HIPAA Security Risk Analysis

Risk Analysis Report

August 1, 2013

Prepared For:

XYZ Medical Center

Prepared By:

Chris Dansie, PhD, CISSP-ISSMP
Pete Niner, CISSP

Clearwater Compliance LLC
800-704-3394

Table of Contents

Executive Summary

Clearwater Compliance performed a Security Risk Analysis of the information systems that contain electronic Protected Health Information (ePHI) at the XYZ Medical Center through an onsite visit and review of provided documentation. Actual testing of the information security controls must be completed in a separate technical security testing work stream.

With the available time and information access, two “High Risks” were identified which represent the most significant areas of risk to the ePHI that XYZ Medical Center creates, receives, transmits and maintains. These ”High Risks” are in the areas of insufficient Data Backup Testing and Weak Passwords.

Additionally, while not necessary a ”High Risks” from a security perspective, another six (6) potential HIPAA Security Rule compliance and/or security risks should be examined. Finally, three Considerations were cited for further review to enhance the XYZ Medical Center overall security and compliance posture.

Importantly, as committed in the project Statement of Work, the Clearwater HIPAA Risk Analysis™ software has been populated with asset information, associated media, threats/vulnerabilities, present controls, and risk ratings for all assets included in the analysis. What this means is that a database repository for ongoing risk analysis and risk management has been created to meet explicit HIPAA Security Rule requirements and Office for Civil Rights (OCR) audit protocols pertaining to the HIPAA Security Risk Analysis requirement at 45 CFR §164.308(a)(1)(ii)(A). Training in the use of this tool will be scheduled with appropriate staff.

Risk Analysis Methods

Background

Clearwater Compliance uses an industry formula for "calculating" risk:

Risk = Impact * Likelihood

By applying this formula, Clearwater Compliance is able to categorize risks as Low, Medium, High and Critical as illustrated in the 5X5 matrix shown below. The categorization of each risk will help prioritize risk remediation efforts. Categorizing risks in this way enables prioritization and facilitates risk management decisions.

Overall Risk

Impact	**Disastrous (5)**	**Low**	Medium	High	High	Critical
	Major (4)	**Low**	Medium	Medium	High	High
	Moderate (3)	**Low**	**Low**	Medium	Medium	High
	Minor (2)	**Low**	**Low**	**Low**	Medium	Medium
	Insignificant (1)	**Low**	**Low**	**Low**	**Low**	**Low**
		Rare (1)	**Unlikely (2)**	**Moderate (3)**	**Likely (4)**	**Almost Certain (5)**
	Likelihood					

The Security Rule does not specify exactly how a risk analysis should be conducted; however, the Department of Health and Human Services (DHHS) and OCR issued "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"[1], in July 2010. This guidance, in turn, references the National Institute of Standards and Technology (NIST) Security Framework and several specific documents such as Special Publication 800-30[2], "Risk Management Guide for Information Technology Systems." This NIST publication offers a comprehensive approach to incorporating risk management into the system or project development life cycle. Threats in the environment are identified, and then vulnerabilities in the information assets are assessed. Threats are then matched to vulnerabilities to describe risk. The Clearwater Risk Analysis and Risk Management Methodology rigorously follows DHHS/OCR guidance and the NIST Security framework.

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
[2] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

The "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"[3] describes nine (9) essential elements a Risk Analysis must incorporate, regardless of the methodology employed. These elements are as follows:

1. **Scope of the Analysis** - All ePHI that an organization creates, receives, maintains, or transmits must be included in the risk analysis. (45 C.F.R. § 164.306(a).)

2. **Data Collection** - The data on ePHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316 (b)(1).)

3. **Identify and Document Potential Threats and Vulnerabilities** - Organizations must identify and document reasonably anticipated threats to ePHI. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

4. **Assess Current Security Measures** - Organizations should assess and document the security measures an entity uses to safeguard ePHI. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

5. **Determine the Likelihood of Threat Occurrence** - The Security Rule requires organizations to take into account the likelihood of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

6. **Determine the Potential Impact of Threat Occurrence** - The Rule also requires consideration of the "criticality," or impact, of potential risks to confidentiality, integrity, and availability of ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

7. **Determine the Level of Risk** - The level of risk could be determined, for example, by combining the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

8. **Finalize Documentation** - The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).)

9. **Periodic Review and Updates to the Risk Analysis** - The risk analysis process should be ongoing. In order for an entity to update and document its security measures "as needed," which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).)

