YOUR HIPAA RISK ANALYSIS IN FIVE STEPS

A HOW-TO GUIDE FOR YOUR HIPAA RISK ANALYSIS AND MANAGEMENT PLAN
YOUR HIPAA RISK ANALYSIS IN FIVE STEPS

A HOW-TO GUIDE FOR YOUR HIPAA RISK ANALYSIS AND MANAGEMENT PLAN

INTRODUCTION

A Risk Analysis is a way to assess your organization’s potential vulnerabilities, threats, and risks to PHI. It is the first and most vital step in an organization’s Security Rule compliance efforts. The Department of Health and Human Services (HSS) states, “Conducting a Risk Analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a Risk Analysis is foundational.”

Unlike popular belief, a HIPAA Risk Analysis and Risk Management Plan are not optional.

There are several reasons why every healthcare organization should take the Risk Analysis very seriously. First, this process will help you identify your organization’s greatest areas of risk. Next, in the event of a data breach or random audit, organizations that have not conducted a thorough and accurate Risk Analysis can expect to be hit with severe financial penalties.

Next, the Risk Management Plan is the compliance step that works through issues discovered in the Risk Assessment and provides a documented instance proving your active acknowledgment (and correction) of patient health information (PHI) risks and HIPAA requirements.

The HHS has stated on multiple occasions they will make examples of healthcare organizations that put PHI at risk. Given the importance associated with the Risk Analysis and Risk Management Plan, you may want to consider working with a HIPAA security expert.
CONDUCTING A RISK ANALYSIS

The purpose of the Risk Analysis is to help healthcare organizations document potential security vulnerabilities, threats, and risks.

A vulnerability might be a flaw in building designs that might lead to PHI being stolen.

A threat is the potential for a person, group, or thing to cause a vulnerability. For instance, what would happen if you have a disgruntled employee? Would they be able to get back into the system and obtain PHI after they were fired?

Lastly, you need to know your risks. Think about the probability that a particular threat may take advantage of a specific vulnerability. For example, if you use a Windows XP machine with access to the Internet, there is an extremely high probability that a hacker will exploit security flaws (due to the discontinued support for WinXP servers) using malicious software and gaining access to PHI.

Though the HHS does not specify an exact Risk Analysis procedure, they do require certain elements be present in a Risk Analysis, specifically:

- Scope analysis
- Data collection
- Vulnerabilities/threat identification
- Assessment of current security measures
- Likelihood of threat occurrence
- Potential impact of threat
- Risk level
- Periodic review/update as needed

THE PURPOSE OF THE RISK ANALYSIS IS TO HELP HEALTHCARE ORGANIZATIONS DOCUMENT POTENTIAL SECURITY VULNERABILITIES, THREATS, AND RISKS.
STEP 1: MAP OUT YOUR PHI FLOW

To identify your scope (the areas of your organization you need to secure), you have to understand how patient data flows within your organization. If you know all the places PHI is housed, transmitted, and stored, you’ll be able to better safeguard those potential vulnerable places.

There are four main parts to consider when defining your scope:

• Where PHI starts or enters your entity
• What happens to it in your system
• Where PHI leaves your environment
• Where potential or existing leaks may be

WHERE PHI ENTERS YOUR ENVIRONMENT

In the PHI lifecycle, it’s important to identify where all PHI enters or is created. By doing this, you know exactly where security should begin.

For PHI entry, think of both new and existing patient records. PHI can begin from patients filling out their own information on physical paper, to the front desk taking messages for their physicians, to business associates faxing you about current or former patient information.

Ask the following questions and document your responses:

• **Email:** How many computers do you have, and who can log on to each computer?
• **Texts:** How many mobile devices do you have, and who owns them?
• **EHR entries:** How many staff members do you have entering data?
• **Faxes:** How many fax machines do you have?
• **USPS:** How is incoming mail handled?
• **New patient papers:** How many papers are patients required to fill out, and where? Front desk? In the examination room?
• **Business associate communications:** How do business associates communicate to you?
• **Databases:** Do you receive marketing databases of potential patients to reach out to? What records and data do you enter into your database?
WHAT HAPPENS TO PHI INSIDE YOUR ENVIRONMENT

You need to know what happens to PHI once it enters your environment. Is it automatically stored in your EHR? Does it go directly to accounting for billing?

