

HIPAA & HITECH Require High Security for Healthcare Records

Healthcare organizations face growing pressure to securely exchange patient data while meeting stringent HIPAA and HITECH compliance requirements. Legacy file transfer methods, including FTP, email, and manual processes, often lack the security, visibility, and governance required to protect sensitive healthcare information.

Stronger security is now required when electronic patient health records are transferred, and tight administrative control and audit reports are essential. Protecting electronic protected health information (ePHI) requires strong security controls, centralized oversight, and comprehensive audit capabilities to support compliance and reduce data breach risk.

GoAnywhere MFT from Fortra is a cross-platform managed file transfer solution designed to help you meet HIPAA/HITECH compliance standards while saving you time and money. By replacing manual processes, disconnected tools, and custom scripts with centralized, automated workflows, GoAnywhere helps healthcare organizations improve operational efficiency, increase reliability, and maintain audit readiness.

Secure, Governed File Transfers for HIPAA Compliance and Healthcare Data Exchange

GoAnywhere helps healthcare organizations securely exchange sensitive data through a centralized, governed, and auditable platform designed to support compliance, security, and operational efficiency. Enterprise-grade security, workflow automation, and centralized visibility helps healthcare organizations secure patient data *without sacrificing speed or productivity*.



GoAnywhere:

- Centralizes file transfer operations, workflows, and governance across healthcare ecosystems
- Automates file transfers and business processes through workflow automation, scheduling, event-based triggers, and no-code workflow design
- Protects sensitive healthcare data using role-based access controls, granular permissions, and multi-factor authentication (MFA)
- Provides centralized monitoring and visibility into file transfer activity across internal systems and external partner exchanges
- Provides detailed audit trails and reporting of every file transfer, identifying users, recipients, and file names transmitted, helping organizations simplify compliance reporting and maintain audit readiness
- Integrates with existing healthcare applications, systems, cloud environments, and business processes

At the same time, GoAnywhere protects ePHI and other data records by:

- Providing end-to-end security through encryption for data at rest and in transit, including AES encryption and OpenPGP file protection options
- Extending secure file transfer services beyond the firewall with GoAnywhere Gateway, helping keep sensitive systems and data out of the DMZ
- Enforcing strict access controls and MFA to reduce unauthorized access risks
- Capturing comprehensive audit logs and reporting for governance, compliance, and operational visibility

GoAnywhere helps reduce data breach risk for both internal and external exchanges, while maintaining the speed required to support patient care and business operations.

With rigorous access control, MFA, audit logging, encryption, and workflow automation capabilities, organizations gain centralized control, visibility, and governance over sensitive healthcare data movement while supporting HIPAA and HITECH requirements.

GoAnywhere Helps You Meet HIPAA/HITECH Data Transfer Security Requirements

The table below highlights how GoAnywhere helps healthcare organizations secure and govern file transfers while supporting compliance requirements. Certain aspects of the standards are considered “addressable,” which means there is some flexibility on how to best implement those requirements.

	HIPAA REGULATION	CORRESPONDING GOANYWHERE FEATURE
REQUIRED STANDARDS	Access Control Prevent unauthorized access from users or software that do not have permissions.	Users and passwords can be authenticated using a variety of techniques including database authentication, LDAP and Active Directory (AD). Accounts can additionally be authenticated using X.509 certificates and SSH keys. Role-based security allows administrative users to access only authorized features. Folders and files can be authorized to user groups or individual users.
	Unique User Identification Ensure each user can be singularly tracked.	Each GoAnywhere user must have a unique user ID and password to log into GoAnywhere. All activity for the user is audited in the GoAnywhere central database, including all file transfer activity. This audit information can be reported within GoAnywhere and can additionally be sent to a central SYSLOG server.
	Integrity Prevent unauthorized access from users or software that do not have permission to view or access.	Folders and files can be restricted from edit/delete access by user and group. This data can be made available for read-only access or can be completely restricted. Encrypted transmissions use hashing algorithms to confirm the integrity of data packets.
	Person or Entity Authentication Provide electronic verification that ensures that the claimed identity of a user is accurate.	Users can be authenticated using a variety of protocols including database, LDAP, AD, SSH keys and certificates.
ADDRESSABLE STANDARDS	Transmission Security Establish electronic security protocols to insulate data in motion from unauthorized access as its transferred across electronic networks.	Files and transmissions are securely transferred using SFTP, FTPS and HTTPS protocols, as well as encryption standards of AES and Open PGP.
	Automatic Logoff Disconnect or terminate electronic sessions based on predetermined rules.	The session timeout can be configured by the administrator so users are automatically logged out after a specific length of inactivity.
	Encryption & Decryption Apply procedures to encrypt and decrypt data such as ePHI (electronic patient health information).	Data can be exchanged securely using SFTP (SSH), FTPS (SSL/TLS), SCP and HTTPS protocols. The files can be individually encrypted using the Open PGP and AES encryption standards.
	Authentic ePHI Demonstrate via electronic records that data has not been altered, compromised, or deleted without authorization.	Audit trails will document when unauthorized attempts are made to alter or delete documents through GoAnywhere.
	Integrity Controls Prevent unauthorized access from users or software that do not have permission to view or access.	Files and folders can be restricted by individual users and group profiles.
	Encryption Apply encryption to ePHI whenever appropriate or necessary.	Files are encrypted and decrypted using the Open PGP and AES encryption standards.



About GoAnywhere MFT

Fortra's GoAnywhere is an award-winning cybersecurity product line trusted by more than 4,000 organizations to securely connect with business partners, automate IT processes, and protect sensitive data at scale. Built for centralized, enterprise-grade control, GoAnywhere helps organizations streamline mission-critical file transfer operations while keeping sensitive information out of the DMZ.

goanywhere.com