LogMeIn HIPAA Considerations

LogMeIn

Contents

Introduction – LogMeIn HIPAA Considerations

The Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, requires all organizations that maintain or transmit electronic healthcare information to establish and implement certain administrative, physical, and technical safeguards to keep that information safe from unauthorized access.

The Department of Health & Human Services has issued specific rules to enforce the act, namely the HIPAA Security Standards published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards, Final Rule).

These rules include Technical Safeguards that apply to covered entities that use remote access products to maintain or transmit electronic healthcare information. To view the HIPAA rules in their entirety, visit the Health Information Privacy page of the U.S. Department of Health and Human Services website at *www.hhs.gov/ocr/privacy/*, or go directly to the *Security Standards: Technical Standards* document.

About this Document

This LogMeIn publication provides a brief introduction to the scope of HIPAA compliance with regard to remote access products (including LogMeIn Pro and Central) and support and collaboration products (including LogMeIn Rescue).

Section A outlines key background information needed to understand the scope of HIPAA compliance with regard to remote access products.

Section B outlines the HIPAA rules' Technical Safeguards (see § 164.312), which apply to remote access products used by entities subject to HIPAA compliance.

Sections C through H demonstrate how LogMeIn helps organizations adhere to, meet, or exceed these safeguards.

When relevant, this document also covers LogMeIn Files, a cloud storage feature provided with LogMeIn Pro.

Important: The information contained in this document is provided to you "AS IS" and does not constitute legal advice or an opinion regarding LogMeIn's HIPAA compliance. LogMeIn makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in or referenced in this document. LogMeIn recommends that you seek the advice of competent legal counsel before relying on any of the statements contained in this document.

General HIPAA Information

Section A – Background information on HIPAA Rules

What entities are covered by HIPAA?	All healthcare clearinghouses, health plans, and healthcare providers that conduct certain transactions in electronic form. This includes entities that use a billing service to conduct transactions on their behalf.
What is considered "electronic" under the terms of HIPAA?	The term “electronic” is used to describe, but is not limited to, the transmitting of healthcare information via the Internet, an extranet, leased lines, dial-up lines, etc.
What are HIPAA transactions?	• Healthcare claims or their equivalent • Healthcare payment and remittance advice • Healthcare claims status • Eligibility inquiries • Referral certifications and authorizations • Claims attachments • First reports of injury

Technical Safeguards Overview

Section B – HIPAA Technical Safeguards § 164.312

These safeguards apply directly to remote access products.

Note: Some items are marked as addressable. Under the terms of HIPAA, the term addressable is somewhat ambiguous, but it essentially means that the covered entity is allowed some flexibility in taking “reasonable” steps to comply with the standard or specification referred to.

Access Control	164.312(a)(1)	Unique User Identification (Required) Emergency Access Procedure (Required) Automatic Logoff (Addressable) Encryption and Decryption (Addressable)
Audit Controls	164.312(b)	(Required)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (Addressable)
Person or Entity Authentication	164.312(d)	(Required)
Transmission Security	164.312(e)(1)	Integrity Controls (Addressable) Encryption (Addressable)

Using LogMeIn to Meet Technical Safeguards

Section C – Access Control § 164.312(a)(1)

(Required)

Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to persons or software programs that have been granted access rights.

Access and Management: LogMeIn Pro, Central

- Access to host computers is protected by separate, unique passwords for the website (LogMeIn.com) and each LogMeIn host computer.
- Access to host computers is protected by Windows or Mac authentication.
- Users can protect their account by turning on two-step verification.
- Users can authenticate to the host using one-time security codes.

Tip: Log in to your account and go to **Account** > **Security**.

- Authenticate to the host using RSA SecurID two-factor authentication.

Tip: Visit help.LogMeIn.com for *implementation details*. Windows hosts only.

- Set a lockout threshold for failed login attempts, known as Authentication Attack Blocker.

Tip: Open LogMeIn and follow this path: **Options** > **Preferences** > **Security**.

