1)(ii)(B) Required** Does your practice formally document a security plan?
- **A9 - §164.308(a)(1)(ii)(C) Required** Does your practice have a formal and documented process or regular human resources policy to discipline workforce members who have access to your organization's ePHI if they are found to have violated the office's policies to prevent system misuse, abuse, and any harmful activities that involve your practice's ePHI?
- **A10 - §164.308(a)(1)(ii)(C) Required** Does your practice include its sanction policies and procedures as part of its security awareness and training program for all workforce members?
- **A11 - §164.308(a)(1)(ii)(D) Required** Does your practice have policies and procedures for the review of information system activity?
- **A12 - §164.308(a)(1)(ii)(D) Required** Does your practice regularly review information system activity?
- **A13 - §164.308(a)(2) Required** Does your practice have a senior-level person whose job it is to develop and implement security policies and procedures or act as a security point of contact?
- **A14 - §164.308(a)(2) Required** Is your practice's security point of contact qualified to assess its security protections as well as serve as the point of contact for security policies, procedures, monitoring, and training?

- **A15 - §164.308(a)(2) Required** Does your practice have a job description for its security point of contact that includes that person's duties, authority, and accountability?
- **A16 - §164.308(a)(2) Required** Does your practice make sure that its workforce members and others with authorized access to your ePHI know the name and contact information for its security point of contact and know to contact this person if there are any security problems?
- **A17 - §164.308(a)(3)(i) Required** Does your practice have a list that includes all members of its workforce, the roles assigned to each, and the corresponding access that each role enables for your practice’s facilities, information systems, electronic devices, and ePHI?
- **A18 - §164.308(a)(3)(i) Required** Does your practice know all business associates and the access that each requires for your practice’s facilities, information systems, electronic devices, and ePHI?
- **A19 - §164.308(a)(3)(i) Required** Does your practice clearly define roles and responsibilities along logical lines and assures that no one person has too much authority for determining who can access your practice's facilities, information systems, and ePHI?
- **A20 - §164.308(a)(3)(i) Required** Does your practice have policies and procedures that make sure those who need access to ePHI have access and those who do not are denied such access?

- **A21 - §164.308(a)(3)(i) Required** Has your practice chosen someone whose job duty is to decide who can access ePHI (and under what conditions) and to create ePHI access rules that others can follow?
- **A22 - §164.308(a)(3)(ii)(A) Addressable** Does your practice define roles and job duties for all job functions and keep written job descriptions that clearly set forth the qualifications?
- **A23 - §164.308(a)(3)(ii)(A) Addressable** Does your practice have policies and procedures for access authorization that support segregation of duties?
- **A24 - §164.308(a)(3)(ii)(A) Addressable** Does your practice implement procedures for authorizing users and changing authorization permissions?
- **A25 - §164.308(a)(3)(ii)(A) Addressable** Do your practice's policies and procedures for access authorization address the needs of those who are not members of its workforce?
- **A26 - §164.308(a)(3)(ii)(B) Addressable** Does your organization have policies and procedures that authorize members of your workforce to have access to ePHI and describe the types of access that are permitted?
- **A27 - §164.308(a)(3)(ii)(B) Addressable** Do your practice's policies and procedures require screening workforce members prior to enabling access to its facilities, information systems, and ePHI to verify that users are trustworthy?
- **A28 - §164.308(a)(3)(ii)(C) Addressable** Does your practice have policies and procedures for terminating authorized access to its facilities, information systems, and ePHI once the need for access no longer exists?

