Case Study: Information Security Risk Assessment for a Small Healthcare Clinic Using the Security Risk Assessment Tool Provided by HealthIT.gov

Scott Lisbon
M.S. in Information Assurance
St. Cloud State University
St. Cloud, MN 56301
salisbon@stcloudstate.edu

Erich Rice
Department of Information Systems
St. Cloud State University
St. Cloud, MN 56301
eprice@stcloudstate.edu

Abstract

Information security risk assessments in the healthcare industry are legally required and demand an ongoing investment of time and resources. Small clinics, in particular, are less likely to have streamlined processes in place to meet these requirements. In this case study, we evaluate a small dental clinic using an assessment tool recommended by the federal government to cover the main benchmarks required by law. We found that the clinic owner demonstrated a proactive approach which balances security needs with business functionality. We identified several areas where improvements could be made, which included addressing vulnerabilities, improving communication with key business associates, and creating an appropriate level of documentation to validate existing processes. This clinic is likely ahead of the security curve and yet still was found to be vulnerable in key areas, a cautionary tale for other healthcare providers who have yet to initiate serious efforts in this area.

1 Introduction

Information security in healthcare is a major topic of interest today given the high value of electronic protected health information (ePHI) on the black market. Healthcare organizations of all sizes must comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (HHS, 2003) or potentially face large fines that result from a security breach. No company wants to be the next data breach victim due to a lack of common sense security controls and suffer reputational damage as a result.

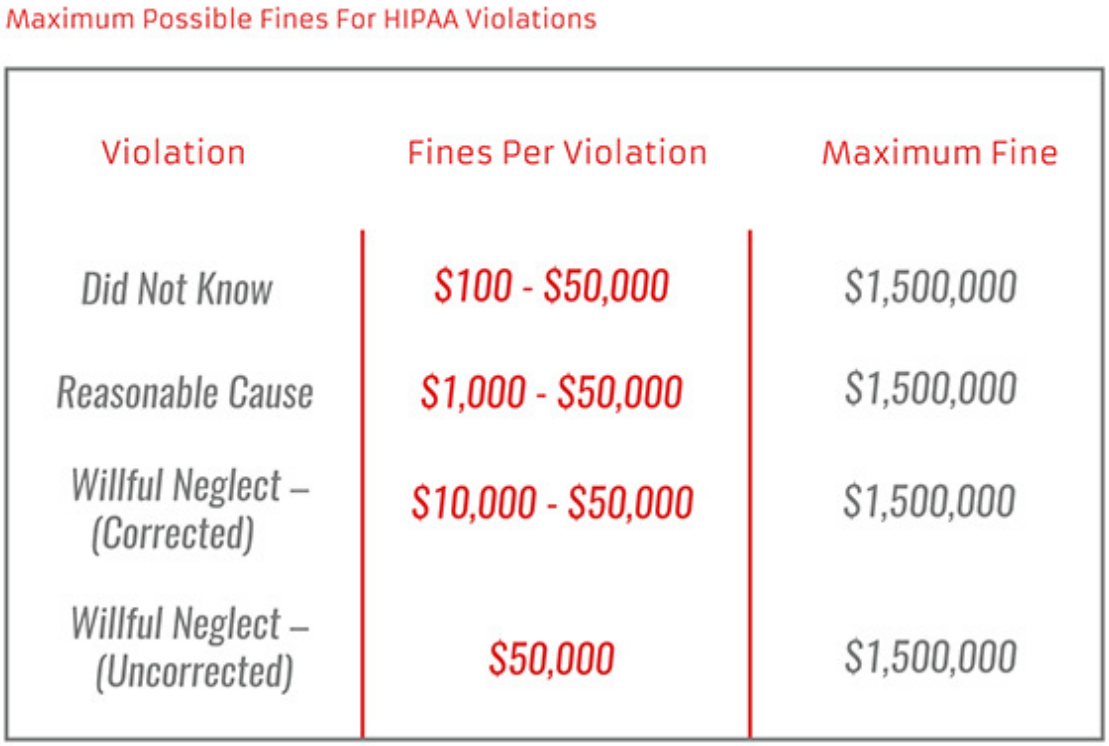

Figure 1: Maximum Possible Fines for HIPAA Violations

The Security Risk Assessment (SRA) Tool provided by HealthIT.gov is designed to meet this challenge for healthcare companies of all sizes. (ONC, 2016) Using the updated version of the tool released in October 2016, we visited a small dental clinic to conduct an information security risk assessment. An important feature to note is the clinic's use of a cloud service provider (CSP) as the primary method to handle patient ePHI. In subsequent sections, we will further evaluate the implications of ePHI being managed in the cloud.