Additionally, you must record all hardware, software, devices, systems, and data storage locations that touch PHI in any way.

Here are common places PHI is stored:

- EHR/EMR systems
- Filing cabinets
- Workstations
- Computers
- Servers
- Laptops
- Email
- Applications
- Mobile devices
- Operating systems
- Calendar software
- Encryption software
- Wireless (networked) medical devices
HOW DOES PHI LEAVE YOUR ENVIRONMENT?

When PHI leaves your organization, it is your job to ensure it is transmitted or destroyed in the most secure way possible. You and your business associate are responsible for how the business associate handles your PHI.

Here are some things to consider when PHI leaves your environment:

- **Business associates:** Are you sending through encrypted transmission? Are they? Is data sent to them kept at a minimum?
- **Email:** What procedures are in place for how patients receive data?
- **Flash drives:** What policies are in place?
- **Trash bins on computers:** How often are these cleared out?

After knowing these processes, you should find gaps in your security and environment, and then properly secure all PHI.
STEP 2: IDENTIFY VULNERABILITIES, THREATS, AND RISKS

Find the problems within your environment, specifically:

- What vulnerabilities exist in the system, application, process or people
- What threats, internal, external, environmental and physical, exist for each of those vulnerabilities
- What probability does each threat triggering a specific vulnerability

Consider these categories in particular as you think about your vulnerabilities, threats, and risks:

- **Digital**: (e.g., weak passwords)
- **Physical**: (e.g., not shredding PHI)
- **Internal**: (e.g., employees)
- **External**: (e.g., hackers)
- **Environmental**: (e.g., fires)
- **Negligent**: (e.g., unknowing employee)
- **Willful**: (e.g., disgruntled former employee)
A VULNERABILITY IS A FLAW IN COMPONENTS, PROCEDURES, DESIGN, IMPLEMENTATION, OR INTERNAL CONTROLS. VULNERABILITIES CAN BE FIXED.

WHAT ARE YOUR VULNERABILITIES?
The HHS explains, “Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access to or disclosure of ePHI. Vulnerabilities may be grouped into two general categories: technical and nontechnical. Nontechnical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems.”

Some examples of vulnerabilities are:
- Unpatched operating system software
- Website coded incorrectly
- No office security policies
- Misconfigured or no firewall
- Computer screens in view of public patient waiting areas
WHAT ARE YOUR THREATS?
A threat is the potential for a person or thing to cause a vulnerability. Physical location, organization size, and systems all have the potential to be a threat.

According to the HHS, “There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental.

Examples of threats can be:
- Geological threats, such as landslides, earthquakes, and floods
- Hackers downloading malware onto a system
- Inadvertent data entry or deletion of data
- Power failures
- Chemical leakage
- Workforce members
- Business associates

WHAT ARE YOUR RISKS?
Risks are the probability that a particular threat will take advantage of a particular vulnerability and the resulting impact on your patients and organization.

For example, a system that allows weak password is vulnerable to attack. The threat is that a hacker could crack the password and break into the system. The risk is the unprotected PHI in your system.

According to the HHS, “risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.”

An example of risk is when remote access is connected to a PHI system with a weak password. There is an extremely high probability (“high” risk) that an external hacker will brute force the password and gain access to the system.
STEP 3: ANALYZE YOUR HIPAA RISK LEVEL

You need to decide what risks could and will impact your organization. This risk and impact prioritization is a crucial part of your Risk Analysis that will eventually translate to your Risk Management Plan.

To analyze your risk level, consider the following:

- **Likelihood of happening**: Just because you are threatened by something, doesn’t necessarily mean it will have an impact on you. For example, organizations in Florida and Colorado technically could both be affected by a hurricane. However, Florida-based organizations have a higher hurricane risk level.

