Clearwater

Whitepaper

Risky Business: How to Conduct a NIST-based Risk Analysis to Comply with the HIPAA Security Rule

In addition to being a HIPAA Security Rule requirement, conducting regular risk analyses is a fundamental business practice, yet many healthcare organizations struggle with the basics, from understanding

Table of Contents

Introduction

Risky business

Despite many warnings from the Office for Civil Rights (OCR) about weaknesses uncovered during its 2011-2012 Phase 1 and 2016/2017 Phase Two HIPAA compliance audits, many covered entities and business associates struggle with understanding and successfully implementing risk analysis and risk management as outlined by the HIPAA Security Rule.

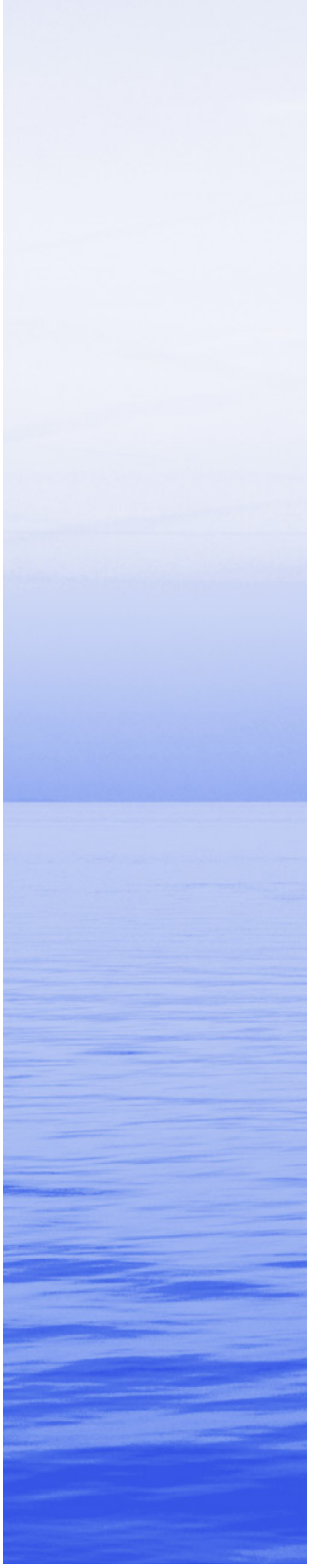
OCR is the enforcement agency responsible for investigating HIPAA complaints, and if warranted, issuing penalties and corrective measures. OCR's investigative process generally begins with a request for a documented risk analysis and risk management plan, and according to an OCR report published in late 2020, most of the healthcare covered entities and business associates OCR reviewed during Phase Two audits were not compliant for HIPAA-mandated risk analysis and risk management

Attackers know many healthcare organizations struggle understanding their risks and how to mitigate them, and they're taking full advantage. In the first half of 2021 there were 360 breaches reported to OCR, outpacing the same period for all previous years. Those 360 breaches exposed data on nearly 23 million patients. Last year, organizations reported 270 breaches of 8 million patients' data in the first six months of the year; in 2019, around 230 breaches that exposed data on 11.2 million patients.

These statistics should be a wakeup call for all covered entities and business associates.

Failing to successfully implement mandated risk analysis and risk management practices can lead to breaches that expose protected health information (PHI), resulting in fines and penalties that can cost your organization thousands—maybe even millions—of dollars, not to mention a loss of public trust and potentially catastrophic consequences for your organization.

Risk analysis and risk management isn't just for HIPAA, it's also a regulatory requirement for PCI and others. But beyond that, regular risk analyses is a fundamental business practice for operational resilience. So why do so many healthcare organizations struggle with the basics, from understanding what's involved to conducting the analysis and beyond?



In this white paper, we'll explore some of these challenges, including OCR guidance on risk analysis and risk management, as well as:

- Understanding risk
- Responding to risk
- Defining risk analysis
- Why risk analysis is good business practice
- Triggering an OCR investigation
- Step-by-step guide to conducting a HIPAA Security Risk Analysis
- Risk analysis best practices
- Other helpful resources

> According to a report published in late 2020, most of the healthcare covered entities and business associates the Office for Civil Rights (OCR) reviewed during Phase Two audits were not compliant for HIPAA-mandated risk analysis and risk management.

