HIPAA Compliance Datasheet

HIPAA Compliance

The Health Insurance Portability and Accountability Act and supplemental legislation collectively referred to as the HIPAA rules (HIPAA) lay out privacy and security standards that protect the confidentiality of protected health information (PHI). In terms of Unified Communication systems, the solution and security architecture must comply with the applicable standards, implementation specifications and requirements with respect to electronic PHI of a covered entity.

The general requirements of HIPAA Security Standards state that covered entities must:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
4. Ensure compliance by its workforce.

How Zoom Enables HIPAA Compliance

In the course of providing services to healthcare customers, the Zoom Platform and Zoom Phone enable HIPAA compliance to covered entities. In provisioning and operating the Zoom HIPAA Services, Zoom complies with the provisions of the HIPAA Security Rule that are required and applicable to it in its capacity as a business associate.

Zoom is responsible for enforcing the administrative, technical and physical safeguards to prevent any unauthorized access to or disclosure of protected health information (PHI) in the Zoom environment.

The following table demonstrates how Zoom supports HIPAA compliance based on the HIPAA Security Rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule).

HIPAA Standard	How Zoom Supports the Standard
Access Control: • Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs. • Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity. • Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic health information during an emergency. • Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. • Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.	• Data in motion is encrypted at the application layer using Advanced Encryption Standard (AES). • Multi-layered access control for owner, admin, and members. • Web and application access are protected by verified email address and password. • Meeting access is password protected by password or waiting room. • Meetings are not listed publicly by Zoom. • Zoom leverages a redundant and distributed architecture to offer a high level of availability and redundancy. • Organizations can select data center regions for data in motion to your account. This setting does not affect the data at rest storage location. • Meeting host can easily remove attendees or terminate meeting sessions. • Host can lock a meeting in progress. • Meetings end automatically with timeouts. • Privacy features allow you to control session attendee admittance with individual or group entry, waiting rooms, forced meeting test passcodes, and locked room functionality.

Audit Controls: • Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	• Data in motion traverse Zoom's secured and distributed infrastructure. • Platform connections are logged for audio and quality-of-service purposes. • Account admins have secured access to manage individual, group, or organization level management.
Integrity: • Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Multilayer integration protection is designed to protect both data and service layers. • Controls are in place to protect and encrypt meeting data.
Integrity Mechanism: • Mechanism to authenticate electronic protected health information. • Implemented methods to corroborate that information has not been destroyed of altered.	• Application executables are digitally signed. • Data connections leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority. • Web and application access are protected by verified email address and password.

Person or Entity Authentication: • Verify that the person or entity seeking access is the one claimed.	• Web and application access are protected by verified email and password. • Meeting host must log in to Zoom using a unique email address and account password. • Access to desktop or window for screen sharing can be locked by host. • Privacy features allow session attendee admittance with individual or group entry, waiting rooms, forced meeting passcodes, and locked room functionality.
Transmission Security: • Protect electronic health information that is stored on the Zoom platform. • Integrity controls: Ensure that protected health information is not improperly modified without detection. • Encryption: Encrypt protected health information.	• Data encryption protects against passive and active attacks on confidentiality. • Data connections leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority. • Zoom employs AES 256-GCM encryption for data to protect health information.

Security and Encryption

Healthcare organizations and account administrators need to have the tools and technology to ensure they're meeting HIPAA standards. Here are just a few safeguards that enable you to ensure the security and privacy of protected health information (PHI).

- Data in motion is encrypted at the application layer using Advanced Encryption Standard (AES).
- Zoom Chat encryption allows for a secured communication where only the intended recipient can read the secured message. Privacy features allow you to control session attendee admittance with individual or group entry, waiting rooms, forced meeting passcodes, and locked room functionality.

Screen Sharing in Healthcare

Medical professionals and authorized healthcare partners can use Zoom to meet with patients and other healthcare professionals to screen-share health records and other resources. Screen sharing transmits encrypted screen capture mouse and keyboard strokes.

HIPAA Certification

Currently, the agencies that certify health technology – the Office of the National Coordinator for Health Information Technology and the National Institute of Standards and Technology – do "not assume the task of certifying software and off-the-shelf products" (p. 8352 of the Security Rule), nor accredit independent agencies to do HIPAA certifications. Additionally, the HITECH Act only provides for testing and certification of Electronic Health Records (EHR) programs and modules.

Thus, as Zoom is not an EHR software or module, our type of technology is not certifiable by these unregulated agencies.

Saying this, Zoom's HIPAA Attestation was performed by a third party that reviewed and affirmed that Zoom implements the controls needed to secure protected health information (PHI) according to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Breach Notification Rule, and the applicable parts of the Privacy Rule. The Attestation was conducted in compliance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) 18, AT-C sections 105 and 205.

Other Security Certification

SOC2:

The SOC 2 report provides third-party assurance that the design of Zoom, and our internal processes and controls, meet the strict audit requirements set forth by the American Institute of Certified Public Accountants (AICPA) standards for security, availability, confidentiality, and privacy. The SOC 2 report is the de facto assurance standard for cloud service providers.