We chose a small healthcare clinic because we felt this type of research is needed to benefit small healthcare providers. Medium-to-large healthcare organizations often have more resources to assess and manage the risks that they face while small healthcare firms typically are more limited in their ability to protect patient ePHI within the context of their overall business and compliance obligations. This has made them a relative afterthought in the information security conversation to date. Common sense informs us that there is variability of IT knowledge, technical implementation, and the degree to which appropriate

best practices are used among providers. Therefore, through this case study we aim to advance the interests of all parties to more effectively manage these risks by moving towards best practices and compliance with the HIPAA Security Rule.

2 Review of Literature

The federal government provides a few key resources of note in the area of information security risk management. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2014) is the current broad information security standard in this area. NIST also released a framework for small businesses, which is geared specifically for the challenges they face and is relevant for many small healthcare clinics. (Paulsen & Toth, 2016) The Balridge Cybersecurity Excellence Builder (NIST, 2016) is a self-assessment tool provided by NIST which gives organizations the ability to invest their time on a targeted basis to better understand their information security risk posture. The Department of Health and Human Services (HHS) provides compliance information specific to HIPAA and the cloud. (HHS, n.d.) Taken together, these federal resources are relevant for any small healthcare clinic to reference on their path to HIPAA compliance.

Earlier we mentioned the existence of limiting factors that small healthcare providers face when making information security decisions. Green, et al. (2015) took a specific look at managing ePHI in low monetary resource practices and found that these providers are lacking in critical areas related to a sound information security posture. They mentioned that, for many of these practices, "ongoing support will be needed…to remain viable." (p. 17) This speaks directly to our aim to impact such organizations through this work.

Perhaps the most cogent recent academic work was performed by Blanke and McGrady (2016) who created a 25-point list of recommendations for risk assessment based on the most recent data for healthcare data breaches, focusing on three key attack vectors: portable devices, insider threats, and physical breaches. A few recent case studies have been conducted in Canada (Desouza & Valverde, 2016), Turkey (Namoglu & Ulgen, 2014), and Iran (Zarei & Sadoughi, 2016) related to information security risk management. Notably in each case, the organization size that was evaluated was of a medium or large size.

Often times researchers have found that a lack of information security education and awareness training has to do with security lapses in healthcare. Fernandez-Aleman, et al. (2015) found this to be the case as well as the need to clearly communicate information security expectations and policy guidelines. This research would perhaps pair well with the work by He and Johnson (2015) that examined how to implement the lessons learned from security incidents more effectively than occurs within the typical healthcare organization. Such research has implications in the area of information sharing which is one of the goals of our efforts. Bai, et al. (2014) offered a decision-making methodology to improve workflow processes and efficiencies related to information security risk, attempting to tackle the low-resource problem on the process level in healthcare. Other work attempted to create a quantitative information security risk assessment method focused on managing the risk of ePHI. (Wei, Lin & Loho-Noya, 2013)

Understanding data loss prevention (DLP) and its associated technologies can provide important insight and benefits to safeguarding ePHI. Beeskow (2015) notes three primary considerations related to DLP: where confidential data is stored, who is accessing the information, and how data is being handled. Another important element within healthcare 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) explores this topic in depth by examining the resilience of healthcare IT personnel in their response to extreme healthcare events. One of the key lessons here is that a well-prepared organization is more likely to protect the patient in these situations while also safeguarding their ePHI, instead of having to make this compromise.

Information security issues in the enterprise previously were boxed into the IT domain and budget. Andre (2017) makes clear that this outdated approach is untenable and requires a risk management-based approach to address the unique challenges in healthcare. Cascardo (2016) details numerous risk analysis and risk management steps that healthcare organizations can take to meet these compliance obligations and reduce the instances 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. As we will see later, these recommendations are in line with some of the key recommendations in our work.

No survey of current information security efforts in healthcare would be complete without mention of the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF). Although it may not be directly applicable for small providers, the CSF (HITRUST, 2017) is a top-level industry standard created and managed in partnership between many of the largest healthcare providers and can be applied to organizations of varying size. Knowledge of this standard is useful for growth-oriented practitioners who may wish to implement different subcomponents of it for their needs.

