# HIPAA Compliance Requirement

## What is HIPAA Compliance?

Any medical information that can be connected to a specific patient is considered "protected healthcare information" (PHI) and is covered by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA compliance requires a serious approach to protecting data. HIPAA compliance is critical for organizations that handle healthcare data, not only to protect patient privacy but also to prevent the bottom line. Data breaches must be reported and HIPAA non-compliance can result in hefty fines. Any organizations handling healthcare data must be HIPAA compliant. HIPAA has rules that require organizations to protect patient privacy and secure patient data. The rules include:

## 01. HIPAA Privacy Rule

Individually identifiable health information is covered by the HIPAA Privacy Rule. This data includes information about a patient's mental or physical health, medical treatments, or payment history. This rule requires organizations to protect data "in any form or media, whether electronic, paper, or oral" when it contains personal information such as name, phone number, birth date, Social Security Number, or any other personal identifier.

The HIPAA Privacy Rule governs how organizations can use patient data, what data they can disclose without the patient's permission, and to whom. The rule also guarantees patients the "Right to Access" most of their personal health information and obtain copies of their medical records. Organizations handling PHI must create and apply written privacy policies and they must notify patients (in writing) about these policies. They also must provide annual HIPAA training for their staff.

## 02. HIPAA Security Rule

The HIPAA Security Rule is a subset of the HIPAA Privacy Rule. The Security Rule tells organizations how to secure the PHI they handle. Specifically, it provides standards protecting electronically protected health information (ePHI). The Security Rule explains how that data should be handled, maintained, and transmitted.

To comply with the Security Rule, organizations must have administrative, physical, and technical safeguards in place.

## 03. HIPAA Omnibus Rule

The Omnibus Rule defines the role of business associates and outlines the criteria for Business Associate Agreements (BAAs).

The Omnibus Rule adds provisions required by the Health Information Technology for Economic and Clinical Health (HITECH) Act to HIPAA obligations. The HITECH Act incentivizes the use of electronic health records (EHR). It also increased security and privacy protection requirements and the legal and financial liability for non-compliant organizations.

## 04. Breach Notification Rule

The Breach Notification Rule requires organizations to notify the U.S. Department of Health and Human Services (HHS) Office for Civil Right (OCR) when a data breach of ePHI has occurred. A data breach is defined by HHS as "an impermissible use or disclosure of under the Privacy Rule that compromises the security or privacy of the protected health information." The Breach Notification Rule profiles which types of breaches must be reported and how.

Breaches are categorized as "minor breaches" (those affecting fewer than 500 people) and "meaningful breaches" (those affecting more than 500 individuals). HIPAA requires organizations to report both minor and meaningful breaches to OCR, however they have different reporting procedures. All meaningful breaches are published on OCR's Breach Notification Portal, or "Wall of Shame" for the public to review.

## 05. HIPAA Enforcement Rule

The Enforcement Rule empowers OCR to:

- investigate HIPAA complaints
- conduct compliance reviews
- perform education and outreach
- levy fines of up to $1.5 million.

In 2020, OCR fined 13 organizations for HIPAA violations, for a total of over $13.5 million. OCR also works with the Department of Justice to refer possible criminal violations of HIPAA.

## How to Become HIPAA Compliant

Organizations must not only follow the HIPAA security and privacy rules, they must document that they have been proactive about doing so. HIPAA legislation is complicated and ever-changing, so it is important to stay current with changes to this legislation.

Step 1.

### Name a HIPAA Privacy Officer and Security Officer

Organizations must assign a Privacy Compliance Officer responsible for the development, implementation, and annual updating of privacy policies. HHS recommends that larger organizations also form a Privacy Oversight Committee for policy guidance and enforcement. The Privacy Officer and Oversight Committee members are required to complete regular training to stay up-to-date on any changes to HIPAA regulations. The Privacy Officer is also responsible for maintaining Notice of Privacy Practices forms (see NPPs in Step 2), managing and updating Business Associate Agreements (see BAAs in Step 5), scheduling trainings and self-audits, and otherwise ensuring that the organization is compliant with the HIPAA Privacy Rule. Organizations must also have a HIPAA Security Officer who makes sure there are policies and procedures in place to protect, detect, and respond to ePHI data breaches. The Security Officer establishes precautions as required by the Security Rule and performs risk assessments to evaluate their effectiveness.

Step 2.

