Clearwater

Whitepaper

# Critical Differences Between a HIPAA Security Evaluations and a Risk Analysis

# Table of Contents



# Introduction

When it comes to electronic personal health information (ePHI), HIPAA requires all covered entities and business associates to be compliant with the HIPAA Security Rule. Unfortunately, many healthcare organizations struggle with Security Rule compliance.

In fact, according to the Ofl ce for Civil Rights (OCR) Phase 2 audit report, most of the 166 covered entities and 41 business associates audited failed to "implement the HIPAA Security Rule requirements for risk analysis and risk management."

There were similar findings in OCR's Phase 1 audits.

Interestingly, the report found little difference in terms of security risk analysis and risk management compliance between covered entities and business associates.

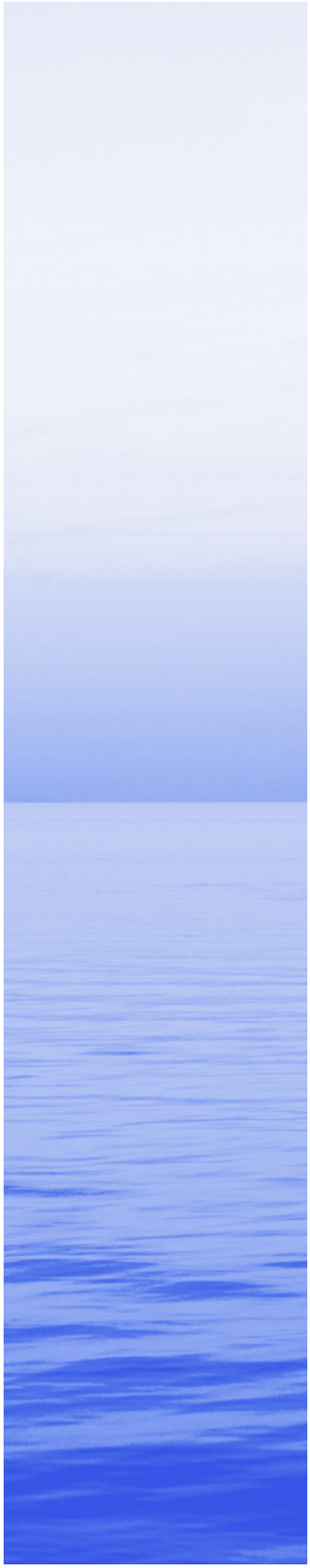
In many cases, instead of conducting a risk analysis, some organizations instead submit their technical testing or their compliance gap assessment (non-technical evaluation) information because many organizations don't have a clear understanding of the distinct differences between the three assessment types or how to conduct them in a manner that meets OCR expectations.

## There's no such thing as HIPAA certified

Some organizations choose to use a SOC2, HITRUST, or similar checklist when they're working toward HIPAA compliance and while these certifications can be helpful in maturing an organization's overall cybersecurity posture, they are not directly related to HIPAA compliance nor is there a certification that the OCR considers HIPAA certified.

Rather, the expectation is that organizations "perform a periodic technical and non-technical evaluation that establishes the extent to which an entity's security policies and procedures meet the security requirements." Healthcare organizations can do so on their own or can choose to work with a third party that specializes in these types of evaluations.

However, should an organization work with a third-party, even one that offers some type of certification, it's important to note that it could still be cited by OCR for security or compliance violations as OCR does not endorse or recognize



those certifications as related to the Security Rule. And while SOC2 and HITRUST certifications offer helpful frameworks and even serve as a source of external proof that an organization has taken cybersecurity seriously, covered entities and business associates alike should be particularly wary of any organization offering a "seal of compliance" or "HIPAA certification" lest they believe this protects them from breaches or assures favorable OCR findings.

## Three core assessments under the HIPAA security rule

The HIPAA Security Rule refers to three different types of assessments: the compliance assessment, which is a non-technical security evaluation; the technical security assessment; and the risk analysis.

Let's take a closer look at each:

### *Compliance assessments (security evlaution – non-technical, at 45 CFR §164.308(a)(8))*

This type of assessment, which can also be referred to as a performance audit, basically answers questions such as:

How compliant are we?

How well are we achieving ongoing compliance?

### *Technical assessments (security evaluation – technical , at 45 CFR §164.308(a)(8))*

The technical assessment takes a look at the efficacy of your security controls. It answers how effective the safeguards are that have been implemented.