- **A29 - §164.308(a)(3)(ii)(C) Addressable** Does your practice have formal policies and policies and procedures to support when a workforce member's employment is terminated and/or a relationship with a business associate is terminated?
- **A30 - §164.308(a)(4)(i) Standard** Do your practice's policies and procedures describe the methods it uses to limit access to its ePHI?
- **A31 - §164.308(a)(4)(ii)(B)** Does your practice have policies and procedures that explain how it grants access to ePHI to its workforce members and to other entities (business associates)?
- **A32 - §164.308(a)(4)(ii)(C) Addressable** Do the roles and responsibilities assigned to your practice's workforce members support and enforce segregation of duties?
- **A33 - §164.308(a)(4)(ii)(C) Addressable** Does your practice's policies and procedures explain how your practice assigns user authorizations (privileges), including the access that are permitted?
- **A34 - §164.308(a)(5)(i) Standard** Does your practice have a training program that makes each individual with access to ePHI aware of security measures to reduce the risk of improper access, uses, and disclosures?
- **A35 - §164.308(a)(5)(i) Standard** Does your practice periodically review and update its security awareness and training program in response to changes in your organization, facilities or environment?
- **A36 - §164.308(a)(5)(i) Standard** Does your practice provide ongoing basic security awareness to all workforce members, including physicians?

- **A37 - §164.308(a)(5)(i) Standard** Does your practice provide role-based training to all new workforce members?
- **A38 - §164.308(a)(5)(i) Standard** Does your practice keep records that detail when each workforce member satisfactorily completed periodic training?
- **A39 - §164.308(a)(5)(ii)(A) Addressable** As part of your practice's ongoing security awareness activities, does your practice prepare and communicate periodic security reminders to communicate about new or important issues?
- **A40 - §164.308(a)(5)(ii)(B) Addressable** Does your practice's awareness and training content include information about the importance of implementing software patches and updating antivirus software when requested?
- **A41 - §164.308(a)(5)(ii)(B) Addressable** Does your practice's awareness and training content include information about how malware can get into your systems?
- **A42 - §164.308(a)(5)(ii)(C) Addressable** Does your practice include log-in monitoring as part of its awareness and training programs?
- **A43 - §164.308(a)(5)(ii)(D) Addressable** Does your practice include password management as part of its awareness and training programs?
- **A44 - §164.308(a)(6)(i) Standard** Does your practice have policies and procedures designed to help prevent, detect and respond to security incidents?
- **A45 - §164.308(a)(6)(ii) Required** Does your practice have incident response policies and procedures that assign roles and responsibilities for incident response?

- **A46 - §164.308(a)(6)(ii) Required** Does your practice identify members of its incident response team and assure workforce members are trained and that incident response plans are tested?
- **A47 - §164.308(a)(6)(ii) Required** Does your practice's incident response plan align with its emergency operations and contingency plan, especially when it comes to prioritizing system recovery actions or events to restore key processes, systems, applications, electronic device and media, and information (such as ePHI)?
- **A48 - §164.308(a)(6)(ii) Required** Does your practice implement the information system's security protection tools to protect against malware?
- **A49 - §164.308(a)(7)(i) Standard** Does your practice know what critical services and ePHI it must have available to support decision making about a patient's treatment during an emergency?
- **A50 - §164.308(a)(7)(i) Standard** Does your practice consider how natural or man-made disasters could damage its information systems or prevent access to ePHI and develop policies and procedures for responding to such a situation?
- **A51 - §164.308(a)(7)(i) Standard** Does your practice regularly review/update its contingency plan as appropriate?
- **A52 - §164.308(a)(7)(ii)(A) Required** Does your practice have policies and procedures for the creation and secure storage of an electronic copy of ePHI that would be used in the case of system breakdown or disaster?

- **A53 - §164.308(a)(7)(ii)(B) Required** Does your practice have policies and procedures for contingency plans to provide access to ePHI to continue operations after a natural or human-made disaster?
- **A54 - §164.308(a)(7)(ii)(C) Required** Does your practice have an emergency mode operations plan to ensure the continuation of critical business processes that must occur to protect the availability and security of ePHI immediately after a crisis situation?
- **A55 - §164.308(a)(7)(ii)(D) Addressable** Does your practice have policies and procedures for testing its contingency plans on a periodic basis?
- **A56 - §164.308(a)(7)(ii)(E) Addressable** Does your practice implement procedures for identifying and assessing the criticality of its information system applications and the storage of data containing ePHI that would be accessed through the implementation of its contingency plans?
- **A57 - §164.308(a)(8) Standard** Does your practice maintain and implement policies and procedures for assessing risk to ePHI and engaging in a periodic technical and non-technical evaluation in response to environmental or operational changes affecting the security of your practice's ePHI?
- **A58 - §164.308(a)(8) Standard** Does your practice periodically monitor its physical environment, business operations, and information system to gauge the effectiveness of security safeguards?