### Create Privacy and Security Policies

Organizations must assign a Privacy Compliance Officer responsible for the development, implementation, and annual updating of privacy policies. HHS recommends that larger organizations also form a Privacy Oversight Committee for policy guidance and enforcement. The Privacy Officer and Oversight Committee members are required to complete regular training to stay up-to-date on any changes to HIPAA regulations. The Privacy Officer is also responsible for maintaining Notice of Privacy Practices forms (see NPPs in Step 2), managing and updating Business Associate Agreements (see BAAs in Step 5), scheduling trainings and self-audits, and otherwise ensuring that the organization is compliant with the HIPAA Privacy Rule. Organizations must also have a HIPAA Security Officer who makes sure there are policies and procedures in place to prevent, detect, and respond to ePHI data breaches. The Security Officer establishes precautions as required by the Security Rule and performs risk assessments to evaluate their effectiveness.

Step 3.

### Implement Security Safeguards

The Security Rule requires three types of safeguards be in place to secure ePHI — including:

**Administrative safeguard requirements:**

1. Documented security management processes
2. Signated security personnel
3. An information access management system
4. Workforce security training
5. Periodic assessments of all security protocols

**Physical safeguard requirements:**

1. control who has access to physical facilities where ePHI is stored
2. secure all workstations and devices that store or transmit ePHI

**Technical safeguard requirements:**

1. Access controls to secure ePHI in the EHR and other databases
2. ePHI data must be encrypted when it is at rest and during transit
3. Audit controls for all hardware and software that manages or transmits ePHI to meet HIPAA network requirements
4. Integrity controls to ensure ePHI is not improperly edited or deleted

For additional HIPAA compliance information, HHS provides guidance materials, checklists, and risk assessments tools.

Step 4.

### Regular Risk Assessments and Self-Audits

Being HIPAA compliant is a continuous process. Regulations require organizations conduct regular audits of all administrative, technical, and physical safeguards to identify compliance gaps. Organizations are also required to have written remediation plans that clearly explain how they plan to reverse HIPAA violations and when remediation will happen. At minimum, annual audit and risk assessments are required for every safeguard and business associate agreements.

Step 5.

### Business Associate Agreements

HIPAA applies to healthcare providers and their business associates. Healthcare providers and other organizations handling PHI must obtain "satisfactory assurances" that any business associates handling PHI are HIPAA-compliant and can effectively safeguard the data. They must enter a Business Associate Agreement (BAA). These BAAs must be annually reviewed and updated to accurately include any changes in the nature of the business associate relationship.

Step 6.

### Determine and Maintain a Breach Notification Protocol

Violating HIPAA doesn't always result in a fine, particularly if the organization can prove that the breach was unintentional and that they were proactive to do everything they could to prevent the breach. However, failing to report a breach is more likely to result in censure. HIPAA requires organizations to have a documented breach notification process that outlines how the organization will comply with the HIPAA Breach Notification Rule. All organizations and their business associates handling PHI must report all breaches to OCR and to inform any patients whose personal data may have been compromised.

Step 7.

### Document, Document, Document

Documenting all HIPAA compliance efforts is a key requirement. Be sure to document all privacy and security policies, all security safeguards, risk assessments and audits, remediation plans, staff training, and any security incidents that occur. All documentation will be reviewed by OCR during HIPAA audits and complaint investigations.

Showing that the organization has done its due diligence to comply with HIPAA requirements can make the difference between whether the organization is censured and fined or not.

## How can Microsec.ai assists with HIPAA compliance?

Organizations using public cloud infrastructure to host applications handling PHI can use Microsec.ai to comply with the HIPAA Security Rule Administrative and Technical Safeguard requirements to document, manage, audit, and enforce security for cloud-native applications and data in public cloud environments.

- Monitoring that ePHI data is encrypted
- Detecting and removing public exposure of ePHI
- Auditing changes to ePHI
- Continuous monitoring of network connections and traffic inside cloud native applications
- Continuous monitoring and assessments of cloud security posture with risk assessments
- Detecting and controlling access to ePHI in cloud storage and databases
- Discovering, monitoring, and protecting, ePHI in cloud storage, databases, volumes, and ePHI data movement within cloud environments
- Controlling network connections, communications, and movement of ePHI between microservices and workloads
- Auditing user and account activity to detect problematic changes in security posture including misconfigurations, new software vulnerabilities, unauthorized access, abnormal user or account activity

## About Microsec.ai

Get easy-to-deploy, runtime visibility, protection, and compliance monitoring for cloud serverless, VM, and Kubernetes environments. Microsec.ai is the only agentless, data-centric, runtime cloud-native application protection platform (CNAPP) that protects your data and applications with data loss prevention (DLP), east-west network traffic control with self-healing micro segmentation, security posture management, and compliance analysis in one unified solution.


If you have any questions, contact us at
sales@microsec.ai