

HIPAA (45 CFR Parts 160 & 164) — 2013 Omnibus Rule

HIPAA Omnibus Rule strengthens privacy, security, and breach notification requirements and extends protections to business associates handling health information.



What it is

The U.S. HIPAA Administrative Simplification (2013 Omnibus Rule) is a regulatory framework that establishes national standards for the privacy, security, and electronic exchange of protected health information (PHI) within the healthcare sector. Its primary goal is to safeguard patient data while supporting the efficient flow of health information for care delivery and payment operations.

Published by the U.S. Department of Health and Human Services (HHS), the rule applies to covered entities such as healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates. It covers critical areas including data protection, privacy governance, cybersecurity safeguards, breach notification, and the standardization of healthcare transactions.

At a glance

PUBLISHER U.S. Department of Health and Human Services (HHS)	TYPE Regulation	VERSION 2013
EFFECTIVE September 23, 2013	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION United States	INDUSTRY Healthcare & Life Sciences	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html>

Why it matters

- **Strengthen data protection practices** Support robust safeguards to reduce unauthorized access, loss, or disclosure of protected health information across all systems.
- **Enhance regulatory compliance alignment** Enable organizations to meet federal health information privacy and security requirements, reducing exposure to legal penalties and enforcement actions.
- **Support organizational accountability** Clarify roles and responsibilities for healthcare data handling, fostering transparency and security-focused operational cultures.
- **Improve incident response capabilities** Require breach notification and risk assessment procedures, enhancing detection, management, and reporting of health data incidents.

How SmartSuite supports HIPAA

HIPAA Security and Privacy Control Library

Structure administrative, technical, and physical safeguards required under HIPAA Security and Privacy Rules.

PHI Risk Assessments and Safeguard Tracking

Track risk analyses, mitigation plans, and safeguards protecting electronic protected health information (ePHI).

Access Controls and Authentication Governance

Manage user access, workforce permissions, and authentication controls protecting PHI systems and data.

HIPAA Incident and Breach Management

Track potential HIPAA incidents, breach investigations, and response activities across healthcare systems.

Vendor and Business Associate Oversight

Monitor business associate agreements, vendor security reviews, and third-party compliance obligations.

Compliance Reporting and Audit Readiness

Provide dashboards showing safeguard implementation status, risk posture, and readiness for regulatory audits.

Common framework mappings

CIS Controls v8.1

COBIT 2019

GLBA Safeguards Rule (16 CFR Part 314)

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

SWIFT CSCF

Official resources

HIPAA Administrative Simplification Statute and Rules

Provides official text and explanation for HIPAA's administrative simplification provisions.
hhs.gov/hipaa/for-professionals/special-topics/hipaa-administrative-simplification-statute-and-rules/index.html

HIPAA Security Rule Guidance Material

Outlines detailed guidance on the HIPAA Security Rule standards and implementation specifications.
hhs.gov/hipaa/for-professionals/security/guidance/index.html

Summary of the HIPAA Privacy Rule

Provides an overview of the HIPAA Privacy Rule, outlining key provisions and requirements.
hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Frequently asked questions

What is the HIPAA Administrative Simplification Rule used for?

The HIPAA Administrative Simplification Rule sets standards to protect the privacy and security of health information while standardizing electronic healthcare transactions. It aims to reduce costs and administrative burdens for healthcare providers, health plans, and clearinghouses (covered entities).

Is HIPAA compliance mandatory for healthcare organizations?

Yes, HIPAA compliance is mandatory for all covered entities and their business associates that handle protected health information (PHI) in the United States. Non-compliance can result in significant civil and criminal penalties.

What is the scope of HIPAA Administrative Simplification?

HIPAA Administrative Simplification applies to healthcare providers, health plans, and clearinghouses that transmit health information electronically. It covers both the privacy and security of PHI and mandates national standards for electronic transactions and code sets.

What are the key requirements of the HIPAA Privacy and Security Rules?

The HIPAA Privacy Rule governs the permissible uses and disclosures of PHI, while the Security Rule establishes safeguards for electronic PHI (ePHI), including administrative, physical, and technical controls. Organizations must implement policies, procedures, training, and documentation to meet these requirements.

How do organizations implement HIPAA controls?

Organizations implement HIPAA controls by conducting risk assessments, developing and enforcing policies and procedures, training workforce members, and applying technical safeguards such as encryption and access controls. Regular monitoring and audits are necessary to ensure ongoing compliance.

How does HIPAA relate to other regulatory frameworks?

HIPAA often overlaps with other healthcare regulations such as HITECH and state privacy laws. While HIPAA establishes federal standards, organizations must also consider applicable state laws and broader security frameworks like NIST when designing their compliance programs.

What are the ongoing compliance requirements under HIPAA?

Ongoing HIPAA compliance requires regular risk assessments, periodic review and updates to policies and procedures, continuous workforce training, incident response planning, and maintaining evidence of compliance activities. Organizations must be prepared for audits and reporting breaches as required by law.

How would SmartSuite support HIPAA Administrative Simplification?

SmartSuite can support HIPAA Administrative Simplification by centralizing risk tracking, managing compliance controls, facilitating evidence collection, and preparing for audits. Its platform streamlines policy management, automates compliance workflows, and generates detailed reports to demonstrate and maintain HIPAA compliance.

License included / downloadable: Yes The HIPAA Omnibus Rule is published by HHS and is publicly available through HHS and the Federal Register. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/hipaa-omnibus-rule-2013