- **A59 - §164.308(a)(8) Standard** Does your practice identify the role responsible and accountable for assessing risk and engaging in ongoing evaluation, monitoring, and reporting?
- **A60 - §164.308(b)(1) Standard** Does your practice identify the role responsible and accountable for making sure that business associate agreements are in place before your practice enables a service provider to begin to create, access, store or transmit ePHI on your behalf?
- **A61 - §164.308(b)(1) Standard** Does your practice maintain a list of all of its service providers, indicating which have access to your practice's facilities, information systems and ePHI?
- **A62 - §164.308(b)(1) Standard** Does your practice have policies and implement procedures to assure it obtains business associate agreements?
- **A63 - §164.308(b)(2) Required** If your practice is the business associate of another covered entity and your practice has subcontractors performing activities to help carry out the activities that you have agreed to carry out for the other covered entity that involve ePHI, does your practice require these subcontractors to provide satisfactory assurances for the protection of the ePHI?
- **A64 - §164.308(b)(3) Required** Does your practice execute business associate agreements when it has a contractor creating, transmitting or storing ePHI?
- **O1 - §164.314(a)(1)(i) Standard** Does your practice assure that its business associate agreements include satisfactory assurances for safeguarding ePHI?

- **O2 - §164.314(a)(2)(i) Required** Do the terms and conditions of your practice's business associate agreements state that the business associate will implement appropriate security safeguards to protect the privacy, confidentiality, integrity, and availability of ePHI that it collects, creates, maintains, or transmits on behalf of the practice and timely report security incidents to your practice?
- **O3 - §164.314(a)(2)(iii) Required** If your practice is the business associate of a covered entity do the terms and conditions of your practice's business associate agreements state that your subcontractor (business associate) will implement appropriate security safeguards to protect the privacy, confidentiality, integrity, and availability of ePHI that it collects, creates, maintains, or transmits on behalf of the covered entity?
- **PO1 -§164.316(a) Standard** Do your practice's processes enable the development and maintenance of policies and procedures that implement risk analysis, informed risk-based decision making for security risk mitigation, and effective mitigation and monitoring that protects the privacy, confidentiality, integrity, and availability of ePHI?
- **PO2 - §164.316(b)(1)(i) Standard** Does your practice assure that its policies and procedures are maintained in a manner consistent with other business records?
- **PO3 - §164.316(b)(1)(ii) Standard** Does your practice assure that its other security program documentation is maintained in written manuals or in electronic form?

- **PO4 - §164.316(b)(2)(i) Required** Does your practice assure that its policies, procedures, and other security program documentation are retained for at least six (6) years from the date when it was created or last in effect, whichever is longer?
- **PO5 - §164.316(b)(2)(ii) Required** Does your practice assure that its policies, procedures and other security program documentation are available to those who need it to perform the responsibilities associated with their role?
- **PO6 - §164.316(b)(2)(iii) Required** Does your practice assure that it periodically reviews and updates (when needed) its policies, procedures, and other security program documentation?

Technical Safeguards

- **T1 - §164.312(a)(1) Standard** Does your practice have policies and procedures requiring safeguards to limit access to ePHI to those persons and software programs appropriate for their role?
- **T2 - § 164.312(a)(1) Standard** Does your practice have policies and procedures to grant access to ePHI based on the person or software programs appropriate for their role?
- **T3 - §164.312(a)(1) Standard** Does your practice analyze the activities performed by all of its workforce and service providers to identify the extent to which each needs access to ePHI?
- **T4 - §164.312(a)(1) Standard** Does your practice identify the security settings for each of its information systems and electronic devices that control access?

