GoToMeeting and HIPAA Compliance

Privacy, productivity and remote support

The Health Insurance Portability and Accountability Act (HIPAA) calls for privacy and security standards that protect the confidentiality and integrity of patient health information. Specifically, if you are transmitting patient data across the Internet during an online meeting or video conference, your online meeting solution and security architecture should strive to provide end-to-end encryption and meeting access control to help avoid interception by anyone other than the invited participants.

GoToMeeting is an online meeting solution that can help your company or office meet these guidelines.

The following matrix demonstrates how GoToMeeting can support HIPAA compliance and is based upon the HIPAA Security Standards rule published in the Federal Register on January 25, 2013 (45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule). The Department of Health and Human Services provides the HIPAA Security Standards on its website: https://www.hhs.gov/hipaa/for-professionals/security/index.html.

For more information about GoToMeeting security, download the GoToMeeting Security white paper at www.gotomeeting.com / security-white-paper.

Technical Safeguards § 164.312

Standards Covered Entities Must Implement	Implementation Specifications R=Required A=Addressable		Key Factors	Support in GoToMeeting
(a) (1) Access Control		R	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.	Meeting access is protected by a unique meeting code and optional strong password authentication. Configurable failed log-in lockout threshold. Meetings are not listed publicly, and access is restricted to invited participants. Meeting organizer can easily disconnect attendees or terminate sessions in progress.
	Unique User Identification	R	Assign a unique name and/or number for identifying and tracking user identity.	Organizers and account administrators* use their unique email address as their login name; they must also enter a unique account password.
	Emergency Access Procedure	R	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	One-click meetings provide rapid, secure access to online meetings from virtually anywhere, which may be used as a supplementary method for providing emergency access to healthcare information.
	Automatic Logoff	A	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Organizer-configurable session inactivity time-out ensures that screen sharing is not enabled indefinitely. Website inactivity time-out automatically logs users out of their GoToMeeting accounts.
	Encryption and Decryption	A	Implement a mechanism to encrypt and decrypt electronic protected health information.	All sensitive chat, session and control data transmitted across the network is protected using the Advanced Encryption Standard (AES) with a 128-bit key. A unique 128-bit AES encryption key is generated and securely distributed to all participants at the start of each session.

Technical Safeguards § 164.312				
Standards Covered Entities Must Implement	**Implementation Specifications R=Required A=Addressable**		**Key Factors**	**Support in GoToMeeting**
(b) Audit Controls		R	Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	All connection and session activity through the distributed network service infrastructure is logged for security and quality-of-service purposes. Account managers** have up-to-the-minute, web-based access to advanced management and reporting tools.
(c)(1) Integrity		A	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Integrity protection mechanisms are designed to ensure a high degree of data and service integrity, working independently of any integrity controls that may already exist on the customer's computers and internal data systems. The presenter can choose to not share keyboard and mouse control, ensuring the integrity of application commands and inputs.
(c)(1) Integrity Mechanism	Mechanism to authenticate electronic protected health information.	A	Implement methods to corroborate that information has not been destroyed or altered.	All executables are digitally signed. All transmitted data is integrity protected using HMAC-SHA-1 message authentication codes.
(d) Person or Entity Authentication		R	Verify that the person or entity seeking access is the one claimed.	Meeting organizers must log in to GoToMeeting using a unique email address and account password. Meeting access is protected by a unique code and optional strong password. Only invited participants may view shared meeting data. Access to data and applications on the presenter's computer is always under the presenter's control.

Technical Safeguards § 164.312				
Standards Covered Entities Must Implement	**Implementation Specifications R=Required A=Addressable**		**Key Factors**	**Support in GoToMeeting**
(e)(1) Transmission Security		R	Protect electronic health information that is being transmitted over a network.	GoToMeeting provides true end-to-end data security that addresses both passive and active attacks against confidentiality. Encryption and Integrity controls are used end-to-end to ensure confidentiality regardless of the network the data is traversing.
	Integrity Controls	A	Ensure that protected health information is not improperly modified without detection.	All transmitted data is integrity protected using HMAC-SHA-1 message authentication codes.
	Encryption	A	Encrypt protected health information whenever deemed appropriate.	All sensitive chat, session, video, audio and control data transmitted across the network is protected using the Advanced Encryption Standard (AES) with a 128-bit key.

