zoom

COMPLIANCE GUIDE

# HIPAA Compliance

**Health Insurance Portability and Accountability Act (HIPAA) Overview**

The Health Insurance Portability and Accountability Act and its 2009 update Health Information Technology for Economic and Clinical Health (HITECH) Act (collectively, "HIPAA") lay out privacy and security standards that protect the confidentiality of patients' protected health information (PHI). HIPAA applies to covered entities (health care providers, health plans, and healthcare clearinghouses) that create, receive, maintain, transmit, or access PHI. Specific HIPAA rules also apply to business associates of covered entities that perform certain functions involving PHI as part of providing services to the covered entity.

Generally, HIPAA requires 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's Role in HIPAA Compliance

Cloud service providers, like Zoom, are usually considered to be business associates when engaged by covered entities to provide services. As a business associate, Zoom is responsible for employing the appropriate administrative, technical and physical safeguards to prevent any unauthorized access to, or use or disclosure of, PHI. Zoom enters into business associate agreements (BAAs) to facilitate our customers' compliance with HIPAA.

The following table describes how Zoom's safeguards support 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.<br>• Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.<br>• Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic health information during an emergency.<br>• Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.<br>• Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information. | • Multi-layered access control for owner, admin, and members.<br>• Web and application access are protected by verified email address and password.<br>• Monitoring, logging, and alerting of failed login attempts, successful authentication, and changes to user access privileges.<br>• Zoom leverages a redundant and distributed architecture to offer a high level of availability and redundancy.<br>• Forced automatic logout of users in the web portal and/or Zoom application after a set amount of time.<br>• Feature-rich client software that leverages a range of encryption technology to assist with user privacy and security, including offering optional end-to-end encryption for Zoom Meetings, Phone, and Mail Service.<br>• Customer data-at-rest is encrypted using a minimum 256-bit AES-GCM either with a Zoom-managed key or a customer-managed key (CMK). CMK functionality allows customers to use their own encryption keys to protect certain data stored at rest within Zoom's infrastructure. |

| Standard | How Zoom Supports the Standard |
|---|---|
| **Integrity** | |
| • Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.<br>• Mechanism to authenticate electronic protected health information.<br>• Implemented methods to corroborate that information has not been destroyed or altered. | • Multilayer integration protection is designed to protect both data and service layers.<br>• Controls are in place to protect and encrypt data.<br>• Internal minimum necessary access privileges, authentication, logging, and monitoring mechanisms to prevent unauthorized access to PHI.<br>• Application executables are digitally signed.<br>• 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.<br>• Admins can enable two-factor authentication (2FA), requiring users to set up and use 2FA. |
| **Transmission Security** | |
| • Protect electronic health information that is stored on the Zoom platform.<br>• Integrity controls: Ensure that protected health information is not improperly modified without detection<br>• Encryption: Encrypt protected health information. | • Customer data is encrypted in transit between customers and Zoom, where supported by the connection method, using Transport Layer Security (TLS) 1.2 or 256-bit AES-GCM.<br>• Data connections leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority.<br>• Streaming real-time media is encrypted at the application layer using Advanced Encryption Standard (AES). |

## Security & Encryption Tools

Zoom gives organizations and account admins tools and technology to help them meet their security and HIPAA compliance objectives. This includes features like:

## Meetings

- Control session attendee admittance with individual or group entry, waiting rooms, forced meeting test passcodes, and locked room functionality.

- Block users authenticated with specific domains from joining meetings.
- Meeting hosts can easily remove attendees, terminate meetings, or lock a meeting in progress.
- Meetings end automatically after idle time.
- Meeting host can lock access to the desktop or window for screen sharing.
- Information barriers can be used to prevent certain groups of users with sensitive information from communicating with others who are not part of designated groups. Information barriers can also be set up for Zoom Phone.
- Enable end-to-end encryption (E2EE), available when all meeting participants join from the Zoom desktop app, mobile app, or Zoom Rooms.

