Clearwater

Whitepaper

Technical Testing and the HIPAA Security Rule: What's Needed to Protect Your Healthcare Organization

Table of Contents

Introduction

The HIPAA Security Rule, is a set of national standards designed to help organizations protect PHI that's created, received, used, or maintained by a healthcare covered entity, with compliance expectations that extend to business associates as well.

Specifically, 45 CFR §164.308(a)(8), addresses the role of technical and non-technical evaluations as related to Security Rule standards. Inasmuch:

"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart."

With no testing methodology or requirement specified and enforcement of this area of the Rule by the Office for Civil Rights (OCR) inconsistent, many organizations are unsure as to what steps they need to take to comply. As a result, we find investments are often being made that don't add significant value from either a compliance or a security standpoint.

In this paper, we review the role of technical testing in strong compliance and security programs and provide examples of what an appropriate technical testing program may look like for your organization.

Understanding the role of technical testing as it relates to the HIPAA Security Rule

It's not uncommon for organizations to ask Clearwater exactly what they need to do when it comes to technical testing to be in compliance with the HIPAA Security Rule. Unfortunately, there is no one-size fits all answer for every organization.

The truth of the answer is: It depends.

There is, fortunately, a way to use the ambiguity in the rule's language to your organization's advantage—if you base your strategies on your organization's strategic goals and objectives, maturity, and capacity for change.

And although the HIPAA Security Rule might be light on requirement details, there are two simplified but important points to keep front of mind:

- Testing of some kind must occur.
- This testing should occur at a regular interval.

So, what type of testing—and at what interval—is right for your organization? Well, that depends on, at a minimum, your organization's:

- Threat model, which is important to define when you're considering which type of testing your organization needs and what interval that testing should occur.
- Use of information technology systems to determine what kind of technical testing is appropriate.
- Risk assessment maturity, which is a significant part of what you have to think about when you're determining what kind of technical testing is appropriate for your organization.

> We find investments are often being made that don't add significant value from either a compliance or a security standpoint.

Understanding risk assessment maturity models

When we talk about risk assessment maturity, it may be helpful to look at it in context of risk assessment frameworks, for example, NIST's Cybersecurity Framework, whose functions align to the cybersecurity lifecycle—identify, protect, detect, respond, and recover.

In this example, there are five levels of maturity based on each of those core lifecycle components: Initial, Repeatable, Defined, Managed, and Optimized.

In this discussion, we'll begin by taking a closer look at each maturity level through the Identify stage.

Initial maturity

- When your organization is in the Initial phase, it typically has little to no cyber risk identification practices. You might be a new company that has not yet implemented processes or hasn't yet conducted technical testing, or it could be in progress. And while an early-stage organization makes sense at this level of maturity, it can also apply to larger organizations, for example, if you've had changes in leadership or positions that shift focus and, because of the scope of the environment, your team may lose track of some processes that result in a lack of clarity about what's in place and how it all works. As a result, you can't identify risks associated with all of your assets.

Repeatable maturity

- At the Repeatable level, your organization generally has processes for cybersecurity risk identification, but they are immature. For example, the processes could be in place, but they don't occur at regular intervals and technical testing may not occur on an ongoing basis. Or, for example, you do patch management, but don't have a regular schedule so you can't always identify which risks exist.

Defined maturity

- At the Defined level, your organization has identified risks to IT assets and you're managing those with standardized, well-defined processes. Your organization is engaging in proactive monitoring based on cyber risks and potential organizational impact. We often encounter many organizations at this level of maturity and they're getting ready to make the transitions to the higher maturity levels of Managed and Optimized.

Managed maturity

- At the Managed level, your organization is able to successfully identify risks to your business environment and can proactively monitor risks on a periodic basis.

Optimized maturity

- The most mature level in this model is Optimized. Here, your organization continuously monitors cybersecurity risks and your risk appetite, risk response, and other risk-related factors are incorporated into your business decisions.

