HIPAA Compliance Rules Overview

Never have a false sense of security.™

An overview of HIPAA Rules and how to begin working toward compliance for covered entities and business associates.
What is HIPAA Compliance?

The Health Insurance Portability and Accountability Act (HIPAA) is a regulation that includes privacy, security, breach notification, and enforcement rules to protect patient healthcare information.

HIPAA Privacy, Security, and Breach rules require covered entities and business associates to:

- Implement policies to secure data
- Ensure compliance accountability (e.g., Risk Analysis)
- Limit access to Protected Health Information (PHI)
- Conduct workforce training
- Safeguard how organizations create, receive, maintain, and transmit PHI

These rules provide additional guidance and authority for the Office of Civil Rights (OCR) to enforce HIPAA compliance through audits and financial penalties. The penalties outlined below are per day and per violation. This means that if you have multiple offenses, you could get fined up to $50,000 per day for each violation until you resolve the violation.

<table>
<thead>
<tr>
<th>VIOLATION CATEGORY</th>
<th>PENALTY</th>
<th>MAXIMUM PER CALENDAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Did not know</td>
<td>$100-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) Reasonable cause</td>
<td>$1,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C)(i) Willful neglect - Corrected</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C)(ii) Willful neglect - Not corrected</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Covered Entities and Business Associates

Two groups must comply with HIPAA Rules—covered entities and business associates.

Covered Entity
A covered entity is a health plan, health care clearinghouse, or health care provider who electronically transmits any health information in connection with a covered transaction, including:

- Healthcare providers
  - Doctors
  - Clinics
  - Psychologists
  - Dentists
  - Chiropractors
  - Nursing homes
  - Pharmacies
- Health insurance companies
- Health maintenance organizations (HMO)
- Company health plans
- Government programs that pay for healthcare
  - Medicare
  - Medicaid
  - Military healthcare programs
  - Veteran healthcare programs

This list also includes the entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content) or vice versa.

Business Associate
A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to a covered entity. Examples of business associates that typically work with PHI are:

- CPA
- Attorney
- IT providers
- Billing and coding services
- Laboratories
- Claims processing or administration
HIPAA Privacy Rule

The HIPAA Privacy Rule provides federal protections for an individual’s protected health information and gives patients various rights concerning their information. The Privacy Rule permits the disclosure of protected health information needed for patient care and other essential purposes.

The HIPAA Privacy Rule spells out administrative responsibilities, discusses written agreements between covered entities and business associates, outlines the need and implementation of privacy policies and procedures, and describes employer responsibilities to train workforce members and implement requirements regarding their use and disclosure of PHI.

The Privacy Rule applies to all healthcare providers, including those who do not use an electronic health record (EHR) system, and includes all electronic, paper, and oral mediums. This rule gives patients rights to their protected health information, access to records, and disclosure on how that information is used or shared.

HIPAA Security Rule

The HIPAA Security Rule requires covered entities, business associates, and their subcontractors to implement safeguards to protect electronic protected health information (ePHI) that is created, received, transmitted, or maintained. It specifies a series of administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

Most violations of the HIPAA Security Rule result from businesses needing to follow policies and procedures to safeguard ePHI. The HIPAA Security Rule:

- Establishes a national set of security standards for ePHI
- Protects health information held or transmitted in electronic form
- Requires administrative, physical, and technical safeguards to secure ePHI
- Supports the Privacy Rule requirement to reasonably safeguard PHI in all forms

HIPAA Breach Notification Rule

The Breach Notification Rule requires covered entities, business associates, and their subcontractors to provide notification following a breach to affected individuals, the Secretary of Health and Human Services (HHS), and the media (if a breach affects more than 500 residents of a State or jurisdiction).

The Breach Notification Rule consists of protocols a business must undertake in the event of data compromise. It includes elements such as:

- What constitutes a breach
- Necessary parties to be notified
- Notification timelines
- Notification methods
- Notification content
- Remediation plan
The Pathway to HIPAA Compliance

The HIPAA Security Rule is often a stumbling block for organizations as it is more technical and requires a trained security professional. Below are products and services SecurityMetrics provides for businesses to work towards HIPAA compliance and increased data security.

1. Risk Analysis
A risk assessment is a foundational onsite assessment that looks at threat sources and vulnerabilities while providing risk determination. A risk assessment can help you understand the likelihood of a breach and the magnitude of threat events, fulfill compliance requirements, and identify threats and vulnerabilities. This assessment is perfect for enterprise merchants and organizations that are required to meet HIPAA compliance requirements.

2. HIPAA Compliance Assessment
A HIPAA compliance assessment offers you an assessor’s degree of assurance that you are meeting your responsibilities with regards to HIPAA compliance under the Privacy, Security, and Breach rules. This assessment is for covered entities and business associates that have HIPAA compliance requirements. A HIPAA assessment can improve your PHI security workflows and provides a final HIPAA compliance report.

3. HIPAA Consulting
HIPAA consulting is perfect for SMB and Enterprise merchants who need to comply with industry mandates but aren’t sure where to begin. Your HIPAA consulting will give you professional guidance on essential cybersecurity and compliance measures. You will also be able to secure your business networks and achieve data security goals.
Additional HIPAA Products

SecurityMetrics offers additional HIPAA products so you can get all the services you need to continue on your path to compliance.

Penetration Testing
Penetration testing is ethical hacking that examines networks, applications, segmentation, and wireless infrastructure for vulnerabilities through the lens of an attacker. A penetration test can help you find the root cause of business vulnerabilities, provide a report for remediation of discovered vulnerabilities, and help achieve compliance with security mandates.

Vulnerability Scanning
An external vulnerability scan is an automated, external network scan that looks for business network and web application weaknesses. This scan is ideal for anyone looking to increase their security posture and can help you identify thousands of risks, meeting compliance requirements.

An internal vulnerability scan is an automated, internal network scan for vulnerabilities that leave businesses open to compromise. SecurityMetrics helps its customers achieve external network security by keeping up with the most current list of vulnerabilities, finely tuning its scan engines to expose weaknesses, and providing extensive support and remediation assistance.

HIPAA Policies and Procedures
HIPAA policies and procedures are customizable HIPAA security policy templates that serve as the blueprint of your organization’s compliance plan. Having up-to-date and accurate policies and procedures helps protect patient data and is a must for complying with HIPAA rules.

HIPAA Workforce Training
HIPAA Workforce training is an online training module that reviews HIPAA Privacy, HIPAA Security, and HIPAA Breach Notification Rules so your employees can be your first defense against threats. HIPAA training is an important part of compliance and necessary for all who deal with patient health information. Managing and training staff on how to protect PHI is easy with this training console that allows you to track employees’ training status, due dates, and courses they have completed.

RESOURCES
- How To Prepare For a HIPAA Audit in Three Steps [Blog]
- Onsite HIPAA Audit [Data Sheet]
- How to Prepare for a HIPAA Audit [Webinar]
- How to Prepare for an Audit [Podcast]