## Team Chat

- Enable or disable the ability for users to chat with or add external contacts and remove any external contacts that have been added.
- Use the chat etiquette tool to define keywords and text patterns to prevent users from sharing unwanted messages.
- Advanced chat encryption allows for a secured communication where only the intended recipient can read the secured message.

## Phone

- Enable end-to-end encryption (E2EE) for one-on-one calls between users on the same Zoom account that occur in the Zoom client. Enabling E2EE for calls disables certain features and requires both call participants to join from the Zoom desktop application or mobile app (PSTN is not supported).
- Add numbers to a block list to prevent calls and SMS to/from certain numbers.
- Hide certain personal data on display in the dashboard and call log after a specified number of days.
- Use the SMS etiquette tool to define keywords and text patterns to prevent users from sharing unwanted messages.
- Define the locations where users can make and accept calls and send SMS.

## Contact Center

- Mask certain personal data elements from display for specified user roles in live text-based engagements and when viewing closed engagements, analytics, and voicemail inbox.
- Role-based permissions to limit users' ability to view or listen, download, and delete content.
- Set video and voice recording policies at an account or queue level.
- Specify regex rules to block the sending of sensitive data from being shared in a chat or SMS engagement.

## Workvivo

- Manage audience access to specific information based on practitioner, location, or any other criteria.
- Admins can create classification tags (e.g., internal, secret, external) to indicate sensitive content. Once a user applies a tag to a piece of content, the tag will be displayed on that content throughout the application.
- Predefine expiration dates on documents so that these disappear from view when no longer required.
- Governance Analytics dashboard to easily view users with elevated access, system admins, editors, space managers, and apps/docs editors.

For more information about Zoom's services, please visit https://www.zoom.com/en/products/.

## Zoom's AI Tools

Zoom provides account administrators and users with controls to manage AI features, including AI Companion features. Zoom does not use customers' audio, video, chat, screen sharing, attachments or other communications like content (such as poll results, whiteboard and reactions) to train Zoom's or its third party artificial intelligence models.

The data used with AI tools like AI Companion is generally retained according to the customer's retention settings for related products (such as Team Chat or Whiteboard). Data is deleted if a user or administrator deletes it or following account termination. Some data may be retained temporarily for debugging, trust and safety, or to comply with legal obligations. The Zoom AI Companion Security and Privacy Whitepaper provides more information about AI Companion's security and privacy features.

## Certification and Attestations

Zoom's services, including Meetings, Team Chat, Phone, and Contact Center, have undergone audits by independent third-party auditors including as part of the SOC 2 + HITRUST certification process. The Health Information Trust Alliance Common Security Framework (HITRUST CSF) is a security framework that leverages nationally and internationally accepted standards and regulations such as GDPR, ISO, NIST, PCI, and HIPAA.

Zoom's SOC 2 + HITRUST report, available through Zoom's Compliance portal, gives customers a view into the controls in place to protect the security and availability of the Zoom platform.

Please visit Zoom Compliance and Zoom's Trust Center for more information and details on other security certifications and attestations.

*This document is not intended as legal advice. Zoom's customers are responsible for ensuring their use of Zoom's services aligns with their obligations under HIPAA. We encourage all customers to seek counsel on what their requirements are under applicable law in the jurisdictions in which they are using Zoom services.*

Zoom Workplace — our AI-powered, open collaboration platform built for modern work — streamlines communications, improves productivity, increases employee engagement, optimizes in-person time, and offers customer choice with third-party apps and integrations. Zoom Workplace, powered by Zoom AI Companion, includes collaboration solutions like meetings, team chat, phone, scheduler, whiteboard, spaces, Workvivo, and more. Together with Zoom Workplace, Zoom's Business Services for sales, marketing, and customer care teams, including Zoom Contact Center, strengthen customer relationships throughout the customer lifecycle.