ARTICLE · HIPAA

The 2026 HIPAA Security Rule Is Getting a Facelift

A plain-language breakdown of every significant change in the 2026 HIPAA Security Rule NPRM and what it means for your tech stack.

10 min read · PDF · Updated May 2026 · **goironfort.com**

In 2025, HHS published a landmark proposed update to the HIPAA Security Rule — the first major revision since 2013. The 2026 NPRM isn't a minor tweak. It's a substantial rewrite that reflects two decades of evolving threats, cloud infrastructure, and healthcare technology that the original rule never anticipated.

The Big Picture: Why This Update Was Overdue

The HIPAA Security Rule has been largely unchanged since 2003. In that time, the healthcare industry has moved from on-premises servers to multi-cloud architectures, from paper fax machines to mobile apps, from isolated hospital networks to interconnected ePHI ecosystems spanning dozens of vendors. The rule's "addressable vs. required" structure — which let organizations substitute alternative measures for many technical controls — created compliance variability that OCR found difficult to enforce consistently.

Change #1: "Addressable" Controls Become Required

This is the most sweeping change. Under the original rule, many implementation specifications were "addressable" — organizations could document why they chose alternative measures. The NPRM converts most addressable specifications to required, eliminating the ambiguity. Encryption at rest and MFA are the two highest-impact examples.

Change #2: Technology Asset Inventory Becomes Required

Covered entities must now maintain a current, documented inventory of all technology assets that touch ePHI — updated at least annually. This formalizes what security-mature organizations already do, but creates new obligations for organizations relying on informal knowledge of their technology stack.

Change #3: Incident Response Gets Specific

The NPRM adds specificity to incident response requirements that were previously vague. Organizations must have written, tested incident response plans with defined roles, escalation procedures, and recovery timelines. The 72-hour breach notification window makes a tested IR plan operationally essential.

Change #4: Vulnerability Management Timelines Defined

For the first time, the HIPAA Security Rule specifies vulnerability remediation timelines. Critical vulnerabilities must be patched within 15 days; high severity within 30 days. Scans must occur at least every six months. This brings HIPAA closer to NIST's vulnerability management framework.

Summary: What You Need to Implement

Requirement	What It Means	Effective
MFA	Required for all ePHI system access	2026
Encryption at Rest	Required for all ePHI stored on any media	2026
Asset Inventory	Annual technology asset inventory required	2026
Vuln Scanning	Every 6 months minimum; 15/30 day remediation SLAs	2026
Breach Notification	72 hours to HHS (down from 60 days)	2026
BAA Updates	24-hour incident notification; subcontractor accountability	2026
IR Planning	Written, tested, role-assigned incident response plan	2026

Get a free HIPAA NPRM gap assessment at **goironfort.com/demo** — see exactly what you need to update.