Another useful industry perspective, which is built around HIPAA compliance, is the HIPAA Journal, offering their professional take including a HIPAA compliance checklist, a layman's explanation of the HIPAA Security Rule, and a sponsored HIPAA risk assessment. (HIPAA Journal, 2016) Many companies exist to provide HIPAA risk assessments for a fee; HIPAA One is one such firm specifically geared to meet these needs for healthcare providers of varying sizes. (HIPAA One, n.d.) In either of these cases, providers would submit information over an online portal or use the vendor's proprietary software solution. In any case, a significant ongoing time and energy investment is required to ensure that the overall process is managed well.

3. Methodology

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. It consists of 156 detailed questions and is run as an executable file, which locally stores the data entries in the assessment. The context of each question is geared towards protecting ePHI through policy guidelines, physical access restrictions, or technical safeguards specific to the requirements laid out in the HIPAA Security Rule.

In assessing whether the business is in compliance with respect to each question, there are fields to detail current efforts, suggest appropriate remediation steps, and mark the risk likelihood and impact. Questions can be flagged for further review at a later time, there is a section for additional notes, and there is a guidance area in the right pane to assist with answering the question. Note the screenshot below for additional context.

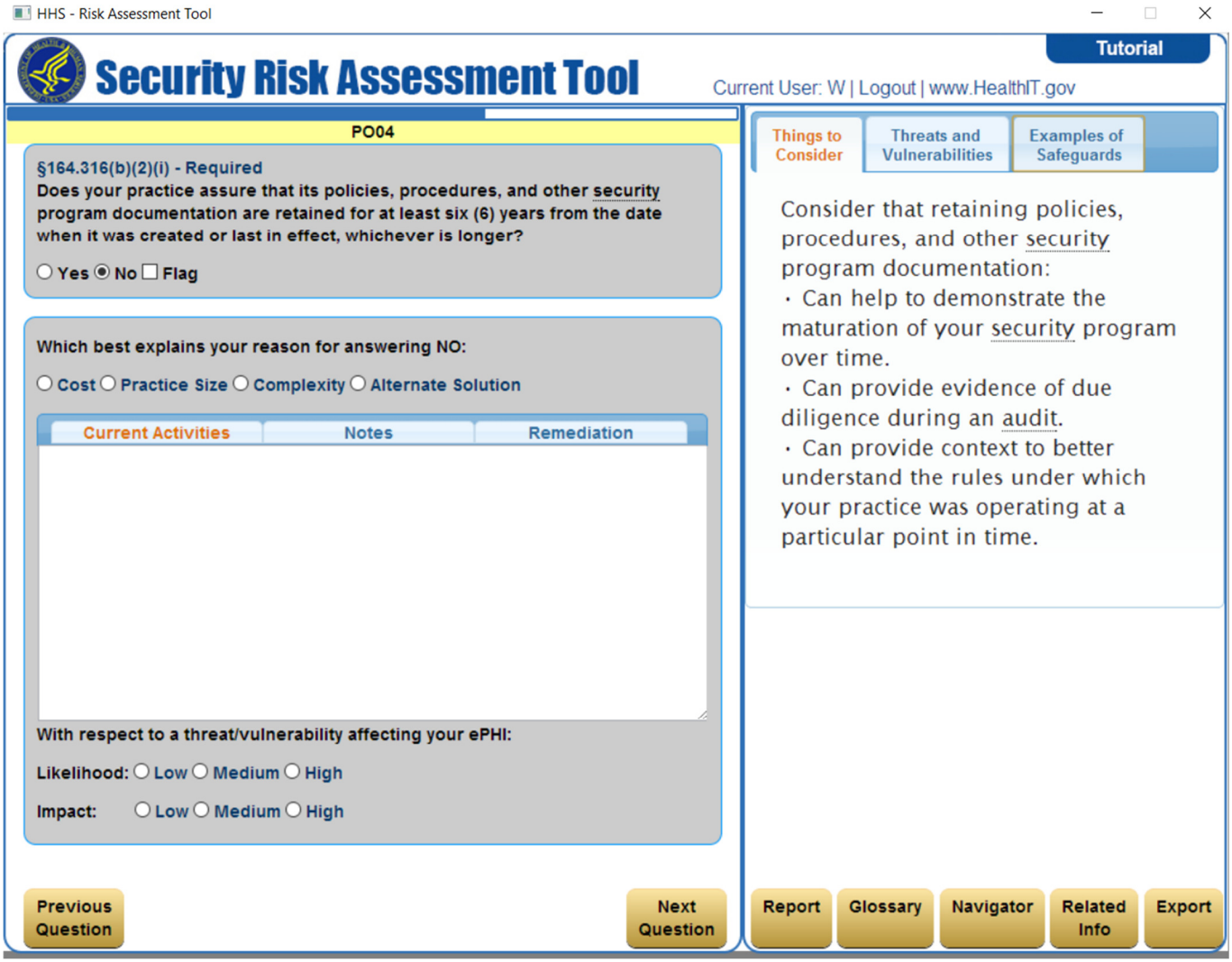

Figure 2: Security Risk Assessment (SRA) Tool

4. Results & Recommendations

We found that the SRA Tool is useful, though it has some drawbacks. The software interface is well packaged and intuitive to move through the questions; however, there were repeated technical problems with loading saved assessments that caused some repetition of work. Since we were taking detailed notes with each step, it was not a major issue but certainly could be if a business owner or team spent quite a bit of time inside the software and experienced this issue. We found the best workaround is to regularly save work and generate updated PDF reports while doing the assessment, where the findings can be easily referenced and concatenated, if necessary, to other reports.

The dental clinic we assessed is responsible for roughly 1,600 patient ePHI records, employs five people, and contains eight stationary devices. The owner remotely connects to the local clinic environment using a virtual private network (VPN) and TightVNC, a remote access program. They have no dedicated IT personnel, so the owner handles these duties. This solution was found to work best since the previous IT contractor tended to make mistakes which cost the owner additional time and other resources.

