CS-108 · Compliance & Frameworks

HIPAA

The U.S. law that governs the privacy and security of protected health information.

Executive Summary

HIPAA, the Health Insurance Portability and Accountability Act, is a U.S. federal law that sets national standards for protecting sensitive health information. Its rules are enforced by the U.S. Department of Health and Human Services (HHS). The Privacy Rule governs how protected health information can be used and disclosed, and the Security Rule sets requirements for safeguarding health information held or transmitted in electronic form.

What It Is

HIPAA is a set of U.S. regulations that protect the confidentiality and security of health information. It applies to covered entities, which generally include health plans, health care clearinghouses, and most health care providers that transmit health information electronically, as well as to their business associates, which are vendors that handle protected health information on their behalf. Protected health information, often abbreviated PHI, is individually identifiable health information, and when it is in electronic form it is referred to as ePHI. The two rules most relevant to security and compliance professionals are the Privacy Rule, which sets limits on how PHI may be used and shared, and the Security Rule, which requires administrative, physical, and technical safeguards for ePHI. The Breach Notification Rule requires notifying affected individuals and regulators after certain breaches.

Why It Matters

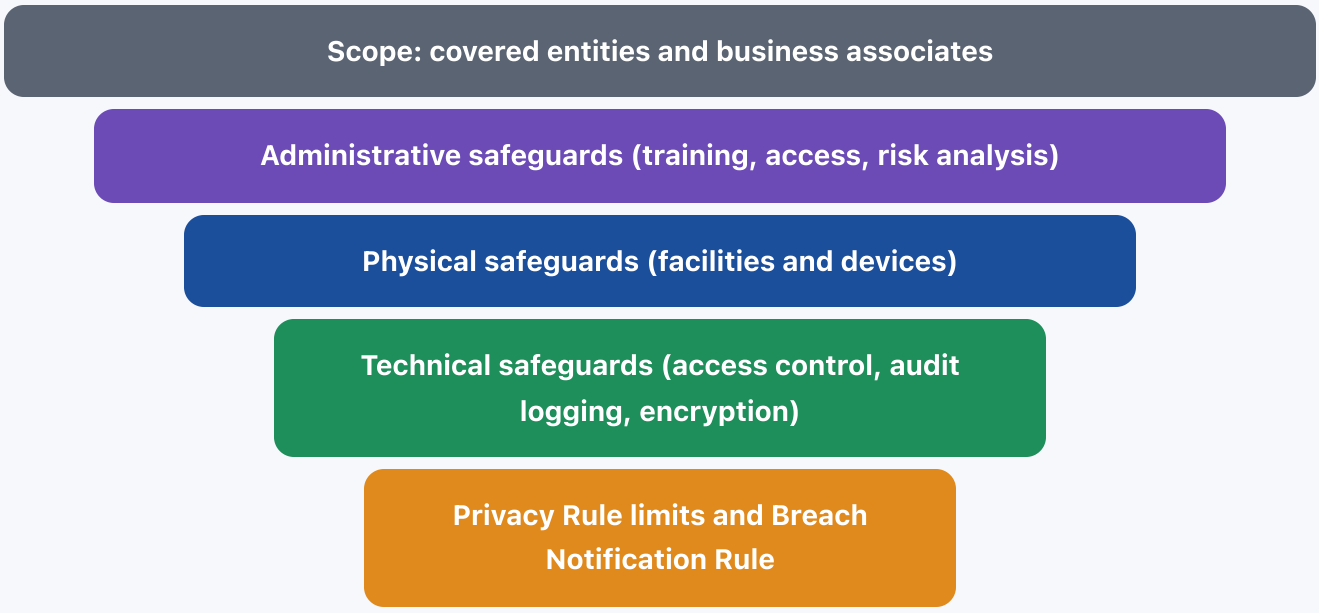
Health data is highly sensitive and highly targeted, and mishandling it carries legal, financial, and reputational consequences. HIPAA violations can lead to significant penalties and mandatory public reporting of large breaches, and business associate obligations mean the law reaches far beyond hospitals into technology vendors, billing companies, and cloud providers. For

organizations that touch health data, HIPAA compliance is a condition of doing business. For professionals, HIPAA expertise is in demand across health care, health technology, and any vendor in the health supply chain, and it pairs naturally with broader security and privacy skills.

How It Works

Compliance starts with determining whether an organization is a covered entity or a business associate and mapping where PHI and ePHI live and flow. The Security Rule is risk-based: organizations must perform a risk analysis, then apply administrative safeguards (such as workforce training and access management), physical safeguards (such as facility and device controls), and technical safeguards (such as access controls, audit logging, and protections for data in transit and at rest). The Privacy Rule constrains how PHI may be used and disclosed and grants individuals rights over their information. Business associate agreements bind vendors to protect the PHI they handle. When a reportable breach occurs, the Breach Notification Rule sets out who must be told and when. Because the environment changes, the risk analysis and safeguards must be reviewed and updated over time.

