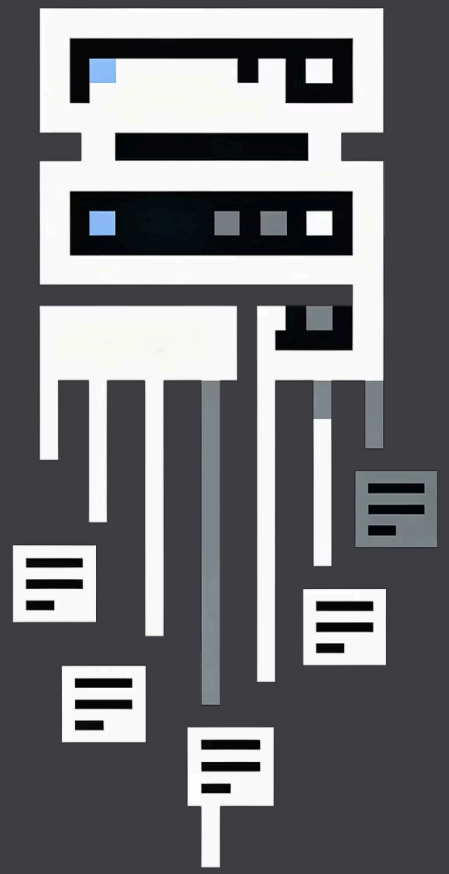
ControlSage

The Complete Guide to HIPAA Compliance

A comprehensive resource for healthcare organizations and compliance teams navigating the evolving landscape of patient data protection.



133M

1 in 3 Americans Had Their Health Data Breached in 2023

Record-Breaking Exposure

Over **133 million records** were exposed in healthcare breaches in 2023 — a historic high that shows no sign of slowing.

Ransomware Dominates

Ransomware and hacking now account for **79% of all large HIPAA breaches**, with cyberattacks escalating exponentially year over year.

2025 Rule Overhaul

HHS proposed sweeping Security Rule updates in December 2024 — the **first overhaul since 2013** — to address the growing threat landscape.

What Is HIPAA — and Who Must Comply?

HIPAA establishes national standards for protecting sensitive patient health information. Compliance is mandatory for two categories of organizations:

Three Core Rules govern compliance: the Privacy Rule, Security Rule, and Breach Notification Rule.

Covered Entities

Health plans, healthcare clearinghouses, and most healthcare providers who transmit health information electronically.

Business Associates

Any vendor or partner that creates, receives, maintains, or transmits PHI on behalf of a covered entity — including cloud providers and IT vendors.

CHAPTER 1

The Privacy Rule

Understanding what counts as protected health information — and how patients retain control over it.

Protected Health Information (PHI): What Counts?

What Qualifies as PHI?

PHI is any **individually identifiable health information** — past, present, or future — held by a covered entity. It spans all formats:

- Paper, electronic (ePHI), and verbal communications
- **18 identifiers** must be removed to achieve de-identification: names, dates, phone numbers, SSNs, geographic data, and more

Minimum Necessary Standard: Only access or share the minimum PHI required for the specific task at hand. Over-disclosure is a violation.

Patient Rights Under the Privacy Rule

1

Right to Access

Patients may access and obtain copies of their health records. Covered entities must respond **within 30 days**.

2

Right to Correct

Patients may request corrections to inaccurate or incomplete PHI held by covered entities.

3

Right to Accounting

Patients may request a full accounting of disclosures and restrict certain uses of their health information.

