

Security always matters.



→ HIPAA and why security always matters

As part of the Health Insurance Portability and Accountability Act (HIPAA), the Privacy Rule assures that individuals' health information is properly protected, while allowing the flow of health information needed to provide high-quality healthcare and protect the public's health and well-being. Knowing the latest regulations and mandates and how they may impact you will help keep you safe.

The Privacy Rule applies to more than just healthcare providers.

The Privacy Rule applies to any healthcare provider (the covered entity) or business associate who transmits health information in electronic form in connection with transactions for which the U.S. Secretary of Health and Human Services (HHS) has adopted standards under HIPAA.

The term "HIPAA compliance" refers to adhering to HIPAA Title II.

Also known as the Administrative Simplification provisions, Title II includes the following HIPAA compliance requirements: National Provider Identifier Standard, Transactions and Code Sets Standard, HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Enforcement Rule.

HIPAA requires notification of patients after a data breach.

The HIPAA Breach Notification Rule requires covered entities and any affected business associates to notify promptly following a data breach of unsecured protected health information.

The HIPAA Privacy Rule protects any transmitted information.

The HIPAA Privacy Rule protects all individually identifiable health information that is held or transmitted by a covered entity or a business associate. This information can be held in any form, including digital, paper, and oral.

Employees, volunteers, and trainees must be trained on HIPAA.

A privacy official must be appointed to be responsible for developing and implementing policies and procedures at a covered entity. Employees must be trained on appropriate administration, and technical and physical safeguards must be maintained to protect the privacy of protected health information (PHI) in a covered entity.

Source: <https://searchhealthit.techtarget.com/definition/HIPAA>

How HIPAA affects voice over IP (VoIP)

- Stored data must be protected against unlawful disclosure.
- Transmitted call metadata must also be protected, as it can include information that may lead to reidentification.
- Transmitted voice data is not covered by HIPAA.



→ What's next

The collaboration environment, including software, voice endpoints, and video endpoints, should be updated to support Transport Layer Security v1.2 (TLS 1.2).

Organizations that fail to comply with these regulations risk fines or criminal charges.

Learn more to find out if this regulation could be impacting your business.

cisco.com/go/voipcompliance