Clearwater

Whitepaper

Cloud Risk Insights from a HIPAA Perspective

Table of Contents

Introduction

If you're a healthcare covered entity or business associate, you're likely no stranger to HIPAA compliance. By now, you should be well-versed in understanding that the law mandates your organization protect the confidentiality, integrity, and availability of all of the electronic personal health information (ePHI) your organization creates, receives, maintains, or transmits.

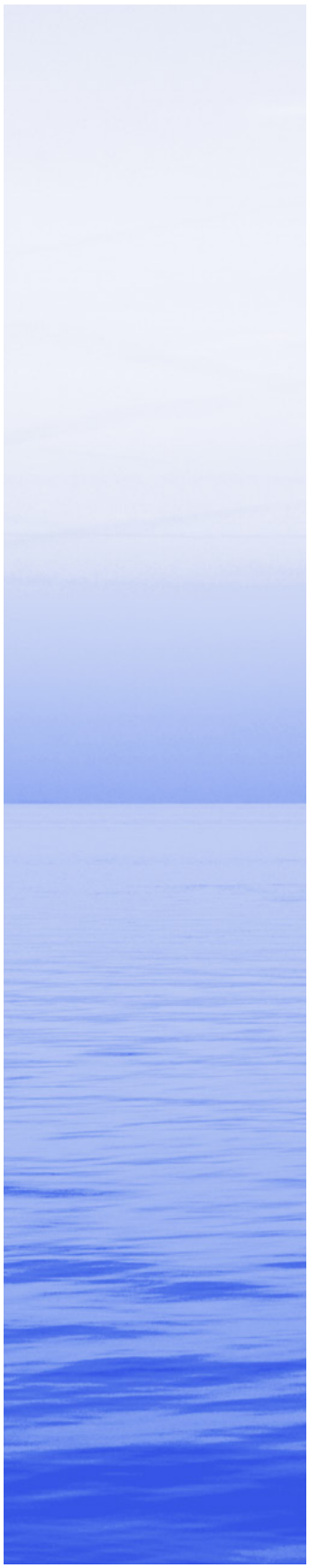
But what exactly does that mean?

For ePHI, confidentiality means your organization has controls to ensure the information isn't exposed to those who shouldn't access it. Integrity means that ePHI can't be modified. Availability means the ePHI is available according to its authorized use.

Many organizations fall short of hitting the mark on the full scope of HIPAA requirements, especially as they relate to HIPAA Security Rule risk analysis and risk management practices.

This is a long-standing issue for the industry, first noted in the Office for Civil Rights (OCR) Phase One audits in 2011-2012 and then again in its 2016-2017 Phase Two audits.

> OCR's 2016-2017 HIPAA Audit Industry Report (Phase Two) found a majority of audited healthcare covered entities (166) and business associates (41) failed to "implement the HIPAA Security Rule requirements for risk analysis and risk management."



More cloud, more risk

Since OCR completed its two rounds of audits, the industry's threat landscape has rapidly evolved and expanded, making it harder for security teams to keep up. That's largely because during and after the coronavirus pandemic, many healthcare organizations rapidly adopted digital products, services, devices, and tools to improve and expedite healthcare services delivery. Much of this lives in or is connected to the cloud.

All of these new services and assets—and their related vulnerabilities and security issues—can quickly overwhelm most security teams and complicate insight into all ePHI risks, which makes it challenging to implement security practices that support ongoing risk management.

This is further compounded if your organization shifts technologies away from on-site security and management into the cloud. While the cloud is not new to the industry, many organizations may just now be realizing the full benefits of cloud adoption and implementation.

If your organization has embraced the cloud, it's important to understand that many traditional security approaches that work for on-site technologies don't function the same for cloud environments. Even so, your HIPAA requirements are still the same.

In terms of HIPAA and ePHI privacy and security, some organizations may not know where all their ePHI is, what it's connected to, and how and to whom it flows. For example, maybe your security practices are homed in on all your public-facing web applications, but you haven't adequately secured your backups and don't actively monitor email communications with ePHI.

What would happen if an employee accidentally emailed ePHI to someone not authorized to access it?

What would happen if a team member clicked a malicious link, opening the door to a ransomware attack, and you hadn't secured your ePHI backup systems?

In these instances, your organization would be out of compliance with HIPAA mandates, but it's deeper than that. Failing to identify these issues before an incident likely means you haven't adequately addressed your HIPAA risk analysis and risk management obligations.

So, what can you do to gain more insight into your risks so you can plan to address these issues long before a breach, audit, or investigation occurs?

Here are 7 things every healthcare provider and business associate should know:

1. Organizations are HIPAA compliant, not products.

While most organizations have HIPAA basics down by now, not all understand that in terms of HIPAA compliance, the focus isn't squarely on systems, products, or security practices. It's about being a HIPAA-compliant organization and ensuring your organizational behaviors meet compliance regarding particular techniques you employ.