These technical assessments may include vulnerability assessments, internal and external penetration testing, and other assessments to seek out security weaknesses that put the confidentiality, availability, or integrity of your PHI at risk.

### *Risk asessment (risk analysis, at 45 CFR §164.308(a)(1)(ii)(A))*

The risk assessment, which in HIPAA terms is referred to as risk analysis, seeks to identify exposures for PHI. It answers what exposures exist to information assets (e.g., ePHI) and what should be put in place to mitigate those risks.

To date, OCR has settled or imposed financial penalties into 111 cases, totaling nearly $132 million.

The most common issues discovered in OCR complaints include:

Impermissible uses and disclosures of PHI.

Lack of safeguards of PHI.

Lack of patient access to their PHI.

Lack of administrative safeguards of ePHI.

Use or disclosure of more than the minimum necessary PHI.

## The distinctions matter

Each HIPAA assessment is separate and distinct, but people often confuse the HIPAA technical and non-technical evaluations with risk analysis. To be HIPAA compliant, you need all three: a HIPAA Security risk analysis, a HIPAA Security evaluation, and complete technical testing of your environment.

## Conducting the assessments

### *Non-technical security evaluations*

HIPAA's non-technical security evaluations are sometimes referred to as compliance gaps or performance assessments. Some people see them as mock audits.

Some examples that would make you non-compliant:

- Incomplete or outdated policies or procedures
- Not taking reasonable and appropriate actions
- Not having implemented reasonable and appropriate safeguards
- Employees that are not trained or don't follow policies and procedures

In simple terms, a compliance assessment seeks to measure how well an organization is performing in terms of the HIPAA Security Rule guidelines. It explores:

- Are policies and procedures documented and up to date?
- Are those policies and procedures universally applied, practiced, and enforced?
- Are policies and procedures reasonable and appropriate and do they comply with implementation specifications?

A compliance assessment should evaluate how well an organization is meeting five core categories of the Security Rule:

1. Administrative safeguards
2. Physical safeguards
3. Technical safeguards
4. Organizational requirements
5. Policies, procedures, and documentation

### *HIPAA technical evaluation*

A HIPAA technical evaluation seeks to determine if there are any vulnerabilities, security issues, or misconfigurations that could put PHI at risk. Here are some examples of technical evaluations:

- External vulnerability assessment and penetration testing
- Internal vulnerability assessment and penetration testing
- Web application assessment
- Wireless security assessment
- Security awareness assessment
- Sensitive data discovery scans

### *Conducting a risk analysis*

According to NIST SP 800-30, a risk analysis is a process that identifies, prioritizes, and estimates risks. These risks may be to "organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations … resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

With a risk analysis, the goal is to identify, rate, and prioritize all risks. If a compliance assessment asks, "How compliant are we?" then the risk analysis asks, "how secure are we?"

A risk analysis helps determine:

- All of the exposures for all information assets (e.g. ePHI)
- All the ways in which the confidentiality, integrity, or availability of ePHI might be compromised

A risk analysis should tell an organization the likelihood a disruption might occur and the potential impact of disruption does occur.

The next step is to determine a risk rating, or risk register, for all of the risks associated with the most critical assets and services that create, transmit, or store PHI and then compare those risks against the organization's risk appetite to determine risk treatment.

OCR offers the following guidance for conducting a HIPAA-compliant risk analysis:

1. Include all sensitive information in the analysis scope
2. Collect and document data about all information assets (asset inventory)
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Finalize documentation
9. Periodically review and update the risk analysis

A risk analysis should never be approached as a one-and-done engagement as the rapid adoption of technologies, services, applications, and medical devices contributes to constant changes in healthcare environments and rapidly evolving threat landscapes. What might not exist as a risk today, could very well be a real risk tomorrow.

While OCR doesn't specify how often an organization should review and update its risk analysis, we recommend at a minimum, this should be done at least once a year. The reality is, a risk analysis could be done every time your environment changes.

A growing number of healthcare organizations are now building risk analysis and risk management into their system development lifecycle, building in the notion of risk management all the way at the beginning of software development or system adoption. This approach essentially builds risk analysis and risk management practices into the very beginning of an organization's processes instead of waiting to evaluate those risks at the end.

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