

# How to Improve Healthcare Cybersecurity and HIPAA Compliance

## TechRounder PDF Edition

Live article:

<https://www.techrounder.com/security/few-tips-to-defend-against-cybersecurity-attacks-with-hipaa-compliance/>

---

By Vipin PG | Published November 25, 2022 | Updated November 25, 2022 | Format: Guide | 8 min read

## Quick answer

Protecting patient data under HIPAA requires moving beyond basic checklists to focus on active risk management. You can secure your environment by conducting deep risk analyses, enforcing multi-factor authentication (MFA), and maintaining a disciplined patching schedule.

There's no such thing as a quiet day in healthcare IT anymore. Between phishing, ransomware, and unmanaged devices on your network, the environment where patient data lives is under constant pressure. This is exactly why HIPAA still matters. The point is the Security Rule gives you a realistic framework to stop a bad day from turning into a full-scale reportable breach.

When you use it correctly, HIPAA points you toward the controls that actually matter. These include risk analysis, strict access limits, better authentication, and solid audit logging. It's about workforce training, keeping up with patches, and having an incident response plan that actually works. HHS continues to provide Security Rule guidance to address these headaches. The 2023 HICP healthcare practices documents also help align these safeguards with the threats teams see on the ground today.

The stakes aren't just theoretical. If you look at OCR's recent enforcement actions, they hit the same weak spots: poor risk analysis, messy access management, and systems that should have been updated years ago. Fundamentals are what break first. This is why HIPAA compliance can help protect your patients and your reputation. If you take it seriously, you're lowering your operational risk. If you treat it as a checkbox, it's just paperwork that won't help when an attacker gets inside.

## How do you perform a real HIPAA risk analysis?

If one thing separates a serious security program from one that's just for show, it's the risk analysis. HIPAA requires a deep, accurate look at the vulnerabilities facing your ePHI. HHS emphasizes this because far too many organizations treat it like a "one and done" form they fill out once a year. A better way to handle it is to use formal risk analysis guidance to map out where your data lives, who touches it, and what happens if a system goes dark.

This process is where you find the stuff attackers love: flat networks where anyone can go anywhere, "stale" admin accounts from former employees, and cloud tools used without IT's knowledge. OCR has been blunt about this in audits. Most organizations they checked failed to properly implement risk management. That should be a wake-up call for everyone in the sector.

A good risk analysis shouldn't feel abstract. It needs to name specific systems, threat scenarios, and who is responsible for fixing things by a certain date. If your team can't explain your biggest risks in plain English, you aren't finished yet.

## What are the best ways to harden healthcare IT systems?

Modern system hardening is about more than just updating a few apps. You need to secure every surface an attacker might touch, especially VPNs, remote support tools, and email clients. In their January 2026 newsletter, HHS pointed out that unpatched software is a direct risk to the availability of patient data. It must be part of your risk analysis.

Attackers don't usually need fancy "zero-day" exploits if your environment is full of old, neglected software. A disciplined patching routine is actually more valuable than almost any expensive security product. Use your own asset inventory and the CISA KEV vulnerability catalog to figure out which flaws are being actively used by hackers and fix those first.

This logic applies to your endpoints too. If you aren't using a piece of software, get it off the machine. Limit local admin rights so a single mistake doesn't compromise the whole box. In healthcare, we often trade security for convenience, but that expands your attack surface until it's unmanageable. You have to push back on that trend.

## **How should healthcare organizations handle authentication and access?**

HIPAA says your authentication has to be appropriate for the risk. In 2026, a simple username and password just doesn't cut it. HHS has issued specific guidance on this, and CISA is clear about the necessity of multifactor authentication. Whether it's email, your EHR, or a third-party portal, MFA should be the standard across the board.

This is also where "least privilege" comes into play. People should only see the data they actually need to do their jobs. We need to get better at disabling old accounts quickly and ending the habit of shared logins. Your staff still need to protect your data with much better account hygiene than they might use for personal social media.

Attackers love "over-provisioned" environments because one compromised account can grant access to everything. By limiting that access, you're essentially shrinking the "blast radius" of any single breach. Every user should have the minimum access necessary for their specific role.

## **Why is a fast patching process critical for HIPAA compliance?**

Keeping your network updated is still one of the most effective things you can do, but patching has to be smart. You can't just update everything once a month and hope for the best. An internet-facing device might get hit in that three-week window before your next update. You need to know which systems are critical and which ones are exposed to the web.

- Identify Critical Systems: Document every system that handles ePHI and prioritize updates for internet-facing assets.
- Manage Legacy Software: For systems that are hard to patch, use network segmentation or extra monitoring to lower the risk.
- Follow HHS Goals: Use the voluntary healthcare cybersecurity goals to turn vague advice into actual expectations.

