Citrix GoToMyPC Corporate HIPAA Compliance Guide

Overview

Privacy, productivity and remote access

The healthcare industry has benefited greatly from the ability to use remote access to view patient data from anywhere and share data among partners and suppliers. Although transmitting patient data across networks improves care, speeds service and reduces healthcare costs, many remote access products inadvertently put patient privacy at risk, especially if the data is sent 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 are transmitting patient data across the Internet, your remote access 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 access products and network must provide access control to allow viewing only by authorized people.

Citrix GoToMyPC Corporate HIPAA Security Guide

Every business that is part of the U.S. healthcare industry needs to comply with the federal standards regulating patient information. In addition to protecting worker health insurance coverage, HIPAA sets forth standards for protecting the integrity, confidentiality and availability of electronic health information. Citrix® GoToMyPC® Corporate is a HIPAA-compliant remote access solution that can help your company or office meet these guidelines.

The following 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://aspe.os.dhhs.gov/admnsimp/FINAL/FR03-8334.pdf.

Citrix Online created the following matrix as a guide to assist healthcare providers in navigating the various HIPAA requirements and to demonstrate how Citrix GoToMyPC Corporate can support HIPAA compliance. General HIPAA requirements can be found in the Frequently Asked Questions section at the end of this document.

Technical safeguards § 164.312

Standard covered entities must implement	Implementation specifications R = Required A = Addressable		Key factors	Support in Citrix GoToMyPC Corporate
(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.	• Host computer access is protected by two levels of strong password authentication. Separate passwords are used for authentication to website and then to the host computer. • Optional support for One-Time Passwords or SecurID token-based two-factor authentication. • Configurable failed log-in lockout threshold. • Account manager organizes users into groups, defining access policy on a per-user or per-group basis. • Account manager can terminate sessions in progress with a single click of the mouse.
	Unique User Identification (Required)	R	Assign a unique name and/or number for identifying and tracking user identity.	• Users and account managers are identified by using their unique email address as their login name.
	Emergency Access Procedure	R	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	• Provides rapid, secure access to a computer desktop 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.	• Manager-configurable session inactivity time-out ensures that GoToMyPC Corporate remote-access sessions are not left running indefinitely. • Website inactivity time-out automatically logs users out of their GoToMyPC Corporate 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), FIPS 197 in 8-bit cipher feedback mode. • 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 Citrix Online's distributed network service infrastructure is logged (including file transfers, remote printing, WAN IP and more) 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 in 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. • Physical access to host cmoputer's screen, mouse and keyboard can be disabled during a session, ensuring the integrity of a remote user's application commands and inputs.
(c)(1) Integrity Mechanism to Authenticate electronic protected health information.	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 via the AES cipher in counter mode with 128-bit keys and additional integrity protection. • Numerous additional structural integrity checks are made on the decrypted session data after it is received to ensure data and service integrity.
(d) Person or Entity Authentication		**R**	Verify that the person or entity seeking access is the one claimed.	• Website access is protected by a strong password; the only way to access individual host computers is via the website. • Each host computer is protected by a unique strong password and optional two-factor authentication. • Access to data and applications on the host computer requires the user to be logged in to Windows with a valid domain account. • Participation in GoToMyPC Corporate sessions may optionally be restricted to only pre-authorized host and client machines identified by their unique network adaptor MAC addresses or disk drive serial numbers.
(e)(1) Transmission Security		**R**	Protect electronic health information that is being transmitted over a network.	• All network traffic is protected and encrypted using 128-bit AES encryption. • After a session ends, no GoToMyPC Corporate software or information is left on the client computer.
	Integrity Controls	**A**	Ensure that protected health information is not improperly modified without detection.	• All session data is compressed using proprietary lossless compression techniques and protected via the AES cipher in counter mode with 128-bit keys and additional integrity protection. • Numerous additional checks are made on the decrypted session data after it is received to ensure network transmission integrity.
	Encryption	**A**	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.

GoToMyPC Corporate product information

Healthcare applications

Physicians, nurses, IS/IT staff, administrative employees and authorized healthcare partners can use GoToMyPC Corporate patented web-based screen-sharing technology to instantly and securely view Mac® and PC desktops and to use files, database applications and other corporate resources from any location connected to the web. Unlike other remote-access solutions, GoToMyPC Corporate 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. GoToMyPC Corporate further protects data confidentiality through a combination of encryption, strong access control and host computer protection methods.

Security, control and customization

Users and administrators have the option of assigning users to groups defined by the features to which they are granted access. Some features may be disabled by an IT administrator to customize the level of security that is appropriate for your organization. In addition, GoToMyPC Corporate offers an Authorization Management Service to ensure that only users with approved GoToMyPC Corporate accounts can access your organization's networks. Because the security features are built in, administrators can rest easy: Security cannot be weakened by inexperienced users.

Encryption

GoToMyPC Corporate 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 dual passwords, end-to-end user authentication, host screen blanking and host keyboard and mouse locking ensure data confidentiality. GoToMyPC Corporate encryption fully complies 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)

A: 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?

A: 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 is Citrix Online doing to help customers address HIPAA regulations?

A: To facilitate our customers' compliance with HIPAA security regulations, Citrix Online is providing detailed information about the security safeguards we have implemented into the GoToMyPC Corporate service. This information is provided in several forms, including security white papers, service-specific HIPAA-compliance matrices and other technical collateral. Additionally, Citrix Online's Client Services group is available to provide guidance and assistance in all deployments.

Q: Is GoToMyPC Corporate HIPAA compliant?

A: Although HIPAA compliance per se is applicable only to entities covered by HIPAA regulations (e.g., healthcare organizations), the technical security controls employed in the GoToMyPC Corporate service and associated host and client software meet or exceed HIPAA technical standards. Furthermore, the administrative configuration and control features provided with GoToMyPC Corporate support healthcare-organization compliance with the Administrative and Physical Safeguards sections of the final HIPAA Security Rules.

The net result is that GoToMyPC Corporate 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 GoToMyPC Corporate in an environment subject to HIPAA regulations?

A: 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 GoToMyPC Corporate in the context of their specific environments, user population and policy requirements to determine which features should be enabled and how best to configure.

Depending on enterprise policy, disabling the File Transfer and/or Remote Printing features may be advisable to ensure host integrity and maximize data containment and confidentiality.

The GoToMyPC Corporate Administration Center offers a comprehensive set of web-based user management, host/client end-point management and auditing features. Organizations are advised to review and use the features that they believe will achieve maximum overall system-assurance levels and compliance with HIPAA-mandated administrative, technical and physical security safeguards.

CITRIX® | online

Citrix Online Division
6500 Hollister Avenue
Goleta, CA 93117
U.S.A.
T +1 805 690 6400
info@citrixonline.com

Media inquiries:
pr@citrixonline.com
T +1 805 690 2969

Citrix Online Europe
Middle East & Africa
Citrix Online UK Ltd
Chalfont Park House
Chalfont Park, Gerrards Cross
Bucks SL9 0DZ
United Kingdom
T +44 (0) 800 011 2120
europe@citrixonline.com

Citrix Online Asia Pacific
Suite 3201
32nd Floor
One International Finance Center
1 Harbour View Street
Central, Hong Kong SAR
T +852 100 5000
asiapac@citrixonline.com

About Citrix Online
Citrix Online solutions enable people to work from anywhere. Our products include GoToAssist® for remote support, GoToManage™ for IT management, GoToMeeting® for online meetings, GoToMyPC® for remote access, GoToTraining® for interactive online training and GoToWebinar® for larger web events.

08.09.10/B-31523/PDF