- **T5 - §164.312(a)(2)(i) Required** Does your practice have policies and procedures for the assignment of a unique identifier for each authorized user?
- **T6 - §164.312(a)(2)(i) Required** Does your practice require that each user enter a unique user identifier prior to obtaining access to ePHI?
- **T7 - §164.312(a)(2)(ii) Required** Does your practice have policies and procedures to enable access to ePHI in the event of an emergency?
- **T8 - §164.312(a)(2)(ii) Required** Does your practice define what constitutes an emergency and identify the various types of emergencies that are likely to occur?
- **T9 - §164.312(a)(2)(ii) Required** Does your practice have policies and procedures for creating an exact copy of ePHI as a backup?
- **T10 - §164.312(a)(2)(ii) Required** Does your practice back up ePHI by saving an exact copy to a magnetic disk/tape or a virtual storage, such as a cloud environment?
- **T11 - §164.312(a)(2)(ii) Required** Does your practice have back up information systems so that it can access ePHI in the event of an emergency or when your practice's primary systems become unavailable?
- **T12 - §164.312(a)(2)(ii) Required** Does your practice have the capability to activate emergency access to its information systems in the event of a disaster?
- **T13 - §164.312(a)(2)(ii) Required** Does your practice have policies and procedures to identify the role of the individual accountable for activating emergency access settings when necessary?

- **T14 - §164.312(a)(2)(ii) Required** Does your practice designate a workforce member who can activate the emergency access settings for your information systems?
- **T15 - §164.312(a)(2)(ii) Required** Does your practice test access when evaluating its ability to continue accessing ePHI and other health records during an emergency?
- **T16 - §164.312(a)(2)(ii) Required** Does your practice effectively recover from an emergency and resume normal operations and access to ePHI?
- **T17 - §164.312(a)(2)(iii) Addressable** Does your practice have policies and procedures that require an authorized user's session to be automatically logged-off after a predetermined period of inactivity?
- **T18 - §164.312(a)(2)(iii) Addressable** Does a responsible person in your practice know the automatic logoff settings for its information systems and electronic devices?
- **T19 - §164.312(a)(2)(ii) Addressable** Does your practice activate an automatic logoff that terminates an electronic session after a predetermined period of user inactivity?
- **T20 - §164.312(a)(2)(iv) Addressable** Does your practice have policies and procedures for implementing mechanisms that can encrypt and decrypt ePHI?
- **T21 - §164.312(a)(2)(iv) Addressable** Does your practice know the encryption capabilities of its information systems and electronic devices?

- **T22 - §164.312(a)(2)(iv) Addressable** Does your practice control access to ePHI and other health information by using encryption/decryption methods to deny access to unauthorized users?
- **T23 - §164.312(b) Standard** Does your practice have policies and procedures identifying hardware, software, or procedural mechanisms that record or examine information systems activities?
- **T24 - §164.312(b) Standard** Does your practice identify its activities that create, store, and transmit ePHI and the information systems that support these business processes?
- **T25 - §164.312(b) Standard** Does your practice categorize its activities and information systems that create, transmit or store ePHI as high, moderate or low risk based on its risk analyses?
- **T26 - §164.312(b) Standard** Does your practice use the evaluation from its risk analysis to help determine the frequency and scope of its audits, when identifying the activities that will be tracked?
- **T27 - §164.312(b) Standard** Does your practice have audit control mechanisms that can monitor, record and/or examine information system activity?
- **T28 - §164.312(b) Standard** Does your practice have policies and procedures for creating, retaining, and distributing audit reports to appropriate workforce members for review?
- **T29 - §164.312(b) Standard** Does your practice generate the audit reports and distribute them to the appropriate people for review?

