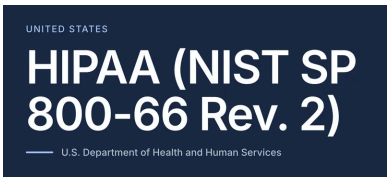
SmartSuite

Framework / Cybersecurity / NIST Special Publications

HIPAA Security Rule (45 CFR Part 164, Subpart C) — NIST SP 800-66 Rev. 2

The HIPAA Security Rule (45 CFR Part 164, Subpart C) requires covered entities and business associates to safeguard ePHI; NIST SP 800-66 Rev. 2 is the guide to implementing it.



What it is

The HIPAA Security Rule (45 CFR Part 164, Subpart C, sections 164.302 to 164.318) is the U.S. federal regulation that requires covered entities and business associates to protect the confidentiality, integrity and availability of electronic protected health information (ePHI). HHS published it as a final rule on 20 February 2003 (68 FR 8334); it took effect on 21 April 2003, and most covered entities had to comply by 21 April 2005. NIST SP 800-66 Revision 2 (February 2024) is the guide that explains how to implement it.

At a glance

PUBLISHER
U.S. Department of Health and Human Services (HHS); NIST publishes SP 800-66 Rev. 2

TYPE
Regulation

VERSION
45 CFR Part 164, Subpart C (68 FR 8334), as amended 2013 (78 FR 5566); NIST SP 800-66 Rev. 2 (February 2024)

EFFECTIVE
April 21, 2003 (compliance: April 21, 2005; small health plans April 21, 2006)

DOMAIN
Cybersecurity

FAMILY
NIST Special Publications

REGION
United States

INDUSTRY
Healthcare & Life Sciences

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: hhs.gov/hipaa/for-professionals/security/index.html

Why it matters

- **Business associates carry their own liability** A business associate is liable for its own Security Rule violations, so a vendor that handles ePHI needs its own risk analysis and safeguards, not only a contract with the covered entity (NIST SP 800-66 Rev. 2, Section 2).
- **Scalable by design** The required standards are the same for every entity, but section 164.306(b) lets size, complexity, infrastructure, cost and risk shape how an entity implements them.
- **Risk analysis anchors the program** Risk analysis and risk management are both Required specifications (164.308(a)(1)(ii)(A) and (B)), and NIST SP 800-66 Rev. 2 describes a method for each in Sections 3 and 4.
- **Documentation is retained for six years** Policies, procedures and the records the rule requires must be kept for six years from creation or from the date last in effect, whichever is later (section 164.316(b)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports HIPAA (NIST SP 800-66 Rev. 2)

ePHI Inventory and System Scope

Record each system that creates, receives, maintains or transmits ePHI, with its owner and data flows, as the first step of the NIST SP 800-66 Rev. 2 risk assessment (Section 3.2).

Risk Analysis and Risk Register

Run the accurate and thorough risk analysis of 164.308(a)(1)(ii)(A), rate likelihood and impact, and record each threat and vulnerability pair in a risk register.

Addressable Specification Decisions

For each Addressable specification, record whether it is reasonable and appropriate, the decision, any equivalent alternative and the approver (164.306(d)).

Safeguard and Policy Library

Map policies and procedures to the administrative, physical and technical standards, with an owner, a review date and every version kept for six years (164.316).

Business Associate Register

Track business associates and subcontractors, their contracts and written assurances, and review dates (164.308(b) and 164.314(a)).

Contingency and Evaluation Tracker

Keep the backup, disaster recovery and emergency mode plans, test results, periodic evaluations and open actions together (164.308(a)(7) and (a)(8)).

Common framework mappings

CIS Controls v8.1 | GDPR | HITRUST CSF v11.5 | ISO 27001:2022 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

HHS: The HIPAA Security Rule

HHS overview of the HIPAA Security Rule for covered entities and business associates.

hhs.gov/hipaa/for-professionals/security/index.html

NIST SP 800-66 Rev. 2: Implementing the HIPAA Security Rule

NIST's February 2024 cybersecurity resource guide with risk assessment steps, key activities per standard and crosswalks.

csrc.nist.gov/pubs/sp/800/66/r2/final

HIPAA Security Standards final rule, 68 FR 8334 (2003)

The 20 February 2003 Federal Register notice that adopted the Security Rule, with its effective and compliance dates.

govinfo.gov/content/pkg/FR-2003-02-20/pdf/03-3877.pdf

HIPAA Security Rule proposed rule, 90 FR 898 (2025)

The 6 January 2025 notice of proposed rulemaking to strengthen the cybersecurity of ePHI; not yet a final rule.

govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf

Frequently asked questions

What is the difference between required and addressable specifications?

A Required implementation specification must be implemented. For an Addressable one, the entity assesses whether it is reasonable and appropriate in its environment. If it is, the entity implements it. If not, it documents why and implements an equivalent alternative measure where reasonable (section 164.306(d)).

Does the Security Rule prescribe a risk analysis method?

No. Section 164.308(a)(1)(ii)(A) requires an accurate and thorough assessment of risks and vulnerabilities to ePHI, but OCR does not prescribe a method. NIST SP 800-66 Rev. 2, Section 3, offers a seven-step method that entities may use or replace with their own.

Is NIST SP 800-66 Rev. 2 mandatory?

No. It is guidance. The document states that it does not modify HIPAA or the HITECH Act and that using it does not ensure compliance with the Security Rule. Its key activities and crosswalks are aids to meeting the rule's standards.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Do business associates have to comply with the Security Rule directly?

Yes. Section 164.306(a) applies to covered entities and business associates, and a business associate is liable for its own violations. Covered entities must also obtain written satisfactory assurances through contracts that meet section 164.314(a).

Has the Security Rule been changed since 2013?

Not yet. HHS proposed changes on 6 January 2025 (90 FR 898), including removing the distinction between Addressable and Required specifications, and comments closed on 7 March 2025. The federal Unified Agenda lists final action as a long-term item for July 2027, so the existing text applies.

License included / downloadable: Yes The Security Rule is a U.S. federal regulation published in the Code of Federal Regulations, and NIST SP 800-66 Rev. 2 is a free NIST publication. Both are available without charge from HHS, the eCFR and NIST.

Full framework page and mappings: smartsuite.com/frameworks/hipaa-security-rule-nist-sp-800-66-rev-2

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.