This report and comprehensive documentation captured in the Clearwater HIPAA Security Risk Analysis™ SaaS tool such as asset-by-asset information, associated media, threats/vulnerabilities, present controls, and risk ratings for all assets demonstrate full compliance with elements 1-8 from this list for the limited number of information assets reviewed during the limited time allocated. Compliance with element 9, Periodic Review and Updates to the Risk Analysis, can be demonstrated by regularly

[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

repeating this process in the future. Clearwater Compliance strongly recommends that a risk analysis be completed annually (at a minimum) or upon any significant changes in organization, people, processes, or technology.[4]

Meeting OCR Risk Analysis Protocols

In June, 2012, OCR made publically available the protocols for OCR audits of HIPAA Privacy, Security and HITECH Breach Rule compliance. There are 77 such protocols for Security Rule compliance, 78 for Privacy Rule compliance and 10 for Breach Rule compliance. Each area being audited breaks down into Audit Performance Criteria, Key Audit Activities and Key Audit Procedures. For the HIPAA Security Risk Analysis requirement at 45 CFR §164.308(a)(1)(ii)(A), there are 5 Key Audit Procedures specified as follows:

1. Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
2. Obtain and review relevant documentation and evaluate the content relative to the specified criteria for an assessment of potential risks and vulnerabilities of ePHI.
3. Evidence of covered entity risk assessment process or methodology considers the elements in the criteria and has been updated or maintained to reflect changes in the covered entity's environment.
4. Determine if the covered entity risk assessment has been conducted on a periodic basis.
5. Determine if the covered entity has identified all systems that contain, process, or transmit ePHI.

The Clearwater HIPAA Security Risk Analysis process helps prepare organizations to meet each of these audit areas.

Our Process

Clearwater Compliance conducted interviews with multiple members of XYZ Medical Center staff, based on the Information Asset Inventory agreed upon in the scope-of-work. The intent of each interview session was to perform the following for each in-scope information asset:

1. Identify and Document Potential Threats and Vulnerabilities
2. Assess Current Security Controls
3. Determine the Likelihood of Threat Occurrence
4. Determine the Potential Impact of Threat Occurrence
5. Determine the Level of Risk
6. Record required documentation
7. Prepare required reporting

The likelihood rating of a particular threat exploiting a potential vulnerability within the environment was determined based on:

[4] Ideally, XYZ Medical Center would conduct a risk analysis before performing any significant changes.

- Historical information, where available
- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

In addition to the historical information provided by XYZ Medical Center personnel, the Clearwater Compliance team used their professional knowledge to estimate the other three factors. The likelihood that a potential vulnerability could be exploited by a given threat source was described as follows:

Level	Likelihood Definition
Rare (1)	May happen once every 20 years
Unlikely (2)	May happen once every 10 years
Moderate (3)	May happen once every 5 years
Likely (4)	May happen once every year
Almost Certain (5)	May happen multiple times a year or is currently happening

Similarly, to analyze the impact of a threat exploiting a particular vulnerability, the team used the following definitions:

Level	Impact (Potential Scenarios)
Insignificant (1)	• Remediate within 1 hour • No interruption of operations
Minor (2)	• Remediate within 8 hours • No serious interruption of operations • Multiple other controls would have to fail for the threat to exploit the vulnerability
Moderate (3)	• Remediate in more than 8 hours • Disruption of operations • Creates new minor vulnerabilities
Major (4)	• Multi-hour interruption of operations • Data breach reportable to HHS annually (< 500 records) • An OCR investigation could potentially result in penalties • Creates a new serious vulnerability
Disastrous (5)	• Multi-day interruption of operations • Data breach reportable to HHS immediately (> 500 records) • An OCR investigation would likely result in penalties • Creates many new serious vulnerabilities

Limitations of the Analysis

The risk analysis is solely based on interviews and subjective observation, not objective technical reports or system/application testing. It relies on information provided by knowledgeable Istaff and subject matter experts.

Vulnerability information was taken from the National Vulnerability Database at the National Institute for Standards and Technology (NIST). It is the Clearwater Compliance assumption that there are other vulnerabilities and threats that we have not identified that could only be identified by deeper analysis, investigation and periodic repetition of the risk analysis process.

Control recommendations were made based on the prior analysis, taking into account best practices, resource constraints, and what controls would be reasonable and appropriate for the environment.