In other words, if you're asking:

- Is this security feature compliant?

You should be asking:

- Does this security feature satisfactorily contribute to our organization being HIPAA compliant?

This is because HIPAA compliance goes beyond asset security; it requires that you:

- Reasonably anticipate threats or hazards that could affect ePHI
- Protect ePHI against reasonably anticipated non-permitted uses or disclosures
- Ensure your entire workforce and business associates that create, receive, maintain, or transmit ePHI to do the same

Yet, many organizations struggle with this because HIPAA doesn't mandate a specific framework or control set to follow. Instead, HIPAA gives covered entities and business associates some leeway in applying their own security measures, as long as those practices are reasonably and appropriately implemented.

Without those specifications, how do you know if your organization is compliant? How do ensure you're conducting a risk analysis the right way?

We'll cover more about risk analysis later in this article, but when we think about securing an organization, its systems, and data we should approach it in the same way we would protect other valuables and assets.

For example, when you close your office at night, you'll likely lock the door on the way out, but is that enough to ensure you've protected your entire organization? While locking the door may be a good first step, you should be thinking about all of the things you're trying to protect.

- What are the reasonably anticipated threats for everything you want to protect?
- What's the threat level?
- How can you mitigate those threats?
- Which security measures will ensure protection?

A locked door is part of the solution, but it's not enough. Focusing your HIPAA efforts solely on systems or security services is like walking away with all of your windows still open and lights on. Sure, you locked the door, but you left a lot of access points—both seen and unseen—for bad actors to take advantage of you.

2. Working with compliant cloud vendors doesn't make your organization compliant.

If your organization conducts routine cloud vendor assessments, you should have insight (via reports, assessments, and attestations) about their third-party security practices.

Many organizations have traditionally conducted these assessments only at the beginning of a new vendor acquisition (i.e. at the time of a contract, service level agreement (SLA), or business associate agreement). However, this must happen throughout the length of your vendor engagement, and even so, knowing your vendor is compliant doesn't ensure that your organization is too.

Many cloud services providers (CSPs), have a shared responsibility model for cloud security. If your organization uses Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP), you should have a business associate agreement about how the CSP processes ePHI. As a best practice, only use services the CSP includes as supported for ePHI processing.

In a shared responsibility model, there are some security components your organization is responsible for, some the CSP should handle, and others where specific circumstances dictate who is responsible for what (for example, applications, network controls, operating systems, etc.).

In general, when working with a third-party CSP, your healthcare organization will likely be responsible for:

- Information and data
- Devices (smartphones, laptops, tablets, computers, etc.)
- Accounts and identities

Your CSP will likely take care of security for:

- Physical hosts
- Physical network
- Physical data center

Even though your SLA or contract may highlight who does what in a shared responsibility model, it's important to understand that ultimately, as the healthcare covered entity, your organization is responsible for ensuring you're HIPAA compliant and you've protected your ePHI.

If your business associates work with additional third parties that access your ePHI, they must be compliant, too. And although your business associates still have some liability, it doesn't absolve you of your organization's HIPAA requirements—even if you have a third party fully manage all of your security and privacy practices. You must do due diligence to ensure they take proper steps to protect your ePHI.

Cloud Deployment Models

Infrastructure as a Service (IaaS):

Scalable virtualized network, storage, and compute services that cloud customers can use to build their solutions.

Platform as a Service (PaaS):

Runtime environments for specific platforms that cloud customers can run their applications on.

Software as a Service (SaaS):
Applications that are run and managed by the service provider.

3. You must conduct a periodic HIPAA-compliant risk analysis.

45 C.F.R. § 164.308(a)(8) requires periodic technical and non-technical evaluations based on the Security standards and whenever your environment or organization changes. This isn't a one-time assessment and should be an ongoing activity.

A good rule of thumb is to conduct a risk analysis at least once a year, more frequently, if you have changes. As a best practice, consider working your risk analysis processes into your operations. Make it part of your organizational culture—the way you do business. This can help ensure you're always working toward continuous compliance goals.

Another benefit is your risk analysis can bridge the gap between your compliance and security teams and your senior executives and board members. By quantifying your risk, you can draw correlations between your compliance and security programs (effectiveness, gaps, needs, etc.) and your organization's overall goals and strategies. It's an extra layer to support operational resilience.

4. Ensure risk-based ePHI protection.

45 C.F.R. § 164.308(a)(1)(ii)(A) says organizations must conduct accurate and thorough assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of your ePHI.

Unfortunately, many organizations don't have a great understanding of what "risk" means in terms of HIPAA mandates. In the simplest terms, a risk considers the likelihood a threat actor might exploit a vulnerability or security weakness, which harms your ePHI.