Understanding risk and other important variables

Before taking a deeper dive into what a HIPAA risk analysis is and how to do it, it's first important to understand what we mean when we talk about "risk" in the first place.

When defining risk, OCR's guidance leans on NIST SP 800-30, citing risk as:

- A function of the likelihood that a given threat will trigger or exploit a vulnerability
- The resulting impact on your organization

OCR goes on to say that you shouldn't look at risk as a single event or a single factor. Instead, it's viewed as a combination of events or factors, for example, a combination of your vulnerabilities and threats that, if exploited, would have a negative impact on your organization.

Here's another way to look at risk: It's a derived value. For example, risk takes into account the probability or likelihood of an event, as well as its severity and impact.

For a risk to exist for your organization, you must have three key factors:

1. An asset
2. A threat
3. A vulnerability

If you're missing one of these three, you don't have risk.

Here's an example:

- Let's say you have a laptop with sensitive information on it.
  - This is your asset.
- This laptop is not encrypted.
  - The lack of encryption is your vulnerability.
- This laptop stays locked away in a secure building. It's never connected to the internet, and no external drives or other devices can connect to it.
  - This would not constitute a risk because there are no threats present.

Now, let's look at this same scenario in a different light. In this example, your asset (the laptop) and vulnerability (no encryption) are the same. But in this version, a nurse has access to the laptop and often takes it to patient visits. Sometimes, she even takes it home after work, and she uses it to browse the web in her off time.

Because the asset has a vulnerability and is now introduced to a threat (the internet and unsecure access while in the nurse's possession), you now have all three variables and you have risk.

In addition to understanding risk, here are a few other key terms that can help you better understand OCR expectations for a HIPAA Security Risk Analysis:

- **Asset:** Any property, system or object that creates, receives, maintains, transmits or otherwise accesses PHI or other sensitive data (i.e. laptop, server, backups, mobile devices, etc.)
- **Controls:** Actions to reduce the likelihood of an undesired event that could occur if a threat exploits a vulnerability.
- **Risk Register:** A rank ordered listing of all the risks identified during your risk analysis process.
- **Threat:** The potential for a person or event to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. You can have natural threats, for

example a weather-related event; human threats, for example, a malware attack; or environmental threats, for example, a power failure or explosion from a chemical leak.

- **Vulnerability:** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Since the HIPAA Privacy Rule went into effect in April 2003, OCR has conducted more than 1,100 compliance reviews. While most of these (98%) have been resolved, many remain under investigation with a range of actions.

In June 2021, for example, OCR settled its 19th HIPAA Right of Access Initiative investigation, and to date for 2021, is investigating almost 400 breach incidents affecting protected health information (PHI) of 500 or more individuals (per breach).

These breaches, affecting both covered entities and business associates, cover a range of breach types, from hacking of email and network servers to unauthorized disclosure or access of PHI through electronic medical records (EMR), papers, and film.

Responding to risk

Once you've established the presence of risk (1. Asset x 2. Vulnerability x 3. Threat) you should then assess the likelihood the threat could exploit the vulnerability. From there, you can better understand the impact or harm to your organization so you can plan how you will respond to that risk.

When it comes to risk response, there are generally four risk-response options:

- Accept
- Transfer
- Mitigate
- Avoid

Generally, the level of likelihood of an adverse event occurring, coupled with the level of potential impact it would have, dictates your risk response.

If you (and/or any vendor you hire to support your risk analysis efforts) are not using the terminology outlined above to address risks in terms of likelihood and impact, you should rethink your approach. And fast.

What is risk analysis?

Now that you have a better understanding of what risk is and the factors that impact it, let's take a closer look at what defines risk analysis.

Earlier, we mentioned OCR's ongoing investigations. The 388 investigations from January through the end of July 2021 show exposures for millions of patient records. Just one breach in early January 2021 potentially exposed more than 3.5 million PHI records through a hacking/IT incident involving a network server for Florida Healthy Kids Corporation, making it one of the largest healthcare data breaches of all time.

This breach occurred through the supply chain, a vendor called Jelly Bean Communications Design, which Health Kids used for website hosting and storage for health and dental insurance applications.

As OCR subjects all of these healthcare organizations and businesses to scrutiny for these breaches—and if trends continue as they have for the past decade—we're likely to see a large number who haven't conducted proper analyses or risk management.

So, what constitutes a formal risk analysis based on OCR guidance?