Risk Analyses examine the information assets, threats, vulnerabilities and risks of an organization at a specific point in time. It is the responsibility of the organization to achieve, demonstrate, and maintain their information security vigilance at all times. Therefore, Clearwater Compliance, LLC makes no representation or warranty as to whether the Company's network and/or computer systems are secure from either an internal or external attack or whether sensitive data is at risk of being compromised. Additionally, Clearwater Compliance, LLC makes no representations or warranties regarding the organization's business activities or operations.

Risk Analysis Results

System Characterization

The XYZ Medical Center serves the outpatient needs of families in Victoria, MN.

Being co-located within the local hospital (Victoria Hospital), the hospital has provided Internet connectivity, firewall and basic facility security. The remainder of technology and security needs have been left to XYZ Medical Center, which they have solved using independent computer consultants.

The small clinic primarily runs as a “paper-based clinic”. There are however multiple desktops and laptops in the clinic, laptops are not used for any process that handles Protected Health Information (PHI). Desktops are used for letter writing and to access the billing and pharmacy systems. The desktops run standalone in a workgroup, not integrated with any directory services or other centralized control. There are two specialty desktops supporting the clinic. One specialty desktop, supporting transcription, is isolated in a dedicated, restricted office, is not connected to the Internet and has a direct attached printer. There is also a desktop dedicated to a pharmacy management application.

There is one server in a locked server/storage room that runs a billing application. It is used to create and print paper bills. This server, the pharmacy workstation and transcription workstation are backed up to media that is taken offsite daily to a locked, fireproof safe in a local bank.

XYZ Medical Center follows local policies and procedures to ensure a trustworthy workforce. Workforce members participate in annual training provided by the practice administrator.

Good or Best Practices Observed

The XYZ Medical Center has implemented a number of information security safeguards that are considered industry good or best practices. These practices include, but are not limited to:

- Strong physical security as a result of co-locating with the hospital
- Exercising tight control over systems with ePHI, such as isolating the transcription system from the Internet and in a dedicated office.
- Preventing laptops without encryption from storing ePHI.
- Ensuring that training and orientation, including proper use of PHI, occurs at onboarding and annually.
- Nightly backups stored offsite in a secure location.
- Encryption of laptops
- Proper workforce member oversight

Control Analysis

Details of the preventative, detective, and compensating controls in place to minimize the likelihood or impact of ***any*** threat's exercising a particular vulnerability are documented in the Clearwater Compliance HIPAA Security Risk Analysis™ Software-as-a-Service application. These can be seen in the application's Risk Rating Report or as part of notes at the threat-vulnerability level.

Identified High Risks and Recommended Remediation Controls

Risks can exist when and only when an asset-threat-vulnerability simultaneously co-exists. For example, a laptop with sensitive data such as PHI or Personally Identifiable Information (PII) may be stolen (the threat) that is not encrypted (the vulnerability that may be exploited) likely represents a risk. The extent or significance of this risk is a function of certain predisposing conditions and controls that may or may not be in place.

The determination of a risk rating for a particular asset-threat-vulnerability combination is expressed as a function of Likelihood and Impact, using the following definitions:

Likelihood of an adverse impact to the organization considering the ability of a specific threat to exploit a specific vulnerability given predisposing conditions, and the controls in place for this media/asset.
Impact (or magnitude of harm) that can be expected to the confidentiality, integrity or availability of

sensitive information if the specific threat were to exploit the specific vulnerability given the predisposing conditions and controls in place for this media/asset. As indicated above, then:

Risk = Impact * Likelihood

Note that both Likelihood and Impact include the control environment in place. Asset-threat-vulnerability pairs that were judged to be so unlikely as to not merit analysis, or controls were rated "negligible" and were not included in the analysis. In the Clearwater Compliance HIPAA Security Risk Analysis™ Software-as-a-Service application there hundreds of media-threat-vulnerability combinations that were analyzed and the existing control environment documented.

From our analysis and the Clearwater Risk Analysis™, a summary of XYZ MEDICAL CENTER risks is as follows:

Risk Category	Number of Risks Rated
Critical Risks	0
High Risks	9
Medium Risks	97
Low Risks	124

Below, please find the documented "High Risks" identified and recommended remediation controls. The exhaustive list of Medium and Low risks is articulated in the Clearwater Compliance HIPAA Security Risk Analysis™ Software-as-a-Service application.

The Medium and Low risks should be watched closely, as it is not uncommon for lower risks to become higher risks as the environment changes over time.