- LogMeIn Files
  - All of the above also apply.
  - Data is encrypted upon upload. In emergencies, authorized LogMeIn personnel may, with your permission, need to access the encryption keys for your files.

Support and Collaboration: LogMeIn Rescue

- Control access permissions at the Technician Group level. Examples: Restrict groups of technicians from using remote control, Connect on LAN, or Unattended Access. Restrict groups of technicians from using file transfer, thereby eliminating their ability to take files from remote computers.

Tip: Open the Administration Center, select a group, and follow this path: **Organization tab** > **Permissions**.

- The customer (end user) must be present at the remote machine, and permit remote access.
- The customer maintains control and can terminate the session at any time.
- Force the customer to always grant or deny a technician's request to use specific functions (remote control, desktop view, file transfer, system information, and reboot and reconnect).

Tip: Open the Administration Center, select a group, and disable the following option: **Organization tab** > **Permissions** > **Use single prompt for all permissions**.

- Access rights are automatically revoked when a session is terminated.
- Access rights are revoked after a specified period of inactivity.

Section D – Audit Controls § 164.312(b)

(Required)

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Access and Management: LogMeIn Pro, Central

- Connection and remote session activity is logged on the host computer to ensure security and maintain quality control.

Tip: To view information on session activity, open LogMeIn and follow this path: **Options** > **Connection and Event Details**.

- Access the Windows Event log or Mac console log to get up-to-the-minute data, including user names and the client computer's IP address, on logon/logout and remote control events.
- On the host computer's hard disk, a detailed log is kept of the remote access product's activities. To protect these files from tampering, the administrator can also specify a different log file location.

Tip: Open LogMeIn and follow this path: **Options** > **Preferences** > **Advanced** > **Event Logs** > **Location of event logs**.

- Configure and log on to a Syslog server, which allows you to view events from multiple locations. Requires LogMeIn Central; Windows hosts only.
- LogMeIn recommends using a relational database to centrally collect log information. Log destinations can be as simple as a Microsoft Access database or as sophisticated as an Oracle server.
- Administrators can also restrict access to host computers to ensure that data can only be queried or modified by qualified administrators.
- Automatically create .avi file video recordings of every remote control session. These recordings enable the user to see the recorded sessions exactly as seen by the remote user. Recordings can be saved to a network location. Windows hosts only.

Note: Open LogMeIn and follow this path: **Options** > **Preferences** > **Advanced** > **Screen Recording**.

- LogMeIn Files
  - LogMeIn Files stores additional audit information when files or folders are made available via a public link. Otherwise, you can rely on account access logs.
  - You can set up an object audit for your registry to create an audit trail of clients linking LogMeIn Files to their computers.
  - LogMeIn recommends using a relational database to centrally collect log information. Log destinations can be as simple as a Microsoft Access database or as sophisticated as an Oracle server.

Support and Collaboration: LogMeIn Rescue

- Automatically create .avi file video recordings of every remote control session. These recordings enable the user to see the recorded sessions exactly as seen by the remote user. Recordings can be saved to a network location.

  Tip: Open the Administration Center, select a group, and follow this path: **Settings tab** > **Screen recording**.

- Remote sessions are logged to ensure security and maintain quality control.

  Tip: Open the Administration Center and follow this path: **Reports tab** > **Report Area: [various]**.

Section E – Integrity policies and procedures, § 164.312(c)(1)

(Addressable)

Access and Management: LogMeIn Pro, Central

- Users accessing a host computer remotely can disable the keyboard or mouse on the host computer, thereby protecting the integrity of data inputs.

  Tip: During remote control, on the remote control toolbar, select **Options** > **Lock Keyboard**.

- Users can set up automatic alerts to identify system events that indicate attempts at unauthorized access. Requires LogMeIn Central; Windows Pro hosts only.

Support and Collaboration: LogMeIn Rescue

- Control access permissions at the Technician Group level.

  Tip: Open the Administration Center, select a group, and follow this path: **Organization tab** > **Permissions**.

  - Restrict groups of technicians from using remote control, Connect On LAN, or Unattended Access.
  - Restrict groups of technicians from using file transfer, thereby eliminating their ability to copy files from remote computers.

