GoToAssist™

HIPAA

HIPAA-Compliance Matrix for GoToAssist™

The following matrix is based on the final version of 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). A copy of the final Security Standards is available here: http://aspe.os.dhhs.gov/admnsimp/FINAL/FR03-8334.pdf.

** Source: HIPAA Technical Safeguards § 164.312.*

Standards that Must Be Implemented by Covered Entities	**Implementation Specifications** **R=**Required **A=**Addressable	**Key Standards:**	**GoToAssist: The following features address HIPAA standards**
(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 those persons or software programs that have been granted access rights as specified in § 164.308." *	• Portal access by support representatives and administrators is protected by strong passwords. • Configurable 'failed login' lockout threshold • Role-based access control on GoToAssist portal controls access to features and services based on assigned roles as account manager, administrators or support representatives. • Only the end user can initiate a GoToAssist session. • End user controls support rep's access to keyboard/mouse functions. • File Transfer and Session Recording features may be disabled by account manager • After a session ends, GoToAssist software is not left running on end user's computer. Support rep cannot re-connect to machine unless end user initiates another session.
	R Unique User Identification (required)	"Assign a unique name and/or number for identifying and tracking user identity." *	• Support representatives, administrators and account managers are identified by using unique email addresses as log-in names.
	R Emergency Access Procedure	"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency." *	• GoToAssist's ability to provide rapid, secure remote access to a PC may be utilized by an end user as a supplementary method for providing emergency access to healthcare information.

Standards that Must Be Implemented by Covered Entities	Implementation Specifications R=Required A=Addressable	Key Standards:	GoToAssist: The following features address HIPAA standards
	A Automatic Logoff	"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity." *	• GoToAssist sessions only terminate if network connectivity is lost or if the end user actively terminates the session. The support rep's ability to remotely operate the end user's keyboard and mouse may interfere with normal inactivity time-out/auto logout implemented by operating system of end user's PC. • One way to address this requirement is to configure the GoToAssist portal to view-only mode. In this mode, the support rep can only draw on the remote screen - the support rep's normal keyboard and mouse activity is not sent to the end user's PC.
	A Encryption and Decryption	"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 in 8-bit cipher-feedback mode. • A unique 128-bit AES encryption key is generated at the start of each session. • If session recording is enabled, all stored session data remains encrypted. The session key is archived using RSA public-key encryption.
(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 Citrix Online's distributed network-service infrastructure is logged for security and quality. • Administrators have up-to-the-minute Web-based access to GoToAssist's advanced management and reporting tools. • Chat, session and connection activity logs may be reviewed.
(c) (1) Integrity	**A**	"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction." *	• Integrity-protection mechanisms in GoToAssist are designed to ensure a high degree of data and service integrity. These mechanisms work independently of any existing integrity controls that may already exist on the end user's PC and internal data systems.

Standards that Must Be Implemented by Covered Entities	Implementation Specifications R=Required A=Addressable	Key Standards:	GoToAssist: The following features address HIPAA standards
	A 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 session data is protected via proprietary, loss-less compression techniques and the use of AES in 8-bit cipher feedback mode. that offers inherent integrity protection. • Additional structural-integrity checks made on the decrypted session data after receipt to ensure data and service integrity.
(d) Person or Entity Authentication	**R**	"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed." *	• Portal access by support reps and administrators is protected by strong passwords.
(e) (1) Transmission Security	**R**	"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." *	• All network traffic is integrity protected and encrypted using 128-bit AES encryption.
	A Integrity Controls	"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of." *	• All session data is protected via proprietary, loss-less compression techniques and the use of AES in 8-bit cipher feedback mode.that offers inherent integrity protection. • Additional checks made on the decrypted session data after receipt to ensure network-transmission integrity.
	A Encryption	"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate." *	• All sensitive chat, session, file-transfer and service-control data transmitted across the network is protected using the Advanced Encryption Standard (AES) FIPS 197 in 8-bit cipher-feedback mode. • A unique 128-bit AES encryption key is generated at the start of each session. • If session recording is enabled, all stored session data remains encrypted. The session key is archived using RSA public-key encryption.

Arrange a Demo: www.GoToAssist.com | Phone: (800) 549-8541
Sales Information: gotoassist@citrixonline.com | Phone: (800) 549-8541
Media Inquiries: pr@citrixonline.com | Phone: (805) 690-6448

Citrix Online Division • 5385 Hollister Avenue • Santa Barbara, CA 93111