4

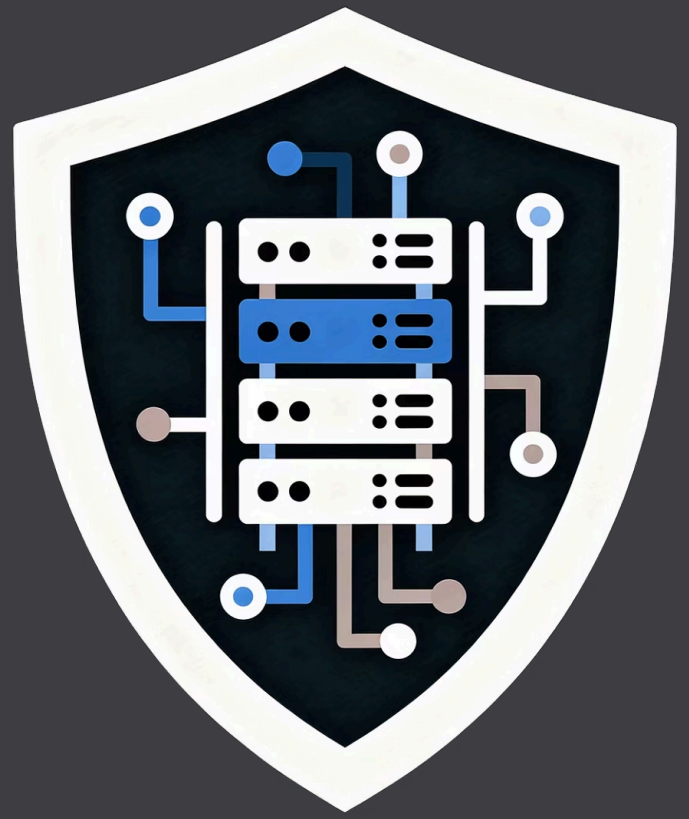
Notice of Privacy Practices

Covered entities must provide a written **NPP** at first patient contact — explaining all rights and how PHI is used.

CHAPTER 2

The Security Rule

Administrative, physical, and technical safeguards that protect electronic protected health information.



Three Pillars of the Security Rule

Administrative Safeguards

- Designate a Security Officer
- Workforce training programs
- Access management policies
- Contingency and continuity planning

Physical Safeguards

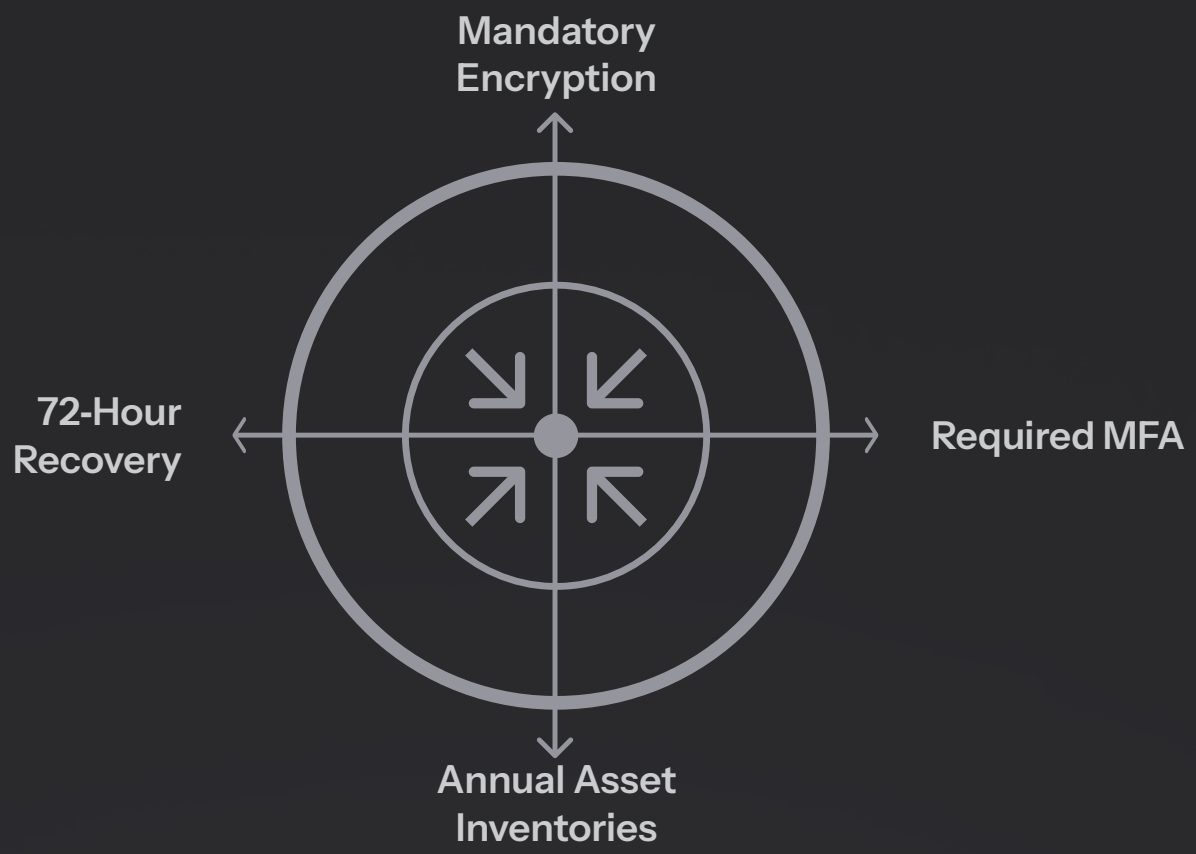
- Facility access controls
- Workstation security protocols
- Device and media disposal procedures
- Visitor access logs

