

NIST SP 800-66 REVISION 1 · REFERENCE EDITION

Basic Implementation of HIPAA Regulations

A modern, reference-style condensation of NIST's foundational HIPAA Security Rule guide — the standards, the framework, and how to apply them.

REFERENCE

STANDARDS MAP

FRAMEWORK

SP 800-66 — Basic Implementation of HIPAA Regulations

A condensed reference to NIST’s foundational guide for implementing the HIPAA Security Rule.

REFERENCE BRIEF

How to use this document

- Treat it as the **bridge** between the HIPAA Security Rule and the broader NIST Risk Management Framework.
- Use it to **defend control choices** — every safeguard maps to recognized NIST guidance.
- Pair it with the implementation playbook for activity-level execution.

What the Security Rule actually requires

The Security Rule mandates that covered entities ensure the confidentiality, integrity, and availability of all EPHI they create, receive, maintain, or transmit. It does this through three categories of safeguards plus organizational and documentation requirements.

SECTION	SUBJECT
§164.306 — General Rules	Confidentiality, integrity, availability; flexibility of approach.
§164.308 — Administrative Safeguards	Risk analysis & management, workforce, training, incident, contingency, evaluation, BA contracts.
§164.310 — Physical Safeguards	Facility access controls, workstation use & security, device and media controls.
§164.312 — Technical Safeguards	Access control, audit, integrity, authentication, transmission security.
§164.314 — Organizational Requirements	Business associate contracts; group health plan provisions.
§164.316 — Policies, Procedures, Documentation	Written rules, retention, availability, updates.

Required vs. Addressable — the recurring distinction

REQUIRED

Must be implemented as written. The only flexibility is in the method.

ADDRESSABLE

Implement, implement an equivalent, or document a defensible reason not to. **Not optional.**

The risk-management framework, condensed

Categorize

Classify systems and EPHI by impact level.

Select & Implement

Choose appropriate controls; deploy them in production.

Assess & Monitor

Test, authorize, and continuously monitor effectiveness.

Considerations when applying the Security Rule

- **Flexibility of approach** — controls scale to size, complexity, capability, and cost.
- **Technology neutrality** — the rule names outcomes, not products.
- **Maintenance** — review and modify safeguards as the environment changes.
- **Scope** — applies to all EPHI a covered entity or business associate creates, receives, maintains, or transmits.

How NIST controls map to the Security Rule

HIPAA STANDARD	NIST SP 800-53 FAMILY
Risk Analysis & Risk Management	RA — Risk Assessment
Workforce Security	PS — Personnel Security
Information Access Management	AC — Access Control

HIPAA STANDARD	NIST SP 800-53 FAMILY
Awareness & Training	AT — Awareness and Training
Security Incident Procedures	IR — Incident Response
Contingency Plan	CP — Contingency Planning
Facility Access & Workstation	PE — Physical & Environmental Protection
Device & Media Controls	MP — Media Protection
Access Control / Authentication	AC, IA — Identification & Authentication
Audit Controls	AU — Audit and Accountability
Integrity / Transmission	SC, SI — System & Comm Protection / Integrity
Policies & Documentation	PL — Planning

Common implementation pitfalls

- Treating "addressable" specifications as optional.
- Skipping the documented risk analysis and jumping to controls.
- Forgetting BAs, subcontractors, and cloud providers.
- Static policies without periodic review.
- Disposal and reuse of media without verifiable sanitization.

What good looks like

- ☐ One named Security Official with authority and budget.
- ☐ Living risk register tied to mitigations and owners.
- ☐ Control catalog cross-walked to NIST SP 800-53.
- ☐ Continuous monitoring program with measurable indicators.

☐ Documented BAs and signed agreements for every vendor.

☐ Policies refreshed annually and after material change.

☐ Six-year retention of policies, decisions, and evidence.

Source: NIST Special Publication 800-66 Revision 1 — "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" (October 2008, NIST). Modernized for clarity and reference use; substantive concepts unchanged.