zoom

COMPLIANCE GUIDE

HIPAA Compliance

HIPAA

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.

The general requirements of HIPAA state that covered entities and business associates must:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI the 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.

Zoom for Healthcare

In the course of providing services to healthcare customers, the Zoom for Healthcare and Zoom Phone for Healthcare platforms help enable a customer's HIPAA compliance program by safeguarding PHI and executing business associate agreements covered entities.

Zoom is responsible for employing the appropriate administrative, technical and physical safeguards to prevent any unauthorized access to, or use or disclosure of, PHI.

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

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.

Standard	How Zoom Supports the Standard
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.	Zoom employs 256-bit AES-GCM encryption for data to protect health information.

Security & 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 PHI.

- Data in motion is encrypted at the application layer using 256-bit AES-GCM encryption.
- Advanced 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

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.

Third-Party Attestation

Zoom has engaged a third-party to audit and attest to Zoom's administrative, technical and physical safeguards to protect PHI. Zoom received a successful attestation regarding internal controls meeting applicable obligations under HIPAA.

The attestation was conducted in accordance 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 Certifications and Attestations

Please visit zoom.us/trust for more information and details on other security certifications and attestations.

Zoom Video Communications, Inc. (NASDAQ: ZM) brings teams together to get more done in a frictionless video environment. Our easy, reliable, and innovative video-first unified communications platform provides video meetings, voice, webinars, and chat across desktops, phones, mobile devices, and conference room systems. Zoom helps enterprises create elevated experiences with leading business app integrations and developer tools to create customized workflows. Founded in 2011, Zoom is headquartered in San Jose, California, with offices around the world. Visit zoom.com and follow @zoom.