- **T30 - §164.312(b) Standard** Does your practice have policies and procedures establishing retention requirements for audit purposes?
- **T31 - §164.312(b) Standard** Does your practice retain copies of its audit/access records?
- **T32 - §164.312(c)(1) Standard** Does your practice have policies and procedures for protecting ePHI from unauthorized modification or destruction?
- **T33 - §164.312(c)(2) Addressable** Does your practice have mechanisms to corroborate that ePHI has not been altered, modified or destroyed in an unauthorized manner?
- **T34 - §164.312(d) Required** Does your practice have policies and procedures for verification of a person or entity seeking access to ePHI is the one claimed?
- **T35 - §164.312(d) Required** Does your practice know the authentication capabilities of its information systems and electronic devices to assure that a uniquely identified user is the one claimed?
- **T36 - §164.312(d) Required** Does your practice use the evaluation from its risk analysis to select the appropriate authentication mechanism?
- **T37 - §164.312(d) Required** Does your practice protect the confidentiality of the documentation containing access control records (list of authorized users and passwords)?
- **T38 - §164.312(e)(1) Standard** Does your practice have policies and procedures for guarding against unauthorized access of ePHI when it is transmitted on an electronic network?

- **T39 - §164.312(e)(1) Standard** Do your practice implement safeguards, to assure that ePHI is not accessed while en-route to its intended recipient?
- **T40 - §164.312(e)(2)(i) Addressable** Does your practice know what encryption capabilities are available to it for encrypting ePHI being transmitted from one point to another?
- **T41 - §164.312(e)(2)(i) Addressable** Does your practice take steps to reduce the risk that ePHI can be intercepted or modified when it is being sent electronically?
- **T42 - §164.312(e)(2)(i) Addressable** Does your practice implement encryption as the safeguard to assure that ePHI is not compromised when being transmitted from one point to another?
- **T44 - §164.312(e)(2)(ii) Addressable** Does your practice have policies and procedures for encrypting ePHI when deemed reasonable and appropriate?
- **T45 - §164.312(e)(2)(ii) Addressable** When analyzing risk, does your practice consider the value of encryption for assuring the integrity of ePHI is not accessed or modified when it is stored or transmitted?

Physical Safeguards

- **PH1 - §164.310(a)(1) Standard** Do you have an inventory of the physical systems, devices, and media in your office space that are used to store or contain ePHI?

- **PH2 - §164.310(a)(1) Standard** Do you have policies and procedures for the physical protection of your facilities and equipment? This includes controlling the environment inside the facility.
- **PH3 - §164.310(a)(1) Standard** Do you have policies and procedures for the physical protection of your facilities and equipment? This includes controlling the environment inside the facility.
- **PH4 - §164.310(a)(1) Standard** Do you have physical protections in place to manage physical security risks, such as a) locks on doors and windows and b) cameras in nonpublic areas to monitor all entrances and exits?
- **PH5 - §164.310(a)(2)(i) Addressable** Do you plan and coordinate physical (facilities) and technical (information systems, mobile devices, or workstations) security-related activities (such as testing) before doing such activities to reduce the impact on your practice assets and individuals?
- **PH6 - §164.310(a)(2)(i) Addressable** Have you developed policies and procedures that plan for your workforce (and your information technology service provider or contracted information technology support) to gain access to your facility and its ePHI during a disaster?
- **PH7 - §164.310(a)(2)(i) Addressable** If a disaster happens, does your practice have another way to get into your facility or offsite storage location to get your ePHI?
- **PH8 - §164.310(a)(2)(ii) Addressable** Do you have policies and procedures for the protection of keys, combinations, and similar physical access controls?

- **PH9 - §164.310(a)(2)(ii) Addressable** Do you have policies and procedures governing when to re-key locks or change combinations when, for example, a key is lost, a combination is compromised, or a workforce member is transferred or terminated?
- **PH10 - §164.310(a)(2)(ii) Addressable** Do you have a written facility security plan?
- **PH11 - §164.310(a)(2)(ii) Addressable** Do you take the steps necessary to implement your facility security plan?
- **PH12 - §164.310(a)(2)(iii) Addressable** Do you have a Facility User Access List of workforce members, business associates, and others who are authorized to access your facilities where ePHI and related information systems are located?
- **PH13 - §164.310(a)(2)(iii) Addressable** Do you periodically review and approve a Facility User Access List and authorization privileges, removing from the Access List personnel no longer requiring access?
- **PH14 - §164.310(a)(2)(iii) Addressable** Does your practice have procedures to control and validate someone’s access to your facilities based on that person’s role or job duties?
- **PH15 - §164.310(a)(2)(iii) Addressable** Do you have procedures to create, maintain, and keep a log of who accesses your facilities (including visitors), when the access occurred, and the reason for the access?