Ideally, your organization should move upward through the model over time. However, regression is possible, as we saw with the COVID-19 pandemic.

For example, prior to the pandemic, you may have had a Defined maturity level, but as your environment changed—for example, moving to remote workforces—your

organization may have changed how it operates, which could have directly affected the regularity of the processes you previously had in place that applied to a mostly on-site workforce.

Other examples of how organizational maturity regression could happen include instances where your organization experiences:

- Changes in personnel or leadership (organizational structure changes)
- Changing priorities as a result of new ownership, leadership, or otherwise
- Changes in technology (specifically, attacker technology)

The role of technical testing

First, what are some examples of technical testing? When we talk about technical testing, generally we're looking at either internal or external testing practices. Some of these practices may also extend into the Cloud.

- Vulnerability scanning: A good place to start to help your organization get more visibility into the state of your infrastructure and what that looks like – for example, from a non-credentialed view (or what an attacker without internal access may see in an attempt to breach your systems and network).
- Network pen-Ttsting: This tends to be a manual process where you're looking at your systems to find exposures. Are there configuration issues? Can unauthorized users perform actions they shouldn't be allowed to? Can they use that to get access to other systems and make lateral movement across your network?
- Social engineering: Testing your organization's vulnerability to a phishing attempt or other physical social engineering ploy to gain credentials or other access to your networks, systems, and assets.
- Application pen-testing: Testing weaknesses in your web applications or mobile applications.
- Assume breach: This is approached from a perspective as if a breach has already occurred and an attacker has access to your network. Here, the goal is to see what can happen with that access, without a lot of focus on initial compromise vector.
- Red team: An authorized and organized attempt to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture.

A look at potential real-world technical testing scenarios

With a degree of ambiguity within the HIPAA Security Rule, it may be helpful to take a closer look at potential real-world scenarios based on organization size and maturity level to get a better understanding of what technical testing could look like for your organization.

These examples are designed to help you understand how you might identify and mitigate risks, while moving upward through the maturity model over time.

Remember, like any cybersecurity practice, technical testing can and should evolve as your organization changes over time.

Example 1: Small-to-mid-sized physicians management group

Business model:

- Operates a small number of regional practices
- Has a small IT team that manages all sites and infrastructure
- Infrastructure is a mix of current and legacy on-site systems, remote access infrastructure, and managed electronic health records (EHR) solutions
- 50-100 information systems/assets, some of which may be cloud-based
- Plans to purchase new practices each year, which results in the absorption of pre-existing IT infrastructure and associated risks

Maturity:

- At the Initial stage of the Capability Maturity Model
- No formalized asset management or risk assessment frameworks in place

The goal in this example is to move from Initial stage to Repeatable, including developing a playbook to help manage risk evaluations.

Technical Testing Timeline:

Here's what the technical testing timeline might look like over the span of two years, including risk evaluation for people, processes, and technology. In this example, complexity and maturity increase during the two-year period.

- Year one:
  - Conduct penetration tests at least quarterly, if possible, to identify and remediate risks. Implement changes to close security gaps and repeat to

ensure remediation and mitigation processes perform as expected.

- Test the "people" risks with social engineering, for example, phishing exercises, to determine where you have risks. You may want to do these exercises at least two times each year, for example, in the first and third quarters.
- Conduct network penetration tests, to see which systems haven't been updated or patched. In your first year, if you have a small IT team, you may want to do this at least once.

- Year two:
  - Conduct penetration tests at least quarterly to identify and remediate risks. Implement changes to close security gaps and repeat to ensure remediation and mitigation processes perform as expected.
  - Conduct additional social engineering testing, which may be more complex and focused, for example, tailored to specific individuals or roles, specifically those who may have previously fallen prey to phishing attempts or clicked malicious links.
  - Increase frequency of network testing from annually to at least twice annually or more frequently as appropriate.
  - Add cloud penetration tests to your processes to identify and address cloud security risks, especially as you move more assets and services to the cloud.

