LogMeIn®

HIPAA

considerations with LogMeIn

Introduction

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 http://www.hhs.gov/ocr/privacy/index.html, or go directly to the Security Standards: Technical Standards document (PDF).

About this Document

This LogMeIn publication provides a brief introduction to the scope of HIPAA compliance with regard to remote access products, including LogMeIn.

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

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

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

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.

Table 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

Table B. HIPAA Technical Safeguards § 164.312

These safeguards apply directly to remote access products.

- All *required* implementation standards or specifications are marked as (Required)
- All *addressable* implementation standards or specifications 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)

Tables C-H. HIPAA Technical Safeguards § 164.312

HIPAA Considerations for LogMeIn Pro^2 and LogMeIn Free

Table C – Access Controls

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 to the host computer is protected by the use of separate, unique passwords for the website (LogMeIn.com) and the host computer.	✓	✓
	Access to the host computer is protected by the use of Windows or Mac authentication.	✓	✓
	Users can authenticate to the host using one-time security codes. ➡ Log in to your account and go to **Account** > **Security**.	✓	✓
	Users can authenticate to the host using RSA SecurID two-factor authentication. Windows only. Visit the Knowledge Base for implementation details.	✓	
	Users can set a lockout threshold for failed login attempts (Authentication Attack Blocker). ➡ From the host, open LogMeIn and follow this path: **Options** > **Preferences** > **Security** From the client, connect to the host Main Menu and follow this path: **Preferences** > **Security**	✓	✓

Table D – Audit Controls

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.	User connection and remote session activity is logged on the host computer to ensure security and maintain quality control. Users have ready access to information on session activity. ➡ From the host, open LogMeIn and follow this path: **Options > Connection and Event Details** From the client, connect to the host Main Menu and follow this path: **Preferences > Advanced > Event Logs**	✓	✓
	Users can log on to the Windows Event log to get up-to-the-minute data, including usernames and the client computer’s IP address, on logon/logout and remote control events.	✓	

Audit Controls § 164.312(b) (Required)			
	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. ➡ From the host, open LogMeIn and follow this path: **Options** > **Preferences** > **Advanced** > **Event Logs** > **Location of event logs** From the client, connect to the host Main Menu and follow this path: **Preferences** > **Advanced** > **Event Logs** > **Location of event logs**	✓	✓
	Users can configure and log on to a Syslog server, which enables the viewing of events from an unlimited number of locations. (Requires LogMeIn Central)	✓	
	Users can use 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 ensure that data can only be queried or modified by qualified administrators. (Requires LogMeIn Central)	✓	

Audit Controls § 164.312(b) (Required)		⊞	
	Users can 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. ➡ From the host, open LogMeIn and follow this path: **Options > Preferences > Advanced > Screen Recording** From the client, connect to the host Main Menu and follow this path: **Preferences > Advanced > Screen Recording**	✓	

Table E –Integrity, policies and procedures

Integrity § 164.312(c)(1) (Addressable)		⊞	
Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Users accessing a host computer remotely can disable the keyboard or mouse on the host computer, thereby protecting the integrity of data inputs. ➡ During remote control, on the remote control toolbar, select **Options > Lock Keyboard**	✓	✓
	User can set up automatic alerts to identify system events that indicate attempts at unauthorized access. (Requires LogMeIn Central)	✓	

Table F –Integrity, mechanism

Integrity § 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.	All data transmitted during remote, chat, or file transfer sessions is protected by 128-bit encryption. User can set up automatic alerts to identify system events that indicate attempts at unauthorized access.	✓	✓
	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.	✓	✓
	User can set up automatic alerts to identify system events that indicate attempts at unauthorized access. ➡ Log in to your account and go to **Account** > **Security**	✓	✓

Table G – Person or Entity Authentication

Person or Entity Authentication § 164.312(d) (Required)			
Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Access to the host computer is protected by the use of separate, unique passwords for the website and the host computer.	✓	✓
	Users have the option of setting up so-called Personal Password to access the host computer to verify that access is authorized. ➡ From the host, open LogMeIn and follow this path: **Options > Preferences > Security** From the client, connect to the host Main Menu and follow this path: **Preferences > Security**	✓	✓
	User can 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. ➡ From the host, open LogMeIn and follow this path: **Options > Preferences > Security** From the client, connect to the host Main Menu and follow this path: **Preferences > Security**	✓	✓

Table H.1 –Transmission Security

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.	All data transmitted during remote, chat, or file transfer sessions is protected by 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.	✓	✓

Table H.2 –Transmission Security, Integrity Controls

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.	All data transmitted during remote, chat, or file transfer sessions is protected by 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.	✓	✓

Table H.3 –Transmission Security, Encryption

Transmission Security, Encryption § 164.312(e)(1) (Addressable)			
Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	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.	✓	✓