- **PH16 - §164.310(a)(2)(iii) Addressable** Has your practice determined whether monitoring equipment is needed to enforce your facility access control policies and procedures?
- **PH17 - §164.310(a)(2)(iv) Addressable** Do you have maintenance records that include the history of physical changes, upgrades, and other modifications for your facilities and the rooms where information systems and ePHI are kept?
- **PH18 - §164.310(a)(2)(iv) Addressable** Do you have a process to document the repairs and modifications made to the physical security features that protect the facility, administrative offices, and treatment areas?
- **PH19 - §164.310(b) Standard** Does your practice keep an inventory and a location record of all of its workstation devices?
- **PH20 - §164.310(b) Standard** Has your practice developed and implemented workstation use policies and procedures?
- **PH21 - §164.310(b) Standard** Has your practice documented how staff, employees, workforce members, and non-employees access your workstations?
- **PH22 - §164.310(c) Standard** Does your practice have policies and procedures that describe how to prevent unauthorized access of unattended workstations?
- **PH23 - §164.310(c) Standard** Does your practice have policies and procedures that describe how to position workstations to limit the ability of unauthorized individuals to view ePHI?
- **PH24 - §164.310(c) Standard** Have you put any of your practice's workstations in public areas?

- **PH25 - §164.310(c) Standard** Does your practice use laptops and tablets as workstations? If so, does your practice have specific policies and procedures to safeguard these workstations?
- **PH26 - §164.310(c) Standard** Does your practice have physical protections in place to secure your workstations?
- **PH27 - §164.310(c) Standard** Do you regularly review your workstations' locations to see which areas are more vulnerable to unauthorized use, theft, or viewing of the data?
- **PH28 - §164.310(c) Standard** Does your practice have physical protections and other security measures to reduce the chance for inappropriate access of ePHI through workstations? This could include using locked doors, screen barriers, cameras, and guards.
- **PH29 - §164.310(c) Standard** Do your policies and procedures set standards for workstations that are allowed to be used outside of your facility?
- **PH30 - §164.310(d)(1) Standard** Does your practice have security policies and procedures to physically protect and securely store electronic devices and media inside your facility(ies) until they can be securely disposed of or destroyed?
- **PH31 - §164.310(d)(1) Standard** Do you remove or destroy ePHI from information technology devices and media prior to disposal of the device?
- **PH32 - §164.310(d)(1) Standard** Do you maintain records of the movement of electronic devices and media inside your facility?

- **PH33 - §164.310(d)(1) Standard** Have you developed and implemented policies and procedures that specify how your practice should dispose of electronic devices and media containing ePHI?
- **PH34 - §164.310(d)(2)(i) Required** Do you require that all ePHI is removed from equipment and media before you remove the equipment or media from your facilities for offsite maintenance or disposal?
- **PH35 - §164.310(d)(2)(ii) Required** Do you have procedures that describe how your practice should remove ePHI from its storage media/ electronic devices before the media is re-used?
- **PH36 - §164.310(d)(2)(iii) Addressable** Does your practice maintain a record of movements of hardware and media and the person responsible for the use and security of the devices or media containing ePHI outside the facility?
- **PH37 - §164.310(d)(2)(iii) Addressable** Do you maintain records of employees removing electronic devices and media from your facility that has or can be used to access ePHI?
- **PH38 - §164.310(d)(2)(iv) Addressable** Does your organization create backup files prior to the movement of equipment or media to ensure that data is available when it is needed?