A risk analysis, based on the HIPAA Security Rule, is NOT just one of these or a combination of some of them:

- Technical testing such as:
  - Network vulnerability scans
  - Web application scans
  - Penetration tests
  - Social engineering tests
- Gap assessments
- Asset inventories
- Threats and vulnerability lists
- Remediation plans for vulnerabilities

It's also important to note here that OCR's risk analysis guidance points out it's not intended to be a one-size-fits-all blueprint, but instead your organization should use it as a clarification about requirement expectations. How your organization actually meets compliance should include evaluation of this guidance, but also your organization's unique characteristics and your environment.

Since it isn't a black-and-white how-to, this is from where much of the confusion arises and why so many organizations struggle to achieve compliance.

However, you may find it helpful that much of the guidance is based on National Institute of Technology (NIST) standards, which have many relevant applicable controls to help secure PHI.

Based on the HIPAA Security Rule, a formal risk analysis should include:

- Create an accurate and thorough assessment (inventory) of potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI your organization creates, receives, maintains, or transmits
- Understand significant threats and vulnerabilities
- Establish effective controls
- Determine a risk rating and likelihood of harm
- Develop compliance documentation and management reports

Why do you need to do risk analysis?

While the HIPAA Security Rule mandates risk analysis, in general, it's just a good business practice. It can help you identify security risks and vulnerabilities so you can make plans to fix them before an attacker gets access to your sensitive and protected data.

A proper risk analysis is the foundation of your security efforts and serves as a platform for effectively conducting risk management activities in a way that will protect your organization and the PHI of those you serve.

Today, risk analysis is even more important in context of HIPAA compliance than ever. If you are a covered entity, you are also responsible for how well your business associates comply with the law, specifically how well they assess potential risks. What's more, if you are a healthcare organization seeking meaningful use (MU) incentive funds, you must certify you've conducted a risk analysis and are addressing your weaknesses.

Failure to comply

Once-upon-a-time, risk analysis requirements were "new," but today, the stakes for failing to comply are high. Your organization can no longer hide behind "not knowing" about risks to avoid OCR penalties and corrective actions.

If done the right way, risk analysis can prepare you for a successful audit experience. It can better equip you to respond to an OCR investigation, or even to avoid an investigation altogether.

And, as we're seeing with recent enforcement actions, if you don't comply, you shouldn't expect just a slap on the wrist if you're penalized. That's because OCR penalties are tiered related to HIPAA violation severity. These tiers can quickly add up to totals that can put many covered entities and business associates out of business.

Consider:

- Tier 1: Your organization wasn't aware of the violation, could not reasonably avoid it, and had taken a reasonable amount of care to abide by HIPAA requirements: Minimum fine $100 up to $50,000 for each violation, with an annual limit of $25,000.

- Tier 2: Your organization should have been aware of the violation, but couldn't avoid it with a reasonable amount of care: Minimum fine of $1,000 up to $50,000 per violation, with an annual limit of $100,000.
- Tier 3: Your organization demonstrated willful neglect of HIPAA requirements and failed to try to correct the issue: Minimum fine of $10,000 up to $50,000 per violation, with an annual limit of $250,000.
- Tier 4: Your organization demonstrated willful neglect of HIPAA requirements and did not attempt to correct the violation: Minimum fine of $50,000 per violation, with an annual limit of 1,500,000.

Triggering an Investigation

If your organization is rolling the dice on risk-analysis, remember, you are placing it at significant risk.

Conducting a formal risk analysis isn't an insurance policy you take out in case your organization is randomly selected for an OCR audit.

The reality is the odds are you'll never be among the chosen few who go through the audit process. The bigger reason for making sure you adhere to the guidelines and thoroughly analyze risks is to avoid formal investigations. An even bigger reason is to maintain the trust and confidence your patients, members, and customers have in your organization.

Many activities can trigger an OCR investigation. Here are some examples:

- Consumer complaints
- Breaches (failure to show an appropriate risk analysis will quickly escalate the severity of your situation)
- State-level inquiries (The State Attorney General's office and other state organizations (i.e. California Department of Public Health) can spark state or federal investigations

6 best practices for risk analysis

So how do you do a risk analysis to help your organization stay clear of an OCR investigation (or be well-prepared to respond if you do)? Here are six best practices to consider.

