Security Risk Analysis White Paper – CSM HOSTING

Written by Richard Lutterbie (CHP)
and Curtis Ray Martin (CHP)

October 2017

DIGITAL DEFENSE REQUIREMENTS UNDER HIPAA

IN THIS ISSUE

Security & Today's Electronically Protected Healthcare Information

The Health Insurance Portability and Accountability Act (HIPAA)has been in place for nearly a decade now and under this set of standards, Covered Entities (CE's) and Business Associates (BA's) must comply with, among other things, the HIPPA Privacy Rule and HIPAA Security Rule. This privacy and security set of rules obligates CE's and BAs to effectively create a data '*chain of trust*' or '*chain of custody*' between the CE, it's downstream BA's and other Agents and Subcontractors.

The HIPAA Security Rule (along with the Privacy Rule and HITECH Breach Notification Rule) are compulsory and statutorily obligated measures designed to protect electronic patient health information (ePHI).

This white paper focuses on the HIPPA Security Rule mandates for CE's in an effort to clarify requirements and aid in the understanding and implementation of Security Management of ePHI from maintaining, assessing and attesting to a CE's control and security practices as it relates to ePHI data.

Over the next two years, growth in the healthcare cyber security solution market is expected to increase 24.6% according to Symantec, a leader in cybersecurity solutions. And while a credit card 'record' is worth about $1 on the black market, healthcare data is worth $50 per record since things like date of birth and SSN's are permanent and not easily changed or cancelled like credit card information. It really is 'one stop' stealing for hackers.

As a result, Healthcare organizations now have to protect a much broader 'attack surface' now that most CE's under Meaningful Use now called, Advanced Care Improvement (ACI)have transitioned from paper to digital PHI systems that leverage mobile platforms and the cloud for IT services. Keeping data protected from attacks by malicious agents is now a major concern for healthcare organizations. As the threat environment has changed, many current cybersecurity solutions are failing to prevent increasing sophisticated attacks. The Department of Health and Human Services(HHS), Office of Civil Rights(OCR) is enforcing HIPAA regulations and has issued multi-million dollar fines to companies that haven't adequately protected their ePHI data. Industry analyst Nancy Fabozzi from Frost & Sullivan explains. "Hospitals are transitioning from their traditional fragmented approach to protecting privacy and security that is highly dependent on HIPAA compliance to a new approach and mindset that is proactive, holistic, coordinated and anchored in integrated solutions designed to protect multiple endpoints".

Risk management, required as part of the Security Rule in HIPAA includes *implementation of security measures to reduce risk to reasonable and appropriate levels to ensure the confidentiality, availability and integrity* of patient data and protect against any reasonably anticipated threats, hazards, or disclosures of data not permitted under HIPAA.

What is the HIPAA Security Rule?

Guidelines to protect ePHI
Page 5

HIPAA – Security Rules – Myths

With all the constant changes to the HIPAA compliance requirements, here's a few myths and facts to keep in mind.

Page #3

What's in a Security Risk Analysis SRA

By Curtis Ray Martin

Your Security Risk Analysis should include scanning all 'connected' devices or IP addresses within your organization across all sites connected to your business. Scans are usually run from a single service device with viability and access to all devices. See your systems administrator for more information on access and privileges required if you use an outside vendor. Also be sure the partner is a qualified, HIPAA compliant entity. Ask to see the engineering teams' latest certifications if you're not sure.

Once the scans are complete, you should receive a comprehensive report. Additionally, most partners will provide you with a composite score detailing where you're the most vulnerable and identifying 'required' and 'addressable' issues so your team can prioritize their efforts. A follow up scan is a great idea too. It can track progress and give management proof of compliance.

Here are a few sample reports you may want to consider for your SRA.