We spent six hours total consulting with the business owner while going through the tool over the course of two site visits. During the first visit, we received additional guidance from a professional information security auditor as we navigated through each question. Over these six hours, we answered a total of 101 out of the 156 questions due to what we perceived as a redundancy between many of the questions. Particularly for a clinic that has a small staff, much less an IT staff, many of the questions in the SRA Tool could be perceived as overkill or asked similar questions from a different angle. We recognized that the tool is a guidepost for HIPAA Security Rule compliance and adapted our efforts accordingly during the assessment. Even so, answering 101 questions in six hours is roughly six minutes per question. For the initial assessment, we feel it is reasonable to expect this type of time investment, as each question requires a certain level of detail and understanding of the compliance requirements. Experienced information security professionals could likely cover these steps in an hour or two by knowing which key questions to ask and determining where additional due diligence is required.

These caveats aside, we found the SRA Tool serves its purpose and will further detail our findings and recommendations from the assessment. As mentioned earlier, the dental clinic utilizes a cloud service provider (CSP) for managing patient ePHI. All ePHI data is entered directly into the CSP web interface and managed according to its HIPAA-compliant business associate agreement (BAA). This results in the transference of a significant portion of risk to the CSP for key administrative, physical, and technical safeguards. A key idea for healthcare providers to understand is that conducting due diligence with the CSP is still required and it is necessary to obtain this information for documentation and auditing purposes.

Documentation is a critical area that is required for HIPAA Security Rule compliance and comes up frequently in the SRA Tool questions. The creation and maintenance of such documentation demonstrates compliance for the key areas and is one of the largest gaps

that we found in this assessment. We will also reveal the vulnerabilities identified during the assessment. Below are a few examples of questions from each of the three categories included in the final report (zoom in 2-2.5x to see them clearly):

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 3: SRA Question Examples

4.1 Areas the Clinic is Doing Well

We will examine this area in terms of the administrative, technical, and physical areas of concern from within the SRA Tool. Note that there is overlap between these areas and their combination forms the overall security posture of an organization. We found the provider takes a number of appropriate steps to prioritize the security of ePHI as detailed in the following subsections.

4.1.1 Administrative Controls

The provider clearly states the name of its security point-of-contact in its BAAs related to accessing ePHI. They handle ePHI in a similar manner to financial records such that appropriate security of ePHI is maintained. A list of all BAAs is maintained, including their accounting firm which tracks 1099 information but does not have ePHI access. The clinic only hires dental-certified individuals after conducting a thorough criminal background check. When an employee is terminated, they promptly disable the user's login access and delete the physical access codes to the building. There also exist termination procedures in the BAA between the clinic and the CSP, should it need to occur. The same BAA with the CSP includes the handling of ePHI and an attorney reviewed and signed off on the language of all BAAs.

