■ FEATURED GUIDE · HIPAA

The Complete 2026 HIPAA Security Rule Survival Guide

Everything health tech teams need to know about the NPRM changes — and a 90-day roadmap to compliance.

42 pages · PDF · Updated May 2026 · **goironfort.com**

What's Inside

1 · What the 2026 HIPAA NPRM Changes

In January 2025, HHS published the most significant proposed changes to the HIPAA Security Rule since its original issuance in 2003. The Notice of Proposed Rulemaking (NPRM) — officially titled the "HIPAA Security Rule NPRM" — responds to a decade of escalating ransomware attacks, data breaches, and increasingly sophisticated threats to electronic protected health information (ePHI).

The core change: many previously "addressable" implementation specifications — where covered entities could choose alternative measures — are now **required**. This shifts compliance from a risk-based discretionary framework to a more prescriptive, auditable standard.

> ■ *Key message: If your HIPAA compliance program was built before 2025, it almost certainly needs updating. The NPRM eliminates the "addressable vs. required" loophole that many organizations relied on.*

Major categories of change include:

- **Multi-Factor Authentication (MFA):** Now required for all systems accessing ePHI. No more addressable workarounds.
- **Encryption at Rest:** Required for all ePHI stored on electronic media, workstations, and servers.
- **Vulnerability Scanning:** Regular scanning required with defined remediation timelines.
- **Technology Asset Inventory:** Annual inventory of all hardware and software touching ePHI.
- **Breach Notification:** Window shrinks from 60 days to 72 hours for all breaches.
- **BAA Updates:** New mandatory terms for incident notification timelines and subcontractor oversight.
- **Incident Response Plans:** Written, tested, and documented response plans with defined roles and timelines.
- **Audit Logging:** Comprehensive audit log requirements with defined retention periods.

2 · Mandatory Technical Safeguards

The technical safeguard changes are the most operationally impactful part of the NPRM. Here is a detailed breakdown of each new required control.

Multi-Factor Authentication

MFA is required for any user accessing ePHI systems — including administrative portals, EHR applications, cloud storage buckets, and remote access systems. The NPRM does not prescribe a specific MFA technology but requires that it be implemented for all workforce members and contractors.

What to do: Audit all systems that access, store, or process ePHI. Enable MFA on every one — starting with email (the most common breach vector), cloud infrastructure, and clinical applications.

Encryption at Rest

All ePHI must be encrypted at rest using an encryption algorithm at least as strong as AES-256. This applies to databases, file servers, backup media, workstations, and portable devices. The NPRM specifies that key management procedures must be documented.

Vulnerability Scanning & Patch Management

Covered entities must conduct vulnerability scans at least every six months on systems touching ePHI, and within 30 days of significant infrastructure changes. Critical vulnerabilities (CVSS ≥ 9.0) must be remediated within 15 days; high severity (CVSS 7.0–8.9) within 30 days.

Scan Frequency	Every 6 months (minimum); within 30 days of major changes
Critical Vuln SLA	15 days to remediation (CVSS ≥ 9.0)
High Vuln SLA	30 days to remediation (CVSS 7.0–8.9)
Scan Scope	All systems that access, store, or transmit ePHI

Documentation	Scan results and remediation records must be retained for 6 years

3 · BAA Updates: New Requirements

Business Associate Agreements must be updated to reflect three new areas: (1) incident notification timelines, (2) subcontractor chain accountability, and (3) termination rights.

Incident Notification Timeline: BAs must now notify covered entities within 24 hours of discovering a suspected security incident — compared to the previous "without unreasonable delay" standard. This change compresses your vendor notification SLAs significantly.

Subcontractor Accountability: BAs must contractually require their subcontractors (sub-BAs) to meet the same security standards and maintain their own BAAs. You must maintain a registry of all downstream subcontractors who handle your ePHI.

4 · The 72-Hour Breach Notification Clock

One of the most operationally challenging NPRM changes is the breach notification timeline reduction. Under current rules, covered entities have 60 days from discovery to notify HHS and affected individuals. The NPRM proposes reducing this to **72 hours for HHS notification** (individual notification timelines unchanged).

> ■ *72 hours sounds like enough time — until you factor in investigation time, legal review, notification drafting, and executive approvals. Most organizations that haven't pre-built their breach response infrastructure will miss this window.*

Pre-built breach response infrastructure should include:

- An incident response team with defined roles (IR Lead, Privacy Officer, Legal, Communications)
- A pre-approved breach notification template reviewed by counsel
- A documented decision tree for breach vs. non-breach determination
- A real-time alerting pipeline from security tools to the IR team
- A pre-configured HHS breach reporting portal account
- Documented contact lists for affected individual notification

5 · Technology Asset Inventory

The NPRM requires covered entities to maintain a current, accurate inventory of all technology assets that create, receive, maintain, or transmit ePHI. This inventory must be reviewed and updated at least annually, and whenever a significant change occurs.

The asset inventory must include:

- Servers and virtual machines
- Workstations and endpoints
- Mobile devices
- Network devices (routers, firewalls, switches)
- Cloud services and SaaS applications
- Medical devices with network connectivity
- Third-party integrations and APIs
- Backup and archival systems

6 · Your 90-Day Implementation Roadmap

Phase	Focus	Key Activities
Days 1–14	Gap Assessment	Conduct a full gap analysis against all NPRM requirements. Inventory all ePHI-touching systems. Iden
Days 15–30	Quick Wins	Enable MFA on all workforce accounts. Patch critical and high-severity vulnerabilities. Draft updated E
Days 31–60	Infrastructure	Implement encryption at rest across all ePHI storage systems. Deploy vulnerability scanning tooling. E
Days 61–75	Documentation	Update policies and procedures for new requirements. Complete workforce training on updated protoc
Days 76–90	Validation	Run a tabletop incident response exercise. Verify asset inventory completeness. Conduct internal aud

7 · How Iron Fort Automates 2026 Compliance

Iron Fort's HIPAA module is updated for 2026 NPRM requirements. The platform continuously monitors your infrastructure against all new mandatory controls, generates your annual asset inventory automatically, manages your BAA lifecycle, and provides guided breach response workflows with built-in 72-hour clock tracking.

Book a free 30-minute gap assessment at **goironfort.com/demo** — our compliance engineers will map your current posture against every NPRM requirement and give you a prioritized remediation roadmap.