The law doesn't expect you to be perfect, but it does expect a process you can defend. If a system stays vulnerable, you should be able to explain why and what you're doing to protect it in the meantime. Consistent patching is still one of the best ways to prevent common cybersecurity attacks. It's all about speed and prioritization.

## **What are the requirements for passwords and encryption under HIPAA?**

Passwords aren't going away, but they shouldn't be your only line of defense. Use a password manager, block the use of simple or reused passwords, and remove any default credentials that came with your hardware. That is the bare minimum for any modern healthcare organization.

Then there's encryption. A lot of people get confused because HIPAA calls encryption "addressable" rather than strictly mandatory. However, encrypting data at rest and in transit is one of the smartest things you can do for your peace of mind. It makes breaches much less damaging and simplifies your legal defense if something goes wrong. HHS is clear that if you're sending data over an open network, it needs protection.

This means you need to look at laptops, phones, backups, and even how people send files. If staff are texting patient info through unapproved apps or moving data to personal thumb drives, you have a major problem. Those small habits are often how the biggest breaches start.

## **How can you monitor endpoints and backups to prevent data loss?**

Laptops and workstations are still the easiest way into your network. Whether it's a doctor's laptop or a workstation in a shared lobby, these are often the "first hop" for an attacker. Old-school antivirus isn't going to cut it anymore. You need endpoint monitoring that can spot weird behavior and alert you before it spreads.

HIPAA also requires you to have a plan for security incidents, which becomes life-or-death when ransomware is involved. The HHS ransomware and HIPAA guidance is worth a read because it connects your prevention efforts directly to your breach reporting duties. Your backups should be isolated from the main network and regularly tested.

If you say you can recover from a disaster but you've never actually tried it, you're in for a rough surprise. By keeping a constant eye on your endpoints, you can better defend against common cybersecurity attacks before they move laterally into your patient-facing systems.

## **How do you turn healthcare staff into a security defense?**

Most breaches don't look like a scene from a hacker movie. They start with a regular person clicking a link they shouldn't or getting tricked into giving up a password. That's why training is a security control, not just a boring HR task to get through once a year. Attackers are hacking people, not just code.

HHS guidance from October 2024 makes it clear that your training needs to cover modern threats:

- Phishing Awareness: Helping staff spot sophisticated emails that look like official requests.
- MFA Fatigue: Teaching staff not to click "approve" on notifications they didn't trigger.
- Help-Desk Scams: Training employees to verify the identity of anyone asking for "urgent" server access.

If everyone from the CEO to the front-desk staff is watching the same generic five-minute video, your training is too thin. The best organizations use real-world scenarios. When staff understand the "why" behind the rules, they become your best defense rather than your biggest risk.

useful change, HIPAA isn't a replacement for a security program, it's the foundation. The organizations that handle this well aren't just "compliant." They are the ones that know where their data is, keep their systems locked down, patch their vulnerabilities, and actually practice what to do when things go wrong. Start with that risk analysis and don't stop there. Strengthen your logins, watch your endpoints, and treat your staff like the important part of the defense they are.

## **Frequently Asked Questions**

## Is encryption mandatory under the HIPAA Security Rule?

HIPAA classifies encryption as an "addressable" standard, meaning you must implement it if it is a reasonable and appropriate safeguard for your environment. If you choose not to encrypt, you must document why and implement an equivalent alternative to protect ePHI. In practice, encryption is considered a standard best practice for securing data at rest and in transit.

## How often should a HIPAA risk analysis be performed?

While HIPAA doesn't set a specific calendar deadline, the law requires you to conduct risk analyses frequently enough to account for changes in your environment. Most experts recommend an annual review or whenever you implement new technology, experience a security incident, or change your business workflow.

## What is the most common cause of HIPAA security breaches?

Many breaches result from basic security failures like phishing, unpatched software, or the loss of unencrypted devices. Recent enforcement actions from the OCR show that a failure to conduct a thorough risk analysis is often the underlying reason why these technical vulnerabilities exist in the first place.

## Does HIPAA require multi-factor authentication (MFA)?

HIPAA requires organizations to implement "person or entity authentication" to verify that someone seeking access to ePHI is who they claim to be. While the word "MFA" isn't in the original text, modern HHS and CISA guidance strongly indicates that MFA is the necessary standard to meet this requirement in today's threat field.

## References

1. hhs.gov - hipaa / for-professionals - <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>
2. 405d.hhs.gov - cornerstone / hicp - <https://405d.hhs.gov/cornerstone/hicp>
3. compliancy-group.com - <https://compliancy-group.com/>
4. hhs.gov - hipaa / for-professionals - <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>
5. cisa.gov - known-exploited-vulnerabilities-catalog - <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
6. cisa.gov - topics / cybersecurity-best-practices - <https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication>
7. hhscyber.hhs.gov - performance-goals.html - <https://hhscyber.hhs.gov/performance-goals.html>
8. hhs.gov - hipaa / for-professionals - <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html>