Technical Safeguards

- Access controls and user authentication
- Audit logs for ePHI access
- Encryption of ePHI in transit and at rest
- Automatic logoff mechanisms

2025 Security Rule Updates: What's Changing

FIRST OVERHAUL SINCE 2013



Published December 27, 2024, HHS's proposed rule requires covered entities and business associates to materially strengthen cybersecurity protections — closing longstanding loopholes that left ePHI vulnerable.

CHAPTER 3

Risk Assessments & BAAs

Identifying vulnerabilities and formalizing third-party obligations before a breach occurs.

Conducting a HIPAA Risk Assessment

A documented risk assessment is not optional — it is a **required foundation** of any HIPAA Security Rule compliance program. Assessments must be reviewed regularly and updated after significant operational changes.

Risk assessments must be **documented in writing** and available for OCR review during an investigation or audit.

Business Associate Agreements (BAAs)

When Required

A BAA must be executed **before sharing any PHI** with third-party vendors — including EHR vendors, billing companies, cloud providers, and IT support firms.

What It Must Include

The agreement must specify permitted uses of PHI, required safeguard standards, and breach reporting obligations and timelines.

Direct BA Liability

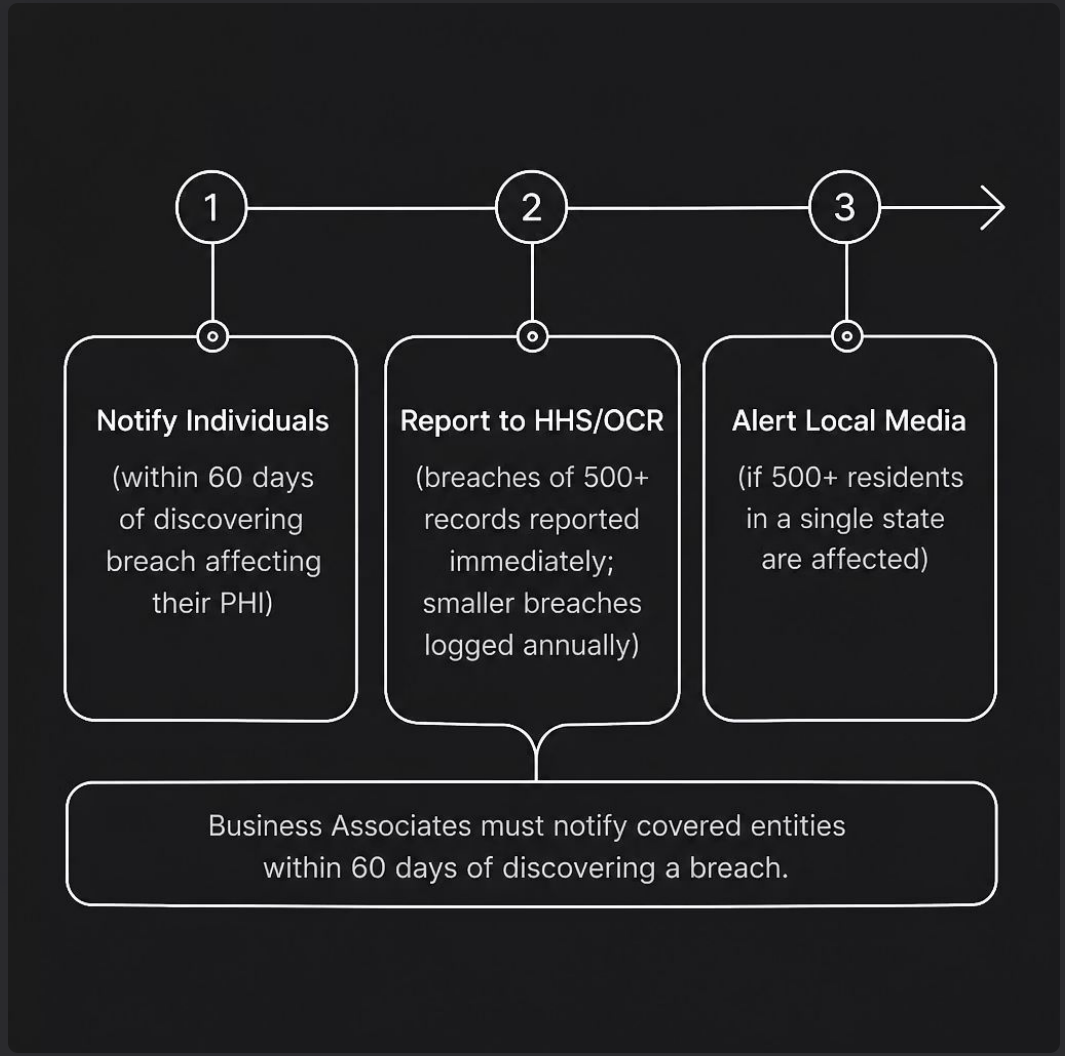
Business associates are **directly liable** under HIPAA — enforcement doesn't stop at the covered entity. Subcontractors of BAs must also sign BAAs.