Architecture Diagram



HIPAA safeguards protect PHI through administrative, physical, and technical layers, bound together by agreements and breach notification.

Visual Workflow

Common Attacks

- Failing to perform or document a thorough risk analysis of ePHI
- Overlooking business associates so vendor handling of PHI is unmanaged
- Granting workforce access to PHI far beyond what each role requires
- Leaving ePHI unprotected on lost or stolen laptops and mobile devices
- Not having a breach response ready, delaying required notifications

Common Mistakes

- Assuming HIPAA applies only to hospitals and not to vendors that handle PHI
- Treating the risk analysis as a one-time document instead of a living process
- Confusing the Privacy Rule with the Security Rule and addressing only one
- Skipping business associate agreements or using ones that are never enforced
- Neglecting audit logging, which is needed to detect and investigate misuse

Best Practices

- Conduct and regularly update a documented risk analysis of ePHI

- Apply least-privilege access and log access to PHI
- Encrypt ePHI on devices and in transit where reasonable and appropriate
- Sign and maintain business associate agreements with every relevant vendor
- Train the workforce on privacy and security and make breach reporting easy
- Keep an incident and breach notification plan ready and tested

Quick Checklist

- [x] Organization's role as covered entity or business associate is determined
- [x] PHI and ePHI data flows are mapped
- [x] A current, documented risk analysis exists
- [x] Administrative, physical, and technical safeguards are in place
- [x] Business associate agreements cover every vendor that handles PHI
- [x] Breach notification plan is documented and workforce training is current

Recommended Tools

GRC platform
Tracks HIPAA safeguards, risk analysis, and evidence

Access management and audit logging
Enforces least privilege and records who touched PHI

Encryption tools
Protects ePHI on devices and in transit

Vendor and BAA management system
Tracks business associates and their agreements

Industry Standards

HIPAA Security Rule
Requires administrative, physical, and technical safeguards for ePHI

HIPAA Privacy Rule
Governs permitted uses and disclosures of PHI and individual rights

NIST guidance on securing health information
Widely referenced help for implementing the Security Rule

Career Relevance

HIPAA is a core competency for GRC analysts, compliance analysts, security auditors, and CISOs in health care and health technology, who run risk analyses, implement safeguards, manage business associate agreements, and prepare for audits. Privacy officers and vendor risk teams also rely on it. For the privacy and AI governance professionals AI-Governance-Jobs.com serves, HIPAA is a leading example of how sensitive data is regulated and a template for governing health-related AI systems responsibly.

Interview Questions

- Who must comply with HIPAA, and what is the difference between a covered entity and a business associate?
- Explain the difference between the Privacy Rule and the Security Rule.
- What are the three categories of safeguards in the Security Rule?
- Why is the risk analysis so central to HIPAA compliance?
- What triggers obligations under the Breach Notification Rule?

Related Certifications

ISC2 HCISPP | ISACA CISA | Certified in Healthcare Privacy and Security (CHPS)

Further Reading

- HHS: HIPAA for Professionals
- HHS: HIPAA Security Rule
- HHS: Breach Notification Rule

Key Takeaways

- HIPAA is the U.S. law protecting the privacy and security of health information, enforced by HHS.
- It applies to covered entities and to business associates that handle PHI on their behalf.
- The Privacy Rule governs use and disclosure of PHI; the Security Rule protects ePHI.
- The Security Rule is risk-based and requires administrative, physical, and technical safeguards.
- HIPAA expertise is in demand across health care and the broader health technology supply chain.

FAQ

Does HIPAA apply to technology vendors?

What is the difference between PHI and ePHI?

Is there a HIPAA certification for organizations?

Related Careers

RELATED ROLES

Grc Analyst | Compliance Analyst | Security Auditor | Ciso

RELATED CERTIFICATIONS

ISC2 HCISPP | ISACA CISA | Certified in Healthcare Privacy and Security (CHPS)

CURRENT OPENINGS

Live roles are on the job board.

GUIDES & SALARY

Browse all jobs

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **HIPAA**
3. Go deeper: GDPR
4. Go deeper: PCI DSS
5. Validate it: work toward **ISC2 HCISPP**
6. Find the role: browse current openings

RELATED SHEETS

CS-110 GDPR | CS-109 PCI DSS | CS-001 Cybersecurity | CS-085 Risk Ratings | CS-009 Core Security Principles