*Account administrators only applicable when buying multiple user subscriptions of GoToMeeting.

Healthcare Applications

Physicians, nurses, IS/IT staff, administrative employees and authorized healthcare partners can use GoToMeeting's patented web-based screen-sharing, video conferencing and audio conferencing technology to instantly and securely meet online with other healthcare professionals and share files, database applications and other corporate resources from any location connected to the web. Unlike other web conferencing solutions, GoToMeeting does not distribute the actual patient data across networks. Rather, by using screen-sharing technology, security is strengthened because only mouse and keyboard commands are transmitted. GoToMeeting further protects data confidentiality through a combination of encryption, strong access control and other protection methods.

Security and Control

Only organizers approved by account administrators can organize GoToMeeting online meetings in accounts with multiple organizers. Organizers control online meeting attendance through the use of meeting ID codes and optional passwords. Only one person can present at a time, and the presenter (either the organizer or a person chosen by the organizer) maintains complete control of screen sharing, in addition to keyboard and mouse control. Thus, participants can only view information the presenter chooses and can only make changes if the presenter allows them to do so. In addition, organizers can disconnect attendees when necessary, and organizers and account administrators can both terminate meetings in progress at any time.

Encryption

GoToMeeting employs industry-standard end-to-end Advanced Encryption Standard (AES) encryption using 128-bit keys to protect the data stream, chat messages and keyboard and mouse input. GoToMeeting encryption is consistent with HIPAA Security Standards to ensure the security and privacy of patient data.

Frequently Asked Questions

Q: What are the general requirements of the HIPAA Security Standards?
(Ref: § 164.306 Security Standards: General Rules)

Covered entities must do the following:

- Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
- Ensure compliance with this subpart by its workforce.

Q: How are covered entities expected to address these requirements?

Covered entities may use any security measures that reasonably and appropriately implement the standards; however, covered entities must first take into account the risks to protected electronic information; the organization's size, complexity and existing infrastructure; and costs.

The final rule includes three "safeguards" sections outlining standards (what must be done) and "implementation specifications" (how it must be done) that are either "required" or "addressable." If "required," it must be implemented to meet the standard; if "addressable," a covered entity can either implement it, implement an equivalent measure or do nothing (documenting why it would not be reasonable and appropriate).

- Administrative Safeguards: Policies and procedures, workforce security and training, evaluations and business associate contracts.
- Physical Safeguards: Facility access, workstation security and device and media controls.
- Technical Safeguards: Access control, audit controls, data integrity, authentication and transmission security.

Q: What are we doing to help customers address HIPAA regulations?

To facilitate our customers' compliance with HIPAA security regulations, we are providing detailed information about the security safeguards we have implemented into the GoToMeeting service. This information is provided in this document, our security white paper and other technical collateral. Additionally, our Client Services group is available to provide guidance and assistance in all deployments.

Q: Is GoToMeeting HIPAA compliant?

Only "covered entities" (e.g. healthcare organizations) are required to comply with HIPAA. Because of the technical and security measures employed by the service, when used properly, GoToMeeting can help covered entities fulfil their HIPAA compliance obligations. (For example, the administrative configuration and control features provided with GoToMeeting support healthcare-organization compliance with the Administrative and Physical Safeguards sections of the final HIPAA Security Rules.)

As a result, GoToMeeting may be confidently deployed as an outsourced remote-access component of a larger information-management system without affecting HIPAA compliance.

Q: What is the best way to deploy GoToMeeting in an environment subject to HIPAA regulations?

Just as HIPAA allows considerable latitude in the choice of how to implement security safeguards, a single set of guidelines is not applicable for all deployments. Organizations should carefully review all configurable security features of GoToMeeting in the context of their specific environments, user population and policy requirements to determine which features should be enabled and how best to configure.

9.21.2018/ LMI0098b PDF