- **Security Risk Report.** This executive-level report includes a Security Risk Score along with summary charts, graphs and an explanation of the risks found in the security scans.
- **Security Policy Assessment Report.** A detailed review of your security policy and procedures from a technical perspective. It often includes policies that are in place on both a domain wide and local machine basis.
- **Share Permission Report by Computer.** Comprehensive lists of all network "shares" by computer, detailing which users and groups have access to which devices and files, and what level of access they have.
- **Share Permission Report by User.** Organizes permissions by user, showing all computers and files to which they have access.
- **Outbound Security Report.** Highlights deviation from industry standards compared to outbound port and protocol accessibility, lists available wireless networks as part of a wireless security survey, and provides information on Internet access and usage.
- **External Vulnerabilities Full Detail Report.** A comprehensive output including security holes, warnings, and informational items that can help you make better network security decisions, plus a full Scan which checks all ports and reports which are open. This is an essential item for many standard security compliance reports.
- **Anomalous User Login Activity.** Methodically analyze login history from the security event logs. The report uses mathematical modeling and proprietary pattern recognition to highlight potential unauthorized users who log into machines they normally do not access and at times they normally do not log in. This report delivers a security professional focus and pinpoints a manageable set of logins to investigate. The alternative is a time-consuming, manual spot check that often misses the mark and is far less reliable.

Use these 5 steps to help your organization move from a reactive to a sustainable, business-driven approach to protecting your data.

1. Comply with key mandates; base security controls.
2. Stay ahead of threats.
3. Let risk assessment DRIVE priorities.
4. IMPLEMENT a sustainable risk-management program.
5. Let business priorities ADVANCE the security policies and practices of your organization.

SRA Myths

Here are some security risk analyses myths to consider.

The security risk analysis is optional for small providers.

False. All providers who are "covered entities" under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.

Simply installing a certified EHR/EMR fulfills the security risk analysis MU or ACI requirement.

False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.

My EHR vendor took care of everything I need to do about privacy and security.

False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product.

However, EHR vendors are only responsible for making **their** products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis.

My security risk analysis only needs to look at my EHR.

False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.

I only need to do a risk analysis once.

False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections. For more on reassessing your security practices, please see the Reassessing Your Security Practice in a Health IT Environment.

FAST FACTS

Cyber theft is booming

125%

Why are Medical Records worth so much? They have most of the data backers want making them ideal for ONE STOP STEALING.

Criminal attacks are the number one root cause of healthcare data breaches are rising. Weak cybersecurity makes electronic protected health information more valuable.

Each Stolen Record

$50+

Credit cards can be canceled when lost or stolen. Medical records can be compromised for years since they contain more permanent information

FOR MORE INFORMATION

CURTIS RAY MARTIN
Contact Info
210-287-9180

Security Areas to Consider	Examples of Potential Security Measures	
Physical Safeguards	Facilities Location of data Equipment	Alarms Locked offices Updates, Passwords & Patches
Administrative Safeguards	Security Officer Training and oversight Access Reviews an assessments	Staff training Monthly reviews Policy enforce-ment
Technical Safeguards	EHR access User Log Audits Network and end point protection	Secure passwords Back ups Encryption Virus and Malware, protection & scans
Policies & Procedures	Written & Documen-ted.	Protocols Record Retention
Organizational Requirements	BA agreements	Vendor manage-ment Reviews and updates

Create an Action Plan

ONCE you've completed your Security Risk Analysis you should create an action plan to implement appropriate security measures to safeguard the confidentiality, integrity and availability of the ePHI and make your practice better at protecting it.

Your action plan should involve a review of the risks to your practice's ePHI identified in your risk assessment to correct any processes that make your patient's information vulnerable. Make sure your analysis examines risks specific to your practice.

For Example – How do you store patient information? Is it more than just the EMR/EHR system in your office or are their records and data stored on shared drives, open desktops or terminals, tablets or other mobile devices that you are not securing. Each scenario carries different potential risks and needs to be dealt with in ways that mitigate that risk and protect ePHI data.

Your risk analysis may also reveal that you need to update your systems software, change the workflow processes, storage methods and services, require password changes and delete user accounts no longer in use. You should expect to review and modify these procedures and technologies and schedule additional training for your staff and take other necessary correct actions to eliminate identified security deficiencies.

In your action plan, be sure to document the relevant information to ensure the plan is followed and you can show you've addressed issues as you've uncovered them. This is particularly important should you have an audit at some point in the future. The plan should include steps your practice takes to remediate or mitigate the identified risks, the individual responsible for implementing the required changes and target date /completion date, or reasonable timeline of when the changes will be implemented.

