HIPAA Compliance Guide

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 video conferencing, 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, Zoom does not access PHI. Rather, for purposes of compliance with HIPAA, Zoom models its compliance under the "conduit exception" which applies to entities that transmit PHI but do not have access to the transmitted information. To fall within this exception, Zoom applies mandatory account settings to healthcare customers' accounts, which nearly eliminate a customer's ability to transmit PHI to Zoom.

We do not have access to identifiable PHI and we protect and encrypt all audio, video, and screen sharing data.

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.	• Meeting data transmitted across the network is protected using a unique Advanced Encryption Standard (AES) with a 256-bit key generated and securely distributed to all participants at the start of each session. • Multi-layered access control for owner, admin, and members. • Web and application access are protected by verified email address and password. • By default, meeting access is password protected. • Meetings are not listed publicly by Zoom. • Zoom leverages a redundant and distributed architecture to offer a high level of availability and redundancy. • Meeting host can easily remove attendees or terminate meeting sessions. • Host can lock a meeting in progress • Meetings end automatically with timeouts.
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.	• Meeting connections traverse Zoom's secured and distributed infrastructure. • Meeting connections are logged for audio and quality-of-service purposes. • Account admins have secured access to meeting 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 in motion and at-rest.
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 transmission is protected using HMAC-SHA-256 message authentication codes.
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.
Transmission Security: • Protect electronic health information that is being transmitted over a network. • 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 transmission is protected using HMAC-SHA-256 message authentication codes. • Zoom employs industry-standard Advanced Encryption Standard (AES) encryption using 256-bit keys to protect meetings.

Security and Encryption

Only members invited by account administrators can host Zoom meetings in accounts with multiple members. The host controls meeting attendance through the use of meeting IDs and passwords. Each meeting has only one host unless a co-host is purposefully added by the host. The host can screen share or lock screen sharing. The host has complete control of the meeting and meeting attendees, with features such as lock meeting, expel attendees, mute/unmute all, lock screen sharing, and end meeting.

Zoom employs industry-standard Advanced Encryption Standard (AES) encryption using 256-bit keys to protect meetings. Zoom enables "Fully Encrypted Persistent Chat" on HIPAA accounts and such encryption is irreversible by Zoom. Zoom's Fully Encrypted Persistent Chat is a fully encrypted messaging system which utilizes public key cryptography with private keys generated and stored only on users' devices. Users authenticate their device to Zoom's key management system (KMS) with their Zoom account allowing these keys to then be registered and used to exchange messages through the Zoom platform without ever revealing their contents to Zoom's servers. Zoom encryption fully complies with HIPAA Security Standards to ensure the security and privacy of PHI.

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 along with mouse and keyboard strokes only. Screen sharing cannot be recorded on a HIPAA account and, therefore, is not stored or otherwise accessible by Zoom in Zoom's environment.

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.

Other Security Certifications

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.

TrustArc:

TrustArc has certified the privacy practices and statements for Zoom and also will act as dispute resolution provider for privacy complaints. Zoom is committed to respecting your privacy. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

EU-US Privacy Shield:

Zoom participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. Zoom has committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List https://www.privacyshield.gov/list.