- **Do your homework.**
  - Review OCR guidance to ensure you have a full understanding of risk analysis requirements. Carefully select an outside partner to assist you in getting and staying compliant.
- **Update your risk analysis periodically.**
  - Thoughtful and effective risk analysis activities should occur at least annually, and should also be triggered whenever there is significant change within your organization.
- **Develop a consistent and repeatable approach**
  - Assign a point person to coordinate risk analysis activities. Use common terminology and processes across your organization. Use a standard format and methodology across regions/facilities.
- **Have a system in place for managing risk. Make sure you have effective tools to help identify and manage risks.**
  - This system should also assist in the management and documentation of your ongoing risk analysis and management activities. Excel spreadsheets or other manual processes will likely come up short, so consider adopting a risk analysis and risk management platform that can improve your visibility and management from within a single solution.
- **Set realistic goals.**
  - When addressing your vulnerabilities, make sure your goals are achievable. OCR will be fair—if you have a plan. Additionally, be diligent in rating your risks so you can prioritize based on severity. You won't be able to tackle everything at once.
- **Examine your vendors.**
  - If you turn over any important operation to an outside partner or associate, you now are responsible for making sure they are doing everything they can to protect information as well. The government will expect that you have appropriately researched and vetted your vendors.

How often should I do a HIPAA risk analysis?

According to OCR, your risk analysis processes should be ongoing. When you'll need to update and document your security measures depends on a range of factors specific to your organization. Some organizations may do this once a year, others may need to do it more frequently as their organization, environment, and risk change.

Are you ready?

How would your organization fare in an OCR audit or investigation? Do you understand all of your risk analysis and risk management requirements? Are your safeguards reasonable and effective enough to prevent a breach?

The financial, legal, regulatory and reputational consequences of not conducting a formal risk analysis and taking steps to mitigate identified risks are dire.

Here are a few key takeaways to remember:

- Your risk analysis scope includes all information assets used to create, receive, maintain or transmit ePHI
- Risk analysis reporting facilitates better, more informed risk treatment decisions
- You should analyze all assets used to create, receive, maintain or transmit ePHI
- Consider all reasonable and appropriate administrative, physical, and technical controls
- Consider all relevant threat sources and threat agents
- Consider and identify all relevant vulnerabilities
- Your risk analysis serves to identify, value and prioritize all risks
- Ensure you have fast, easy, anytime, anywhere access to your risk management profile
- Ensure you're meeting your business risk management goals
- Ensure your risk analysis processes specifically address risk analysis elements as outlined in OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule
- Ensure your risk analysis meets the requirements set out in the OCR Audit Protocol on Risk Analysis

As a healthcare entity, your information is more valuable and more vulnerable than ever. As a result, industrywide, our focus on risk analysis will continue to grow and will likely remain the top priority for OCR as it audits and investigates HIPAA compliance. Remember, if your organization fails to show good faith effort in this area, you may be consistently and substantially penalized.

Are you ready, or are you at risk?

Other resources

Need more help? Here are some suggestions for business associates and covered entities.

On-Demand Webinars

How to Perform a Risk Analysis That Achieves Compliance and Security

Advancing Cyber Risk Analysis: The Power of Prediction

From Risk Analysis to Risk Response: How to Respond to Your Identified Cyber Risks

White Papers

From Risk Analysis to Risk Reduction: A Step-by-Step Approach

Let the Buyer Beware: The Need for HIPAA Risk Analysis in Healthcare M&A Transactions

How the NIST Cybersecurity Framework Helps Healthcare Organizations Establish and Mature Cybersecurity Programs

Blogs

Making it Easier to Identify Your Most Critical Risks

The Realities and Legalities of Risk Analysis and Risk Management in Healthcare

Using Clearwater's IRM|Analysis® Software to Perform an OCR-Quality® Risk Analysis on Telehealth Systems

Performing OCR-Quality® Risk Analysis on New Systems and Processes

OCR Re-Affirms Enterprise-wide Risk Analysis is the "Most Important Thing You Can Do to Protect Yourself" Against a Cyber Attack

Clearwater Solutions for Risk Analysis

Risk Analysis

IRM|Analysis®

ClearAdvantage® Program

Guides

30-Minute Guide to Hiring the Best Risk Analysis Company

Security Risk Assessment Tool v3.2

Guide to Privacy and Security of Electronic Health Information

NIST Guide for Conducting Risk Assessments

OCR Final Guidance on Risk Analysis

HHS Security Risk Assessment Tool

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact