

**Healthcare
Security**

Navigating HIPAA Updates and Changes

**A strategic guide for healthcare
security and compliance leaders**

The Compliance-Comfortable Era is on the Way Out

Since 2003, HIPAA's Security Rule has given healthcare organizations room to maneuver. Safeguards were split into two buckets: **“required”** and **“addressable.”** The second category was supposed to mean “assess and apply as appropriate.” In practice, many organizations treated it as “optional.”

That era is ending.

The proposed HIPAA Security Rule overhaul, published in the Notice of Proposed Rulemaking (NPRM, 90 FR 898, January 6, 2025), eliminates the addressable/required distinction entirely. Every safeguard would become mandatory under the proposed rule. Encryption at rest. Penetration testing. Annual risk analysis. Patching timelines would be measured in days, not quarters. The NPRM also introduces entirely new standards that weren't in the original rule. The most significant is multi-factor authentication on every relevant electronic information system, not just those that store ePHI, but any system that could affect its confidentiality, integrity, or availability.

Whether this rule passes in its current form or gets adjusted at the margins, the direction is clear. OCR's Phase 3 audit program, launched in December 2024 under the current rule, has announced plans to audit 50 organizations. And a federal appeals court's decision in *University of Texas M.D. Anderson Cancer Center v HHS* to overturn a \$4.3 million fine, because the encryption requirement was merely “addressable,” exposed exactly why regulators want these loopholes closed.

The question for security leaders isn't whether to prepare. It's how fast you can close the gap between where you are and where the rule expects you to be.

What's Actually Changing: Five Requirements That Will Hit Hardest

The NPRM is a dense, 300-page document. But the changes that matter most for healthcare organizations come down to a handful of mandates that, for many, represent a significant operational shift.

1.

MFA Across All Relevant Electronic Information Systems, No Exceptions

The proposed rule requires multi-factor authentication across every 'relevant electronic information system,' defined as any system that creates, receives, maintains, or transmits ePHI, or that otherwise affects its confidentiality, integrity, or availability. That scope is broader than most organizations expect. It pulls in infrastructure and support systems, not just the applications where patient data lives.

Here's where it gets difficult. Most hospitals don't have a centralized asset inventory. They don't have a reference architecture that maps which applications hit which servers. They don't have clear ownership records. A former hospital CISO on Coalfire's healthcare advisory team describes the problem this way: If a zero-day drops today, you have to get 60 people on a call and figure out who owns each server.

Before you can deploy MFA everywhere, you need to know what "everywhere" looks like. That means centralized asset management comes first. It's the unglamorous prerequisite that makes every other control possible.

2.

Encryption Required at Rest and in Transit

Under the proposed rule, encryption would no longer be addressable. It would be mandatory.

Many organizations have handled in-transit encryption reasonably well, especially those in the Microsoft ecosystem. But encryption at rest is a different story. Internal databases, on-premise data centers, legacy applications—plenty of healthcare organizations have significant gaps here. If your data sits unencrypted on a server in your facility, the proposed rule says that's not acceptable.

The *M.D. Anderson v HHS* case makes this painfully concrete. Unencrypted laptops and flash drives led to a multi-million-dollar fine. The fine was overturned on appeal after the Fifth Circuit found that the encryption standard, as written, did not support the penalty. The addressable nature of the requirement was central to that ruling. The proposed rule would close that gap.

3.

Critical Patches in 15 Days, High Severity in 30

The NPRM would set explicit timelines for vulnerability remediation. Critical vulnerabilities would need to be patched within 15 days. High-severity vulnerabilities would be subject to a 30-day remediation. Everything else falls under “reasonable and appropriate” judgment.

On paper, most hospitals already have patching policies that say something similar. In practice, the gap between policy and execution is wide. Some critical patches bring down infrastructure. Some affect FDA-approved medical devices that require their own approval cycle before updates can be applied. When a device manufacturer releases a patch for a patient monitor, it has to go through FDA testing first. That cycle can take months. Under the proposed rule, the hospital is still liable if something happens in the meantime.

Organizations will need to get creative: network segmentation to isolate systems that can’t be patched quickly, compensating controls, documented risk assessments for every exception. The proposed rule would force organizations to document compensating controls and segmentation strategies for systems that cannot be patched within the window, rather than allowing exceptions to go undocumented.

4.

Annual Penetration Testing, Risk Analysis, and Compliance Assessments

The proposed rule would require three distinct annual exercises, and each one matters on its own.

First, annual penetration testing. Not a vulnerability scan with a few extra steps. A proper, scoped penetration test by qualified professionals.

Second, an annual risk analysis. This is a specific regulatory requirement under 45 CFR 164.308(a)(1)(ii)(A), and the NPRM defines minimum requirements for what constitutes a thorough one. Previously, organizations could conduct a risk analysis and then coast for a year or more, checking off changes incrementally. Some did them every three years. Under the proposed rule, that approach would no longer be viable.

Third, an annual compliance assessment. This is broader than a risk analysis. It evaluates your overall posture against the full set of HIPAA requirements, not just the risks to ePHI. Whoever performs these needs demonstrable skills and expertise. OCR has specifically called this out.

5.

Business Continuity Gets Teeth

The Change Healthcare breach was specifically referenced in the NPRM. That event put business continuity and disaster recovery under a spotlight. Proposed requirements include backup testing every 30 days, 72-hour maximum recovery time, and a mandate that business associates report activation of their continuity plans within 24 hours.

The stakes here go beyond regulatory compliance. Healthcare is designated as critical infrastructure by CISA, and for good reason. When systems go down, the consequences extend to life-saving care, medication delivery, and patient safety. Resilience isn’t an IT metric. It’s a patient outcome.

That makes the hard questions unavoidable. Have you identified the criticality of your applications and systems from a business perspective, not just a technical one? When was the last time you ran a full test of your business continuity plan, not a tabletop, but an actual exercise? Does your BC plan integrate with your incident response planning, or do they live in separate binders owned by separate teams? And on the vendor side: do you know where your data goes, are you monitoring your third-party vendors, and can you recover if one of them goes down? For many organizations, the honest answers to these questions are uncomfortable.



The Regulatory Moment: Why This Is Happening Now

Healthcare has always been a prime target for cyberattacks. The average healthcare breach costs \$10.1 million, according to the NPRM's own preamble (90 FR 898, paragraph 130, published January 6, 2025). Ransomware attacks have forced hospitals to divert patients, shut down operations, and in some cases, lose entire medical record systems.

The stakes are not theoretical. In January 2024, a ransomware attack on Lurie Children's Hospital in Chicago took its Epic EHR offline for nearly four months, exposed the protected health information of approximately 792,000 patients, and left clinicians recording patient information manually while systems were rebuilt (Source: Lurie Children's Hospital public breach notification, 2024). The operational and reputational fallout from incidents of this scale reaches far beyond the IT organization.

But the HIPAA Security Rule hadn't been meaningfully updated since 2013. The gap between the threat landscape and the regulatory framework had become untenable.

Two things pushed this forward. First, the M.D. Anderson appeals court ruling made it clear that OCR couldn't effectively enforce penalties when safeguards were merely "addressable." The agency needs the legal foundation to hold organizations accountable, and the proposed rule provides it. Second, OCR is resuming audits after largely pausing around 2020. They've announced plans to select 50 organizations for audit. If you're selected, you'll need evidence, not just a policy document.

Even if the final rule gets delayed or modified at the margins, the direction is locked in. The Trump administration paused the review process briefly, but the underlying legal and enforcement pressure hasn't gone away.

"The direction is clear. The core requirements in the NPRM reflect where OCR enforcement is already heading under the current rule. Organizations should prepare on that basis regardless of the final rule's timing or specifics."

— Swathi West, Managing Director, Healthcare Advisory at Coalfire



The Responses That Will Leave You Exposed

Waiting to See What Happens

This is the most common and most dangerous response. When the NPRM dropped last winter, CISOs across the industry scrambled. Calls were set up, boards were briefed, budgets were discussed. Then the review period stalled and momentum evaporated. “Let’s cross the bridge when we get there” became the default stance.

That’s a mistake. One organization Coalfire works with took the opposite approach: they proposed a five-year, \$30 million roadmap to prepare for the proposed rule before it was finalized. When the rule does pass, they’ll be positioned to execute. Organizations that wait will be scrambling to build a plan while their peers are already halfway through one.

Treating HIPAA as a Checkbox

Conduct a risk analysis every three years, file it, and treat the documentation as evidence of compliance. File it. Move on. This approach has been common for years, and it worked when enforcement was light and audits were rare. Under the proposed rules, it won’t hold up. The proposed rule would require risk analyses on an annual basis, not just when something changes.

A compliance assessment is broader, evaluating your overall posture against the full set of HIPAA requirements rather than just risks to ePHI. Under the proposed rule, compliance assessments would also be required annually, alongside the risk analysis. You can have a checkmark on either one and still have critical gaps in your actual security posture. The question isn’t “are we compliant?” It’s “could we survive an OCR audit right now, with evidence, interviews, and documentation to back it up?”

No Program Behind the Assessment

Even organizations that do thorough risk analyses often have no program to act on the findings. The report gets delivered. Nobody has the staff or tools to address it. Findings sit in a spreadsheet. Next year, the same findings reappear.

Do you have a GRC tool? Is there a team responsible for tracking remediation? Can you show progress year over year? If not, you’re generating evidence of your own gaps without a plan to close them.

The Conversation CISOs Need to Have With Their Boards

If you're a CISO at a midsize healthcare organization, these rule changes create an uncomfortable set of board conversations. Budget requests are the obvious one. But the harder conversation is about foundational readiness.

Most hospitals operate by plugging in new applications and systems as needed. Patient care comes first, and technology decisions are driven by clinical needs, not security architecture. The result is an environment where nobody has a complete picture of what's running, who owns it, or where ePHI lives.

The board conversation isn't just "we need more money." It's "we need to know what we have before we can protect it." Centralized asset management. Role and responsibility mapping. A reference architecture. These are phase-zero requirements that most hospitals haven't completed.

And this isn't just the CISO's problem. Cybersecurity risk is organizational risk. When a hospital gets hit by ransomware and diverts patients for weeks, the fallout lands on the CEO, the board, the CFO. The idea that cybersecurity belongs solely to the security team is outdated and dangerous. Boards need to own this. For organizations where SEC cyber disclosure requirements apply, board-level oversight of cybersecurity risk is already a fiduciary expectation, not just a best practice.



The AI Complication

HIPAA was written for a world of fax machines and email. AI introduces risks that the original framework never anticipated. Doctors are using ambient listening apps that record patient conversations and generate chart notes. Revenue cycle teams want automation to route calls. Clinicians are pasting symptoms into ChatGPT.

The privacy implications are staggering. Many of these tools haven't been vetted for HIPAA compliance. Patients don't know they're being recorded. Nobody is reviewing the AI-generated notes for accuracy. And the apps storing this data may not have adequate data retention or destruction policies.

The proposed HIPAA rules are designed to be technology-agnostic, meaning AI tools go through the same risk analysis process as any other system. But the speed at which AI is being adopted, often driven by board-level pressure to stay competitive, outpaces most organizations' ability to govern it.

The practical approach, according to Coalfire's healthcare advisors: don't try to ban AI. Instead, establish governance. Create a process where teams can submit use cases. Approve specific tools. Give people something secure to use, because if you don't, they'll use whatever they find on their own.



Coalfire's AI Security & Trust Engineering Perspective

AI doesn't break HIPAA, but it breaks assumptions that many security programs still rely on.

Through Coalfire's AI Security & Trust Engineering work, we see a developing pattern across healthcare systems: AI tools are introduced as "productivity features," not regulated systems. That means they often bypass the controls that HIPAA expects: identity and access management, risk analysis, data flow mapping, access control, vendor oversight, and documentation.

The organizations making progress aren't trying to slow AI adoption. They're treating AI like infrastructure: engineering security and compliance into how models are selected, integrated, monitored, and governed from day one.

Questions about building and securing your AI systems? Ask us.

Coalfire's AI Security & Trust Engineering team helps healthcare organizations govern and utilize AI with confidence.

Where Coalfire Fits: Beyond the Assessment

Most compliance firms do one thing. They audit you, hand you a report, and leave. Coalfire does that too, but the difference is what happens after.

Our healthcare practice covers the full lifecycle. Risk analysis to tell you where you stand. Advisory services to help you build a holistic risk and compliance program. Cloud engineering to deploy the technical controls like rolling out MFA across all relevant electronic information systems. Penetration testing through an in-house offensive security team. Vulnerability management support to help you meet those 15-day patching windows. Annual compliance audits to keep you current.

One team. One relationship. Through the full compliance journey.

The OCR Advantage

Coalfire's HIPAA risk assessment reports have been used successfully in OCR audits. When your organization is selected and asked to produce evidence, having documentation built to align with OCR's real-world expectations makes a measurable difference.

Our dedicated healthcare team also conducts CMS ARC-AMPE audits, where many of the requirements reflected in current HIPAA updates are already enforced in practice. This gives Coalfire a clear, on-the-ground view of what regulators are actually looking for, and how healthcare organizations can prepare in a defensible way.

Beyond compliance, Coalfire supports **healthcare M&A transactions** with pre-acquisition cybersecurity diligence, helping buyers identify inherited risk before deals close—and before those risks become compliance or operational liabilities.



Built on Operator Experience

Coalfire's healthcare practice is led and staffed by former hospital CISOs, compliance officers, and security leaders who have sat in the same chair you're sitting in today.

That experience shapes how engagements are scoped, how findings are prioritized, and how remediation is sequenced—so recommendations align with the operational realities of running a health system, not just what looks good on paper.

What Security Leaders Should Be Doing (Now)

HIPAA expectations will continue to evolve, but the fundamentals of a strong security program do not. Here's what our Healthcare team recommends:

- Get your asset inventory in order. You cannot protect what you don't know you have. Centralized asset management is the foundation for MFA deployment, encryption, patching, and every other control. It's also the foundation for performing an accurate risk analysis (90 FR 898, p-927).
- Conduct a gap assessment against the NPRM requirements as part of a programmatic remediation plan, not as a standalone exercise. The core mandates are clear enough to start identifying where your gaps are today. The real value is with remediation, not just assessment.
- Have the board conversation now. Present the new requirements, the budget implications, and a phased roadmap. Organizations that started this conversation early will be far ahead when the rule is finalized.
- Stress-test your risk analysis against OCR standards. Could your current assessment survive an audit? Coalfire can review your existing risk analysis and tell you whether it's OCR-ready, so you're not guessing.
- Build a program, not just a report. A risk assessment without a remediation plan is just documentation of your failures. Make sure you have the staff, tools, and accountability structures to act on findings.
- Govern AI before it governs you. Establish an intake process for AI use cases. Approve specific tools. Vet them through HIPAA security and privacy requirements.

Need help with healthcare security and HIPAA?

Our Healthcare team helps you stay ahead by treating the health of your whole organization—not just the symptoms of a single gap. We'll help you align with the latest NPRM requirements while building a posture that keeps your operations resilient and secure.

Because the next OCR audit won't wait for you to be ready.

For any healthcare security needs, including HIPAA or HITRUST, get in touch with our team at coalfire.com/hipaa-meeting