Example 2: Tech startup

Business model:

- Developed mobile and web application to interface with wearable tech–mostly cloud-hosted assets (including hosting sensitive user data)
- In the growth phase and looking for investors

Maturity:

- Built-in moderate level of asset management and risk assessment processes early on
- Allocated resources to sourcing and managing third-party technical testing at regular intervals
- Sees technical testing as function of both HIPAA Security Rule compliance and Intellectual Property (IP) protection

- At Repeatable maturity level, but wants to quickly move into Defined
- Program has elements of both Repeatable and Defined processes

Technical testing timeline:

Here's what the technical testing timeline might look like over the span of two years, including risk evaluation for people, processes, and technology.

- Year one and year two:
  - Conduct vulnerability scanning at least once each quarter against all cloud assets to identify all associated risks as well as processes needed to remediate these risks.
  - Conduct social engineering exercises at least twice a year, for example, in the second and fourth quarters, especially to decrease IP risks.
  - Add in additional testing, at least twice a year, for all web applications and mobile applications hosted in the cloud to determine any misconfiguration or other security issues.
  - Conduct cloud penetration tests at least once a year. These tests may vary depending on organization goals, but similar to network pen tests, you should implement best practices and then test against them to see if they're performing as designed.

Example 3: Large integrated delivery network (IDN)

Business model:

- Operates numerous hospitals, imaging sites, health clinics
- Thousands of employees
- Mix of vendor solutions, in-house developed web/mobile applications and accompanying backend databases/on-site data storage, cloud assets

Maturity:

- Regularly undergoes risk analyses, tabletop exercises, technical evaluations
- Medium-sized IT team with processes in place, but generally overwhelmed by the number of systems managed
- Closer to Managed maturity level than Optimized in most respects
- Interested in building capacity in order to implement better processes

Technical testing timeline:

Here's what the technical testing timeline might look like over the span of two years, including risk evaluation for people, processes, and technology. In this example, complexity and maturity increase during the two-year period, and for example purposes, this large organization has a significantly sized IT team that has the capacity to handle concurrent tests and remediation management.

- Year one and year two:
  - Unlike the previous two examples for smaller organizations at lower maturity levels, here, this team has the ability to increase vulnerability scanning cadence from once per quarter to at least six times throughout the year.
  - Conduct quarterly social engineering exercises.
  - Conduct a mix of web application and mobile application penetration tests throughout the year.
  - Conduct assume breach testing at least once a year.
  - Include twice-annual (or more) network pen tests as well as one or more cloud penetration tests.
  - In year two, move into Red Team phase, which is generally a three- to six-moth phase with specific testing designed to mitigate or remove risks for the organization

Each of the three above examples are predicated on conducting planning discussions with your organization to ascertain goals and objectives. The actual timeline and activity tempo depends on your organization's ability to execute and its appetite for change. But ultimately, every plan looks different, and you should maintain flexibility to adapt as your organization and/or external factors change.

Reframing security rule ambiguity

While historically the ambiguity within Security Rule may have caused some organizations frustration, we actually have the ability to reframe how we think about the leeway in the language. It's not about what the Security Rule lacks—what it doesn't lay out black and white for your organization to do—it's about embracing the understanding that:

- Your organization is responsible for periodic technical testing.
- You should test in a regular cadence that is appropriate for your organization based on a range of factors including your threat model, capacity for change, goals and objectives, and your organizational maturity level.
- You are empowered to make decisions for your organization based on where you are and what you need to accomplish.
- Simply conducting occasional vulnerability scans or testing is not sufficient.
- You should determine which kind of testing is appropriate for your organization at which intervals, with the understanding that the threat landscape is increasing in scale and complexity.
- Establishing a regular cadence of technical testing can help diminish risk and likelihood of incidents.

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