Section F – Integrity mechanism, § 164.312(c)(2)

(Addressable)

Mechanism to authenticate electronic protected health information. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Access and Management: LogMeIn Pro, Central

- All data transmitted during remote, chat, or file transfer sessions is protected by at least 128-bit encryption.
- When the encryption level on the client browser permits, all data transmitted during remote, chat, or file transfer sessions is protected by 256-bit TLS 1.2 encryption.
- User can set up automatic alerts to identify system events that indicate attempts at unauthorized access.

Note: Log in to your account and go to **Account** > **Security**.

- LogMeIn Files
  - File integrity is protected during transmission as described here: *Section H.2 – Transmission Security § 164.312(e)(1) Integrity Controls* on page 10.
  - To ensure file integrity at rest, LogMeIn recommends configuring your file integrity tool to cover your mounted drive. The standard options available in the Files user interface do not offer integrity protection at rest.
  - Users can set up automatic alerts to identify user events that indicate unauthorized activity.

Support and Collaboration: LogMeIn Rescue

- End-to-end 256-bit TLS 1.2 encryption of all data.
- MD5 Hash for enhanced traceability of file transfers when File Transfer is enabled.

Section G – Person or Entity Authentication§ 164.312(d)

(Required)

Access and Management: LogMeIn Pro, Central

- Access to the host computer is protected by the use of separate, unique passwords for the website and the host computer.
- Set up a Personal Password to access the host computer to verify that access is authorized.

Tip: Open LogMeIn and follow this path: **Options** > **Preferences** > **Security**.

- Configure an IP address lockout to prevent unauthorized remote access from a specific client computer. With IP address filtering, users can grant or prevent access for multiple IP addresses.

Tip: Open LogMeIn and follow this path: **Options** > **Preferences** > **Security**.

Support and Collaboration: LogMeIn Rescue

- The technician's identity is defined by a unique email address, or via an SSO ID, and the technician must be authenticated.
- Excessive number of unsuccessful login attempts (five unsuccessful attempts) will lock the account.
- Use IP address restrictions to limit access to the Technician Console.

Tip: Open the Administration Center, select a group, and follow this path: **Settings tab** > **IP Restrictions (Technician Console)**.

Section H.1 – Transmission Security § 164.312(e)(1)

(Required)

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Access and Management: LogMeIn Pro, Central

- All data transmitted during remote, chat, or file transfer sessions is protected by at least 128-bit encryption.
- When the encryption level on the client browser permits, all data transmitted during remote, chat, or file transfer sessions is protected by 256-bit encryption.

Support and Collaboration: LogMeIn Rescue

- End-to-end 256-bit TLS 1.2 encryption of all data.
- MD5 Hash for enhanced traceability of file transfers when File Transfer is enabled.

Section H.2 – Transmission Security § 164.312(e)(1) Integrity Controls

(Addressable)

Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Access and Management: LogMeIn Pro, Central

- All data transmitted during remote, chat, or file transfer sessions is protected by at least 128-bit encryption.
- When the encryption level on the client browser permits, all data transmitted during remote, chat, or file transfer sessions is protected by 256-bit encryption.
- All data transmitted during remote, chat, or file transfer sessions is protected by 128-bit encryption.

Support and Collaboration: LogMeIn Rescue

- End-to-end 256-bit TLS 1.2 encryption of all data.
- MD5 Hash for enhanced traceability of file transfers when File Transfer is enabled.

Section H.3 – Transmission Security, Encryption § 164.312(e)(1)

(Addressable)

Access and Management: LogMeIn Pro, Central

- All data transmitted during remote access, chat, or file transfer sessions is protected by at least 128-bit encryption. You can set up automatic alerts to identify system events that indicate unauthorized access attempts.

- When the encryption level on the client browser permits, all data transmitted during remote, chat, or file transfer sessions is protected by 256-bit TLS 1.2 encryption.

Support and Collaboration: LogMeIn Rescue

- End-to-end 256-bit TLS 1.2 encryption of all data.