HIPAA Compliance Guide, January 2015

HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) lays out privacy and security standards that protect the confidentiality of patient health information. In terms of video conferencing, the solution and security architecture must provide end-to-end encryption and meeting access control so the data in-transit cannot be intercepted.

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

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information 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.

Zoom is HIPAA Compliant

Zoom Video Communications is HIPAA compliant. We sign the HIPAA Business Associate Agreement (BAA) for healthcare customers, meaning we are responsible for keeping your patient information secure and reporting security breaches involving personal healthcare information. We do not have access to identifiable health information and we protect and encrypt all audio, video, and screen sharing data.

How Zoom Supports HIPAA Compliance

The following table demonstrates how Zoom supports HIPAA compliance based on the HIPAA Security Standards 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 Support Matrix

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.	• Multi-layered access control for owner, admin, and members. • Web and application access are protected by verified email and strong password. • Meeting access is protected by password. • Meetings are not listed publicly. • Meeting host can easily disconnect attendees or terminate sessions in progress. • Meeting data transmitted across the network is protected using a unique Advanced Encryption Standard (AES) with a 128-bit key generated and securely distributed to all participants at the start of each session.

• 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 ends 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 and reports.
Integrity: • Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Multi-layer integrity protection is designed to protect both data and service layers. • Controls are in place to protect data in-motion and at-rest.
Integrity Mechanism: • Mechanism to authenticate electronic protected health information. • Implement methods to corroborate that information has not been destroyed or altered.	• Application executables are digitally signed. • Data transmission is protected using HMAC-SHA-1 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 strong password. • Meeting host must log in to Zoom using a unique email address and account password. • Access to desktop or window for screen sharing is under the host's control.
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 whenever deemed appropriate.	• End-to-end data security protects passive and active attacks against confidentiality. • Data transmission is protected using HMAC-SHA-1 message authentication codes • Meeting data transmitted across the network is protected using a unique Advanced Encryption Standard (AES) with a 128-bit key generated and securely distributed to all participants at the start of each session.

Security and Encryption

Only members invited by account administrators can host Zoom meetings in accounts with multiple members. Hosts control meeting attendance through the use of meeting IDs and passwords. Each meeting can only have one 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 end-to-end Advanced Encryption Standard (AES) encryption using 128-bit keys to protect meetings. Zoom encryption fully complies with HIPAA Security Standards to ensure the security and privacy of patient data.

Screen Sharing in Healthcare

Medical professionals and authorized healthcare partners can use Zoom's screen sharing, and video and audio conferencing to meet with patients and other healthcare professionals and screen-share health records and other resources. Zoom does not distribute the actual patient data. Screen sharing transmits encrypted screen capture along with mouse and keyboard strokes only, not the actual data. Zoom further protects data confidentiality through a combination of encryption, strong access control, and other protection methods.

HIPAA Certification

Currently, the agencies tasked with certifying 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 Final Security Rule) or accredit independent agencies that 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.