The practice performs segregation of duties with its ePHI processes, where possible, and also processes cash payments in this manner. The employee handbook is a guideline for job descriptions in the practice and explicitly forbids violation of the office ePHI policy, which would result in termination. Employees perform cleaning duties with no outside contractors who have facility access for this purpose.

The owner implements 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 has full administrative access while the office manager has access to most administrative functions except for adding and removing users. Other clinical personnel have strictly role-based access for their jobs, including clinical

notes and health histories but no other ePHI. It is notable that there exist billing codes within the CSP database that abstracts much of the ePHI details. This effectively accounts for an additional layer of access control in the day-to-day functioning of the business. The owner proactively manages both environments in consultation with the CSP to maximize functionality while ensuring there are appropriate access controls on all electronic devices to maintain the confidentiality and integrity of ePHI. Within the clinic environment, this includes systems reviews, multiple firewalls, operating systems updates to all devices, and regular password resets.

A final note regarding the availability of ePHI is, should a failure of service by the CSP occur, the clinic would be able to temporarily house ePHI data on site until the CSP service becomes available.

4.1.2 Technical Controls

Many of the SRA Tool questions related to technical controls are provided within the CSP interface. The CSP provides for encryption of ePHI within its interface for data at rest and in transit. It also performs regular backups of this data and maintains an extremely high availability of the service, making an outage unlikely and an acceptable risk for the practice. It has an auto-logoff policy for idle users, which pairs with the clinic's auto-logoff policy of 4-6 hours to address this requirement. The owner follows the CSP recommendations for security settings within the CSP interface and pairs these with practical technical controls in the local environment. The practice avoids the use of shared accounts at any level and maintains a list of authorized users and passwords that are securely maintained.

4.1.3 Physical Controls

The clinic does an overall effective job of complying with physical security requirements. They use an internal security system which includes motion alarms and locks. This system has been tested to confirm it is in working order. The risk of protecting the facilities and equipment has been transferred to a third-party security firm, as reflected in its BAA. Clinic employees have free access to the facility; this access is revoked when employees leave the company. Should a breach occur after hours when the doors are locked, a security team is promptly dispatched.

The owner proactively and effectively maintains a Facility User Access List that includes active employees as well as accountants who have 1099 access, but no facility access. The facility itself was designed to avoid scenarios where a casual passerby could view ePHI on clinic devices and the front desk computer is always monitored. The practice also maintains an inventory of devices containing ePHI and ensures that any physical security measures implemented occur with minimal impact to the business.

4.2 Areas to Improve

We will subdivide this section based on the vulnerabilities discovered, necessary follow-up communication with the CSP, and a significant level of documentation which must be produced and maintained going forward. Note that the clinic is doing well in certain areas, yet must also improve in the same areas as well. For instance, the owner may say they are performing certain administrative functions; however, without documentation, there is no way to validate this reality should a breach or audit occur. Such considerations are important when examining both sections, respectively.

4.2.1 Vulnerabilities & Remediation

We found that a primary vulnerability of single-factor authentication (SFA) using a password exists for accessing ePHI in the cloud from clinic devices. A secondary vulnerability is the lack of proper mitigation practices when the clinic receives ePHI from patients via email. The clinic uses written forms for recording ePHI and implements faxes between clinics over a plain old telephone service (POTS) line for sharing this data as needed, which is standard industry practice. A tertiary vulnerability related to this is the ePHI being compromised on the printer-fax machine by accessing the printer memory card either physically or via an internet-based intrusion.

To remediate the SFA issue, we recommend the healthcare provider work with the CSP to implement multifactor authentication and document the results of this endeavor. In this security climate, a password is considered a weak control when it protects all of the ePHI and is accessed over the Internet. This is an important process to undertake for any liability issues that may come up should a breach occur.

When the clinic receives email from patients containing ePHI, it must take special measures to record the information while not retransmitting it over the Internet. Replies to emails contain metadata which, even if the ePHI were to be deleted, could be reconstructed by an unauthorized third party. Therefore, we advise that the clinic implement a policy where users must not reply directly to any received emails containing ePHI. Instead, clinic personnel should create a new message with no ePHI in it to send. Additionally, all clinic messages should have a legal disclaimer at the bottom of the email that absolves the clinic of liability for any ePHI received. The clinic should also consider an email retention policy that conforms with the knowledge that client ePHI may exist in a mailbox folder without a process for managing it and implement it accordingly.