For there to be a risk, you need these three components:

1. An asset
2. A vulnerability
3. Threat of exploit

If any of these three components are missing, you don't have risk. You must have insight into all of your assets and understand all of your reasonably anticipated threats so you can effectively assess your risk.

A simple equation to help: Impact x Likelihood = Risk Level

Automating part or all of your workflows can help ensure that your risk analysis processes are a part of your organization's way of doing business. With Clearwater's risk analysis solution, you can reduce risk faster and more efficiently—while using fewer resources—by simplifying the management of your risk remediation workflows.

5. All ePHI, everywhere, needs protection.

§ 164.306 general requirements say if you're a healthcare covered entity or business associate, you must ensure the confidentiality, integrity, and availability of all ePHI you create, receive, maintain or transmit.

How can you do that effectively? Comprehensive visibility is key. That means you need to know where all your ePHI is, where it flows, and all related dependencies. For example, all your databases, file systems, email systems, and logs.

It's also necessary to know which asset or service can access that ePHI, who can access it, and how it's used. To do so, you'll need a comprehensive inventory of your assets, including those that may have been forgotten or reside outside your primary location or region. Often, organizations think ePHI resides in just one system or database, but after evaluating dependencies discover there are other assets or systems that need additional security controls.

Give specific attention to your mobile devices and those that remotely connect to your ePHI systems, for example, employing identity and access management (IAM), access controls, or configuration APIs.

6. Every risk analysis should include nine core elements.

OCR has set forth guidance to help organizations with a proper risk analysis, but the technical specifications once again can be determined by each organization. However, every risk analysis should include:

1. Analysis scope: All ePHI your organization creates, receives, maintains, or transmits must be included in the risk analysis.
2. Data collection: You must document ePHI data gathered using these methods.
3. Identify and Document Potential Threats and Vulnerabilities: Identify and document reasonably anticipated threats to ePHI.
4. Assess current security measures: Assess and document security measures to safeguard ePHI.
5. Determine threat occurrence likelihood: Consider the likelihood of potential risks to ePHI.
6. Determine threat occurrence potential impact: Consider the "criticality," or impact, of potential risks to ePHI confidentiality, integrity, and availability.
7. Determine risk level: For Example, analyze the values assigned to the likelihood of threat occurrence and the resulting impact.
8. Finalize documentation: Document your risk analysis, but it doesn't have to be in a specific format.
9. Periodically review and update your risk assessment: Your risk analysis process should be ongoing. Employ continuous risk analysis to identify when you need those updates.

7. Don't forget about third-party risks.

Many organizations don't have good insight into all the risks third-party relationships introduce to ePHI, especially those in the cloud. Remember, however, that the cloud is inherently built on third-party services, so they must be included in your security assessments and evaluations.

If your third party accesses your ePHI, then it falls under HIPAA scope, and you need a business associate agreement.

A few things to keep your eyes on in your cloud environment:

- Data connections to your cloud workloads
- Marketplace products and services
- Libraries and code dependencies
- DevOps services within and out of the cloud

Never put too much faith in your vendor's machine images without verifying it is doing everything it should to protect your ePHI and be sure to review your CSP business associate agreement.

Since your cloud vendor won't likely give you direct visibility into its processes and infrastructure, be sure to review third-party attestations. If you face an audit or investigation, you want to confidently say that you've looked at those attestations and ensured the vendor did what it said it would do to protect your ePHI.

It's also good practice to keep a list of risk-approved alternative vendors. If you find your existing third-party vendor is not living up to your compliance and security agreements and won't take the necessary steps to mitigate or remediate those risks, you'll want to be prepared to move to another vendor who will.

Key takeaways

While HIPAA compliance mandates that your organization meets its standards for risk analysis and risk management practices—on-site, in the cloud, or in a hybrid environment—it's generally just good business practice.

A quality risk analysis can help your organization better anticipate and identify security risks so you can stay ahead of attackers and be well-poised to ace an OCR audit or respond to an OCR investigation.

Failing to do so could result in fines and penalties that could quickly add up to the hundreds of thousands—or even millions—of dollars, potentially putting many healthcare organizations out of business.

The Clearwater connection

Because healthcare's threat landscape is so rapidly evolving, many healthcare organizations benefit from partnering with a company like Clearwater that specializes in HIPAA compliance and cybersecurity, either as a managed service or by adopting a software solution like IRM|Analysis.

With Clearwater's support, your organization can approach HIPAA compliance with the confidence that you're:

- Knowledgeable about all of your assets and exposures
- Making more intelligent risk analyses by using AI-driven and community-powered predictive risk ratings
- Making better business decisions based on risk ratings
- Getting real-time risk information as your environment or organization scales or changes
- Benchmarking your risk metrics against peer healthcare organizations
- Ready to ace your next OCR audit

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