- **Potential impact**: How would this particular risk effect your organization? For example, while a computer screen might accidentally show PHI to a patient in the waiting room, it probably won’t have as big of an impact as an attacker accessing your unsecured WiFi.

Every vulnerability and associated threat should be given a risk level. The typical designations are ‘high,’ ‘medium,’ and ‘low.’ Documenting this information gives you a prioritized list of security issues.
STEP 4: CREATE YOUR RISK MANAGEMENT PLAN

The Risk Analysis outcome should directly feed into a Risk Management Plan. You should also include all HIPAA Security, Privacy, and Breach Notification requirements in your Risk Management plan.

There are many ways to approach the Risk Management Plan, but ultimately the process will consist of three main steps:

1. Plan how you will evaluate, prioritize, and implement security controls.
2. Implement security measures that address the greatest areas of risk first.
3. Test the security controls you’ve implemented and be sure to keep an eye out for new areas of risk.

THE HIPAA SECURITY RULE REQUIRES YOU TO COMPLETE THE RISK ANALYSIS AND RISK MANAGEMENT PLAN AT LEAST ONCE A YEAR.
Although specific items included in a Risk Management Plan vary, the following points are industry best practices:

- **Each HIPAA rule and its takeaway:** You should list each HIPAA rule (all 157 of them) and the corresponding resolutions.

- **Risk level:** Each vulnerability discovered should be assigned a risk level. You can get some of this information from the Risk Analysis, but may have to estimate the rest based on current breach and hacker activity.

- **Date completed:** Including a completion date is great for both HHS documentation and your own records.

- **Completed by:** This is great for practices where two or more people (such as a doctor and office manager) are completing a Risk Management Plan together.

- **Comments:** It’s helpful to include a comments section next to each requirement, especially what policy and procedure the item is associated with and how you will implement the task.

---

**68% OF ORGANIZATIONS HAVE CREATED A FORMAL HIPAA RISK MANAGEMENT PLAN.**

*From the SecurityMetrics HIPAA Security Rule Report*
STEP 5: DOCUMENTATION

One of the most important parts of your Risk Analysis is documentation. If you don’t document the previous steps, you can’t prove to the HHS that you’ve completed a complete and thorough Risk Analysis. They will want to see documentation, your Risk Management Plan, and regular progress on addressing the items identified in that risk management plan.

AS FAR AS THE HHS IS CONCERNED, IF IT’S NOT DOCUMENTED, IT NEVER HAPPENED.
THIRD-PARTY SCANS AND TESTS

It’s difficult, if not impossible, to find every weakness in your organization on your own. To take your security to the next level and to avoid weaknesses in your IT system, consider implementing additional services such as:

- **Internal and external vulnerability scans**—automated testing for weaknesses inside and outside your network
- **Penetration tests**—live, hands-on testing of your system’s weaknesses and vulnerabilities
- **Nmap scanning**—a simple network scan that identifies open ports and services on your network
- **Gap analysis**—consultation on where your gaps in security and compliance exist and what steps need to occur next
AN AUDITOR’S PERSPECTIVE

As we work with individual entities, we find that because they attempt to perform a Risk Analysis with only in-house talent or a non-security professional, many vulnerabilities and risks are missed.

A COMPLETE AND THOROUGH RISK ANALYSIS IS CRITICAL AS THE LAUNCHING PAD FOR SECURING YOUR PATIENT INFORMATION.

An in-house Risk Analysis can be a great first step toward HIPAA compliance, but if your staff is pulled too thin (as they almost always are), you probably won’t see accurate results. Also, keep in mind that some IT staff members don’t want to show the boss their own security blunders.
CONCLUSION

A Risk Analysis should be updated periodically (at least annually), especially when new vulnerabilities, threats, and risks arise. It can be a lengthy process, so start by identifying (and resolving) your organization’s top weaknesses, and repeat the Risk Analysis process for medium and low risks.

HOW VULNERABLE IS YOUR PATIENT DATA?

Join over 800,000 organizations and let SecurityMetrics protect your patient data.

consulting@securitymetrics.com | 801.705.5656