Protecting the printer-fax memory physically is a simple as adding locks onto the device itself. People often forget that a network printer has an embedded operating system that can be exploited by internet-based command injection attacks. (Sheridan, 2017) This could expose the ePHI that went through the fax machine or allow a hacker to move laterally from the printer to other areas of the network (i.e. the front desk machine), which would then give the hacker access to the CSP interface and the ePHI contained therein. On this basis as well as the other common attack vectors of email phishing and web application

attacks, we propose supplemental countermeasures for the clinic to pursue.

The clinic should start by implementing 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, the clinic 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 is segregated. This would prevent an internet-based intrusion on one device from affecting other devices.

Each of these supplemental countermeasures is proposed in the spirit of staying ahead of the curve. Small business owners should know that the risk of a cyberattack cannot be eliminated. However, by considering steps such as the ones outlined above and implementing a practical solution, healthcare organizations can demonstrate due diligence in understanding the threats to client ePHI which is the intent of this exercise.

4.2.2 CSP Follow-up Communication

While a significant transference of risk to the CSP occurred, due diligence is still required to understand and document how the CSP is handling patient ePHI. The clinic should check with the CSP regarding any security certifications held i.e. the service organization controls (SOC) standards. 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 ePHI. Encryption includes data at rest as well as in transit. All of these answers should be well documented as part of the overall compliance documentation for the clinic. These are important steps to validate the cloud assurance of ePHI and CSP personnel are available to answer such questions.

4.2.3 Create & Maintain Documentation

We found that, out of the 101 SRA Tool questions answered, 38 of these questions required the creation of documentation to validate procedures already in place or new procedures that will be implemented as a result of the assessment. The clinic owner performed most of the information security processes on an ad hoc basis without proper documentation. It is very clear from the federal resources that it is not enough to simply say that some compliance activity is occurring. It must be documented appropriately and the documentation must be periodically updated to reflect changes in the organization as well as the evolving threat vectors. We will now detail the required documentation that the clinic must create and maintain to meet administrative, technical, and physical benchmarks from the SRA Tool. Again, there may be some redundancies and overlap due to the nature of the questions in the SRA Tool.

The clinic owner must formally document a security plan as well as their full list of duties as the security point-of-contact. The results from this risk assessment should be documented and they should formally document a program to mitigate threats and vulnerabilities to ePHI that were mentioned in this assessment where risk should be classified as high, moderate, or low. This can pair with policies and procedures to assess and manage risk to ePHI. In these policies, the practice must describe how its risk management program prevents ePHI exposure.

The clinic must specifically document how they handle ePHI in a similar manner to financial records. They 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 ePHI to those who need it and deny access to others. Within the employee handbook, they should check the termination language to ensure it is formal, review the language related to termination for misusing ePHI, and include an Acceptable Use section with language about devices being monitored and tracked. The practice should create security training documentation that should include sanction policies, how malware can get into systems, and good practices to follow to protect ePHI.

They must document a Disaster Recovery Plan (DRP) and Contingency Plan (CP). The CP should include how ePHI will be handled should a CSP failure occur. The clinic owner should evaluate when it would be practical to test the CP and document when such testing occurs. This includes identifying and assessing the criticality of information systems applications and how ePHI would be accessed and stored during the implementation of the CP.

Creating such documentation is the first step, and we advise the following documentation updates be performed by the clinic on at least an annual basis. They should instantiate a process in writing for periodic review of risk assessment policies and procedures. Periodic employee training should occur regarding information security threats to ePHI. All contract language should be reviewed to ensure HIPAA compliance, the CP should be tested, workstation locations should be updated, and the employee handbook should be updated as appropriate.

Technical and physical documentation must also be created. The clinic needs to document how an individual who seeks access to ePHI has their identity verified as well as the clinic's definition of emergencies that are the most likely and impactful to consider. These technical scenarios will drive the DRP and CP documents. They 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 the owner's use of remote access to the facility, how the positioning of workstations limits unauthorized viewing of ePHI, and all security procedures for the secure storage and destruction of ePHI data. It must also include procedures related to the protection of keys, combinations, and other physical access controls. Any modifications or repairs to physical security features must also be documented.

