Remote Support HIPAA Compliance Guide

Privacy, productivity and remote support

The healthcare industry has benefited greatly from the ability to receive remote support from technology providers and internal IT departments. However, since the computers being serviced often contain confidential patient data, many remote support products inadvertently put patient privacy at risk, especially if the data is sent or made accessible over unsecured networks such as the Internet.

For this reason, 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 transmit patient data across the Internet, your remote support products and security architecture must provide end-to-end encryption so the data cannot be intercepted by anyone other than the intended recipient. In addition, the remote support products and network must provide access control to allow viewing only by authorized people.

HIPAA compliance guide
We created the following matrix as a guide to assist healthcare providers in navigating the various HIPAA requirements and to demonstrate how GoToAssist Remote Support can support HIPAA compliance. General HIPAA requirements can be found in the Frequently Asked Questions section at the end of this document. The matrix is based upon 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). The Department of Health and Human Services provides the HIPAA Security Standards on its website: http://www. hhs.gov/ocr/privacy/hipaa/understanding/ srsummary.html.

Healthcare applications
Authorized technology providers and IS/IT staff can use GoToAssist Remote Support patented web-based screen-sharing technology to instantly and securely view PC and Mac desktops and provide remote assistance to healthcare workers from any location connected to the web. Unlike other remote-support solutions, GoToAssist Remote Support does not distribute actual data across networks. Rather, by using screen-sharing technology, security is strengthened because only mouse and keyboard commands are transmitted. GoToAssist Remote Support further protects data confidentiality through a combination of encryption, strong access control and computer protection methods.

Security, control and customization
Support administrators have the option of assigning representatives to groups defined by the features to which they are granted access. Some features may be disabled by an administrator to customize the level of security that is appropriate for your organization. Because the security features are built in, administrators can rest easy: Security cannot be weakened by inexperienced users.

Encryption
GoToAssist Remote Support employs industry-standard end-to-end Advanced Encryption Standard (AES) encryption using 128-bit keys to protect the data stream, file transfers, chat and keyboard and mouse input. Additional built-in security features such as strong passwords, end-to-end user authentication and unique session connection codes ensure data confidentiality. GoToAssist Remote Support encryption fully complies with HIPAA Security Standards to ensure the security and privacy of patient data.

Technical safeguards § 164.312

Standards covered entities must implement	Implementation specifications R=Required A=Addressable		Key factors	Support in GoToAssist Remote Support
(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.	• PC and Mac access is 100% permission based and the customer retains overriding control at all times. • Representatives and managers must log in using strong passwords to access the GoToAssist Remote Support solution. • Technicians running GoToAssist Remote Support as a service must log in with the proper credentials of a local or domain administrator.
	Unique User Identification	R	Assign a unique name and/or number for identifying and tracking user identity.	• Representatives and administrators are identified by using their unique email address as their log-in name.
	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), FIPS 197. • A unique 128-bit AES encryption key is generated at the start of each session.
(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 our distributed network service infrastructure is logged for security and quality-of-service purposes. • All remote-support sessions, chat, diagnostics and customer feedback can be recorded and archived on GoToAssist Remote Support servers.
(c)(1) Integrity		A	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Integrity protection mechanisms in GoToAssist Remote Support 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. • Customer has complete overriding control of all keyboard and mouse activity.
(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 session data is compressed using proprietary lossless compression techniques and protected using HMAC-SHA1 message authentication codes. • Numerous additional structural integrity checks are made on the decrypted session data after it is received to ensure data and service integrity. • Session recording, if enabled, would show if any data was inadvertently affected by the remote-support session.
(d) Person or Entity Authentication		R	Verify that the person or entity seeking access is the one claimed.	• Access to GoToAssist Remote Support is protected by a strong password and a unique user log-in ID. • Representatives must be approved and set up by an administrator before they can access client computers.

Standards covered entities must implement	Implementation specifications R=Required A=Addressable		Key factors	Support in GoToAssist Remote Support
(e)(1) Transmission Security		R	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Integrity protection mechanisms in GoToAssist Remote Support 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. • Customer has complete overriding control of all keyboard and mouse activity.
	Integrity Controls	R	Ensure that protected health information is not improperly modified without detection.	• All session data is compressed using proprietary lossless compression techniques and protected using HMAC-SHA1 message authentication codes. • Numerous additional checks are made on the decrypted session data after it is received to ensure network transmission integrity.
	Encryption	R	Encrypt protected health information whenever deemed appropriate.	• All sensitive chat, session, file transfer and service control data transmitted across the network is protected using AES (FIPS 197) in counter mode. • A unique 128-bit AES encryption key is generated at the start of each session.

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 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 you doing to help customers address HIPAA regulations?

To facilitate our customers' compliance with HIPAA security regulations, we're providing detailed information about the security safeguards we have implemented into the GoToAssist Remote Support service. This information is provided in several forms, including security white papers, service-specific HIPAA-compliance matrices and other technical collateral. Additionally, our staff are available to provide guidance and assistance in all deployments.

Q: Is GoToAssist Remote Support 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, GoToAssist Remote Support can help covered entities fulfil their HIPAA compliance obligations. For example, the administrative configuration and control features provided with GoToAssist Remote Support help maintain healthcare organization compliance with the Administrative and Physical Safeguards sections of the final HIPAA Security Rules.

The net result is that GoToAssist Remote Support may be confidently deployed as a remote-support component of a larger information-management system without affecting HIPAA compliance.

Q: What is the best way to deploy GoToAssist Remote Support 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 GoToAssist Remote Support in the context of their specific environments, user population and policy requirements to determine which features should be enabled and how best to configure.