CHAPTER 4

Breach Notification & Penalties

When a breach occurs, the clock starts immediately. Here's exactly what the law requires — and what non-compliance costs.

Breach Notification: The Clock Starts Immediately



Key Notification Rules

- **Individuals:** Notify within 60 days of discovering a breach affecting their PHI
- **HHS/OCR:** Breaches of 500+ records must be reported immediately; smaller breaches are logged in the annual summary
- **Media:** Notify prominent local media outlets if 500+ residents in a state are affected
- **Business Associates:** Must notify covered entities within 60 days of discovering a breach

⚠ Failure to notify on time is itself a separate HIPAA violation — compounding penalties significantly.

HIPAA Penalties: The Real Cost of Non-Compliance

$141

Minimum Per Violation

Unknowing violation — covered entity had no knowledge despite reasonable diligence.

$71K

Max Per Violation

Cap per individual unknowing violation. Annual limit reaches **$2.1M** per violation category.

$2.1M

Annual Willful Neglect Max

Willful neglect left uncorrected after 30 days: $68,928–$2,134,831 per violation.

10 yrs

Criminal Imprisonment

Up to 10 years imprisonment for intentional misuse or wrongful disclosure of PHI.

Penalty figures reflect the August 8, 2024 federal inflation-adjusted schedule published by HHS.

Build Your HIPAA Compliance Program Today

Six foundational actions every healthcare organization must complete. Start here — document everything.

01

Appoint a Privacy & Security Officer

Designate dedicated personnel accountable for Privacy Rule and Security Rule compliance across the organization.

02

Complete Your Annual Risk Assessment

Document all ePHI systems, identify threats and vulnerabilities, rate risk levels, and implement your risk management plan.

03

Audit Vendor Relationships & Execute BAAs

Map every third-party vendor touching PHI and ensure a signed BAA is in place before any data is shared.

04

Train All Workforce Members

Deliver documented training on Privacy and Security Rule requirements — and repeat it annually.

05

Implement Encryption, MFA & Audit Logging

Secure all ePHI systems with encryption in transit and at rest, multi-factor authentication, and comprehensive access logs.

06

Establish & Test Breach Response Procedures

Document your breach notification workflow, assign response roles, and conduct tabletop exercises to verify readiness.

Sources

- HIPAA Security Rule NPRM | HHS.gov
- Summary of the HIPAA Privacy Rule | HHS.gov
- Summary of the HIPAA Security Rule | HHS.gov
- HIPAA Penalties Effective August 8, 2024