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

HIPAA Security Rule, guided by NIST SP 800-66 Rev. 2, requires safeguards to protect electronic protected health information.

What it is

The HIPAA Security Rule, supported by guidance in NIST SP 800-66 Rev. 2, is a federal regulation and best practice framework that helps organizations safeguard electronic protected health information (ePHI) through the implementation of administrative, physical, and technical security controls. Its core objective is to ensure the confidentiality, integrity, and availability of health data processed by covered entities and their business associates.

Published by the U.S. Department of Health and Human Services (HHS), with NIST providing technical guidance, this rule applies to healthcare providers, health plans, and business associates handling ePHI. The framework addresses key areas such as access control, security risk analysis, workforce training, incident response, and ongoing monitoring to support regulatory compliance and effective risk management in the healthcare sector.

At a glance

PUBLISHER U.S. Department of Health and Human Services (HHS)	TYPE Regulation	VERSION HIPAA Security Rule / NIST SP 800-66 Rev. 2
EFFECTIVE April 21, 2003	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	INDUSTRY Healthcare & Life Sciences	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

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

Why it matters

- **Strengthen data protection practices** Safeguard the confidentiality and integrity of electronic protected health information against unauthorized access and breaches.
- **Enhance regulatory alignment** Enable healthcare organizations and their business associates to systematically meet mandatory federal requirements for data security.
- **Increase audit readiness** Foster continuous improvement and documentation of policies to support internal and external auditing with confidence.
- **Promote operational resilience** Improve recovery processes, business continuity, and ongoing monitoring to reduce the impact of security incidents on healthcare operations.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

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

ePHI Scope and System Inventory

Define where ePHI is stored and transmitted, with clear boundaries and owners.

Safeguard Library and Ownership

Track administrative, physical, and technical safeguards with owners and procedures.

HIPAA Risk Analysis and Mitigation

Run HIPAA risk analysis, track mitigation plans, and document risk decisions.

Evidence and Audit Trail

Centralize policies, training, access controls, and monitoring evidence per safeguard.

BA Agreements and ePHI Vendor Monitoring

Manage BA agreements, due diligence, and ongoing monitoring for ePHI vendors.

Audit and Compliance Reporting

Report safeguard status, open gaps, and readiness across systems and teams.

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

HIPAA Security Rule Guide

Provides official guidance on implementing the HIPAA Security Rule to protect electronic health information.

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

NIST SP 800-66 Revision 2

Outlines security practices for healthcare to support HIPAA compliance.

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

Frequently asked questions

What is the HIPAA Security Rule used for?

The HIPAA Security Rule is designed to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). It establishes federal requirements for safeguarding health data processed by covered entities and their business associates in the healthcare sector.

Is compliance with the HIPAA Security Rule mandatory?

Yes, compliance with the HIPAA Security Rule is mandatory for all covered entities and business associates that create, receive, maintain, or transmit ePHI. Non-compliance may result in both civil and criminal penalties enforced by the U.S. Department of Health and Human Services (HHS).

Who must comply with the HIPAA Security Rule?

The HIPAA Security Rule applies to healthcare providers, health plans, healthcare clearinghouses (collectively, "covered entities"), and their business associates that handle ePHI. This includes any organization that processes or stores ePHI on behalf of covered entities.

What are the key safeguards required by the HIPAA Security Rule?

The HIPAA Security Rule requires organizations to implement administrative, physical, and technical safeguards. These include conducting risk assessments, managing workforce security, controlling access to ePHI, protecting against unauthorized disclosures, and ensuring ongoing evaluation of security measures.

How do organizations implement the HIPAA Security Rule using NIST SP 800-66 Rev. 2?

Organizations use NIST SP 800-66 Rev. 2 as technical guidance to map HIPAA Security Rule requirements to practical security controls and risk management practices. Implementation typically involves risk analysis, selecting required and addressable controls, documenting policies, training staff, and maintaining evidence of compliance activities.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does the HIPAA Security Rule relate to other security frameworks?

The HIPAA Security Rule aligns with broader cybersecurity and privacy standards, such as NIST Cybersecurity Framework or ISO 27001, but focuses specifically on ePHI. NIST SP 800-66 Rev. 2 helps organizations bridge HIPAA requirements with recognized information security best practices for the healthcare sector.

What are ongoing compliance requirements for the HIPAA Security Rule?

Maintaining HIPAA Security Rule compliance requires periodic risk assessments, regular review of security controls, continuous policy updates, ongoing workforce training, incident response planning, and robust documentation. Organizations should monitor and update their safeguards to address emerging threats and regulatory updates.

How would SmartSuite support HIPAA Security Rule (with NIST SP 800-66 Rev. 2 Guidance)?

SmartSuite can help organizations manage HIPAA Security Rule compliance by centralizing the tracking of risks, maintaining a library of control requirements, supporting evidence collection, and streamlining audit preparation. The platform enables ongoing monitoring, remediation workflow management, and comprehensive reporting to demonstrate and sustain alignment with HIPAA and NIST SP 800-66 Rev. 2 best practices.

License included / downloadable: Yes The HIPAA Security Rule and NIST SP 800-66 guidance are publicly available through HHS and NIST publications.

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

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.