Vulnerability	Likelihood	Impact	Risk Rating
Insufficient data backup	3	5	High

Remediation Recommendations

- Consider an online, secure data backup and recovery service; OR,
- Replace the old tapes with fresh media and clean the tape backup system.
- Develop Policies and Procedures pertaining to Media Testing.
    - Modify (and document) the procedures based on analysis of the Recovery Point Objective (RPO) for key applications at XYZ Medical Center containing ePHI. Use the RPO to determine the necessary backup and retention schedules.
    - Validate the schedules to make sure that both legal and contractual requirements for retention are being met, and can continue to be met in the future.
- Follow the new procedures to regularly test the backups to ensure that pharmacy and billing systems can be properly recovered.

Vulnerability	Likelihood	Impact	Risk Rating
Weak passwords	5	3	High

Remediation Recommendations

- Examine all workstations and server accounts to ensure that there are no accounts for which there is no password (a “blank” password) and if a violation is discovered, set a strong password immediately.
- Execute a clinic-wide password reset effort requiring use of a strong password and repeat quarterly.
- Develop Policies and Procedures pertaining to password management and regularly audit to ensure the policy is being followed.

Considerations

In light of the small size of the medical center, consider the following to reduce PHI and ePHI risk and operating costs/complexity through one or all of the following methods:

- Migrate the pharmacy management application to a well-vetted, Software-as-a-Service application, which would significantly reduce the security risk and operational/technical overhead of maintaining a local application.
- Migrate the billing application to a well-vetted, Software-as-a-Service application, which would significantly reduce the security risk and operational/technical overhead of maintaining a local application. This could be a dedicated billing system or a complete practice management system.
- Move the "paper-based" health record keeping to a well-vetted, Software-as-a-Service EHR application, which would significantly reduce the physical security risk of storing PHI on paper, reduce the cost of storage/destruction of paper PHI, reduce the need for expensive printers/toner, streamline the record keeping process and qualify for Meaningful Use funds from CMS.

Appendix

Control Notes and Risk Ratings

Risk Rating Review

Rating Review

Export to Excel | Print

Media And Storage Devices	Asset Name(s)	Threat Agent	Threat Action	Vulnerability	Risk Likelihood	Risk Impact	Risk Rating
Desktop	PACs, Clinical App Server, Transcriptions	Careless IT personnel	Insecure configuration of systems	Vulnerabilities in system configurations	5: Almost Certain	5: Disastrous	25
Laptop	Electronic Medical Record System	System Cracker	Theft of sensitive data	Vulnerabilities in custom applications	5: Almost Certain	5: Disastrous	25
Desktop	Electronic Medical Record System	Inclement weather	Physical damage to equipment	Insufficient equipment redundancy	4: Likely	5: Disastrous	20
Desktop	PACs, Clinical App Server, Transcriptions	Careless user	Information leakage	Endpoint Leakage Vulnerabilities	4: Likely	5: Disastrous	20
Disk Array	Financials, Practice Management System	Careless user	Corruption or destruction of important data	Insufficient data backup	4: Likely	5: Disastrous	20
Electronic Medical Device	Document Management, Billing System, Email	System Cracker	Social Engineering	Overly-trusting employees	4: Likely	5: Disastrous	20
Laptop	Electronic Medical Record System	System Cracker	Theft of sensitive data	Vulnerabilities in commercial software	4: Likely	5: Disastrous	20
Desktop	Electronic Medical Record System	Careless user	Installation of malicious software	Overly-trusting employees	4: Likely	4: Major	16
Desktop	PACs, Clinical App Server, Transcriptions	Inclement weather	Unavailability of key personnel	Lack of key person redundancy / cross-training	3: Moderate	4: Major	12
Disk Array	Financials, Practice Management System	Users with Malicious Intent	Social Engineering	Overly-trusting employees	3: Moderate	4: Major	12
Laptop	RIS	Fire	Fire damage to equipment	Insufficient equipment redundancy	3: Moderate	4: Major	12
Laptop	RIS	Flood	Water damage to equipment	Insufficient equipment shielding	3: Moderate	3: Moderate	9
Laptop	RIS	Burglar, Thief or anyone who finds a lost device	Access to sensitive data on laptop once in possession of the laptop	Vulnerabilities in user authentication	3: Moderate	2: Minor	6
Laptop	RIS	Burglar, Thief or anyone who finds a lost device	Access to sensitive data once in possession of the device	Vulnerabilities related to encryption of sensitive data	3: Moderate	2: Minor	6
Laptop	RIS	Burglar, Thief or anyone who finds a lost device	Corruption or destruction of important data	Vulnerabilities related to data backups	2: Unlikely	3: Moderate	6