5. Discussion

While not a one-size-fits-all solution, the SRA Tool hit the mark in providing an overarching context to conduct a risk assessment in a small clinical setting. There are many areas where future work could occur. A closer evaluation of the factors 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.

Cloud assurance is an emerging issue of concern across vertical industries and is certainly one that could drive further study in the area of protecting ePHI. Frameworks such as that proposed by Abuhussein and Shiva (2016) or under development by Halabi and Bellaiche (2017) could help drive this conversation forward when it comes to the practicality of protecting ePHI in the cloud. The CloudTrust Protocol is an additional mechanism that could bring greater clarity in this area through future work. (Cloud Security Alliance, n.d.)

Another area that could be more closely analyzed is the comparative risks between using a CSP vs. on-site servers for small healthcare providers. Given all of the technical requirements to secure ePHI under HIPAA, how realistic is it to expect compliance without a cloud solution for a clinic with limited IT knowledge, a limited budget, and who may not even have an IT staff? Understanding where the breakdown can occur within each solution set could be a driving factor in the future marketplace. 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 relatively weak information security posture in many cases.

It is our hope that our work contributes to greater transparency in the area of information security risk assessment in the healthcare industry. Such efforts have implications in the area of information sharing, an area of information security that is on the rise in the healthcare industry. (Snell, 2016) One also wonders at what point consumers will start demanding better information security practices en masse from various healthcare providers. Stalled federal legislation such as the Transparent Ratings on Usability and Security to Transform Information Technology (TRUST IT) Act of 2015 may need to be re-examined to give consumers more information regarding healthcare organizations which fail to prioritize the protection of their data. (Leventhal, 2015)

6. Conclusion

We observed that the clinic owner is a tech-savvy individual who likely is doing more from a security standpoint than the typical small healthcare clinic. Even so, we identified many areas where improvements could be made to put the clinic in line with best practices outlined by the SRA Tool. While this tool does not guarantee HIPAA Security Rule compliance, going through the process and following its recommendations demonstrates due diligence which will minimize the impact of a data breach or audit. Information security is a moving target and requires periodic assessment and analysis to keep up with the changes. Only a proper prioritization of time and resources will ensure that small healthcare clinics, such as the one featured in this case, do not fall behind.

References

Abuhussein, A., & Shiva, S. (2016). A framework for cloud security assessment: A scenario-based, stakeholder-oriented approach. *1st Annual Research Workshop on Advances & Innovations in Cyber Security, The University of Memphis, Memphis, TN, USA.*

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

Beeskow, J. (2015). Reducing security risk using data loss prevention technology. *HFM (Healthcare Financial Management)*, *69*(11), 108-112.

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.

Cloud Security Alliance. (n.d.). CloudTrust Protocol Working Group. Retrieved from https://cloudsecurityalliance.org/group/cloudtrust-protocol/

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

Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of cloud service providers. *Journal of Information Security and Applications*, doi:10.1016/j.jisa.2017.01.007

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.). Guidance on HIPAA and cloud computing. Retrieved from https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html?language=es

HIMSS. (2016). ONC and OCR update HIPAA security risk assessment tool. Retrieved from http://www.himss.org/news/onc-and-ocr-update-hipaa-security-risk-assessment-tool

HIPAA Journal. (2016). HIPAA compliance checklist. Retrieved from http://www.hipaajournal.com/hipaa-compliance-checklist/

HIPAA One. (n.d.) HIPAA security risk analysis. Retrieved from http://www.hipaaone.com/hipaa-security-risk-analysis/

HITRUST. (2017). Introduction to the HITRUST CSF. Retrieved from https://hitrustalliance.net/documents/csf_rmf_related/v8/CSFv8_1Introduction.pdf

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*.

Leventhal, R. (2015). Health IT legislation would establish consumer rating system for EHRs. *Healthcare Informatics*. Retrieved from http://www.healthcare-informatics.com/news-item/health-it-legislation-would-establish-consumer-rating-system-ehrs

Namołlu, 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

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

Sheridan, K. (2017). Why printers still pose a security threat. *Dark Reading*. Retrieved from http://www.darkreading.com/endpoint/why-printers-still-pose-a-security-threat/d/d-id/1328316?

Snell, E. (2016). ISAO SO releases cybersecurity information sharing guidance. *HealthIT Security*. Retrieved from http://healthitsecurity.com/news/isao-so-releases-cybersecurity-information-sharing-guidance

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

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