Performing a Security Risk Analysis

Today, Patient Protected Health Information is stored electronically, so the risk of a breach of that data is very real. Although there are no official guaranteed methods, there are 'best practices that security analysis and management have in common under the HIPAA Security Rule. To help you conduct a risk analysis for your medical practice here are a few suggested methods.

DEFINE the scope of your risk analysis and collect import data regarding the ePHI pertinent information.

IDENTIFY potential threats to patient privacy and assess your practices to prevent a breach.

ASSESS the effectiveness of implemented security measures in protecting against identifiable threats and vulnerabilities.

DETERMINE and assign risk levels based on the likelihood and impact of a threat occurrence.

PRIORITIZE the remediation of mitigation of identified risks based on the severity of their impact on by your patients and practices.

DOCUMENT your risk analysis including information from the steps above as well as the risk analysis results.

REVIEW and update your risk analysis on a periodic basis.

ATTEST as a CE you are required to attest to having performed a SRA

THREAT DETECTION

USING THE RIGHT TECHNOLOGY MAKES ALL THE DIFFERENCE. IT'S MUCH EASIER TO SPOT ATTACHERS AND THEIR METHODS AND STOP THEM IN THEIR TRACKS

Hacking Techniques have become more sophisticated and they continue to evolve every day making them very difficult to detect and respond to. To combat this trend and make security a possibility for organizations with limited resources be sure to consider a partner that can deliver best of breed technology on a monthly or quarterly basis. This provides ongoing scans of your IT operations and the expert technical support to help you spot and mediate risks within your network and end points.

SCANS and REMEDIATION

Be sure to scan your ENTIRE network and be sure you get all your end point devices (routers, PC's, tables, servers etc.) since they all can be potential targets. A good security service provider can run vulnerability scans through-out the year so you can see not only what's happening to your systems but also be assured your team's doing all they can to close gaps in and fix problems as they occur. Remember, it's your responsibility to run SRA's through-out the year. One time isn't enough.

FAST FACTS

Fines totally in the Millions

Data Loss

Did you know the most common HIPAA Violations are due to theft of unencrypted devices? Does your Security Risk Analysis check to be sure ePHI data storage devices and sites (CLOUD) are encrypted?

Just on Laptop

$2.5M+

Even seemingly simple theft or data loss can cost you millions.

One Malvern PA based CE was fined $2.5 Million dollars when they reported the theft on a single, unencrypted laptop. In another case a Texas based Hospital was fined the same amount for the theft of a single patient's ePHI.

LEARN MORE

WWW.CSMHOSTING.COM

323-909-8107

EMAIL: SALES@CSMHOSTING.COM

The Security Rule

This establishes a set of national standards for confidentiality, integrity and availability of ePHI. The Department of Health and Human Services (HHS), Office of Civil Rights (OCR) is responsible for administering and enforcing these standards, in concert with its enforcement of the Privacy Rule, and may conduct complaint investigations and compliance reviews.

When a covered entity is deciding which security measures to use, the HIPPA Security Rule does not dictate those measures but requires the covered entity to consider several factors like the size, complexity and capabilities of the organization. It also needs to review and assess it's technical, hardware and software infrastructure for potential vulnerabilities. It also should include the costs of security measures and the likelihood and possible impact of potential risks to ePHI. ***Covered Entities must review and modify their security measure to continue protecting ePHI in a changing environment.***

When Data encryption isn't enough.

Protecting ePHI from theft is just the beginning. Your systems must have security measures in place to PREVENT the theft in the first place. While data loss results in the some of the biggest fines, knowing you're vulnerable could put you and your organization at risk. HIPAA requires that you take reasonable steps to secure not only your data but access to it as well. That means secure passwords, virus and malware checks, intrusion detection and database protection.

ADVANCE THREAT PROTECTION can safeguard your users, your data and prevent data loss. Data can be 'physically' stolen but more and more often, thieves are getting into your network through social engineering tricks or phishing schemes. And once their inside your network they can drop malware or 'bots' on your network that access databases.