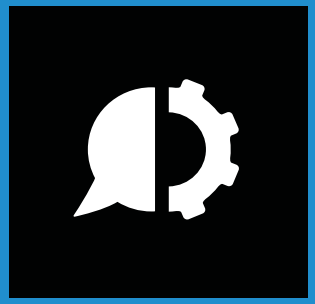
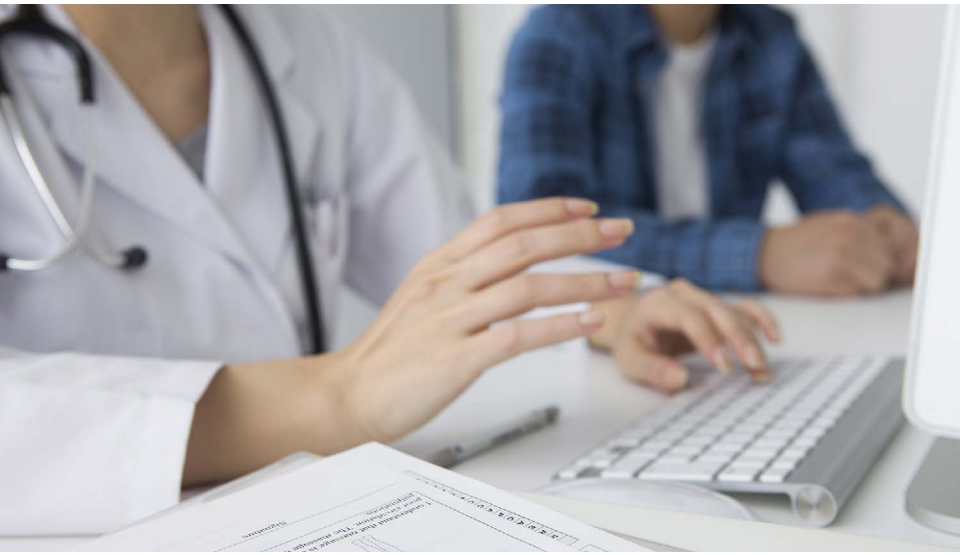
GO ANYWHERE™
Managed File Transfer

Five Ways to Improve Electronic Patient Record Handling for HIPAA/HITECH with Managed File Transfer



INTRODUCTION



The healthcare industry is under increasing pressure to make health information more accessible to both patients and healthcare providers, while simultaneously ensuring that patient data remains private and secure. As hospitals, physician practices, and other providers transition to electronic health record (EHR) solutions to ensure the former, they must closely follow the guidelines and requirements of the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH) and the Affordable Care Act (ACA) in regards to the security of electronic patient health information (ePHI).

Meeting HIPAA and HITECH security and compliance requirements is a formidable challenge. Even as clinicians are able to more easily share patient files, test results, x-rays, and other data, strong security is required when these records are transferred, along with tight administrative controls and thorough audit report. Securing ePHI that is exchanged among providers and their trading partners can be complex, time-consuming and expensive.

While many healthcare organizations have effectively secured the transmission of ePHI, they often have to utilize expensive programming resources to write scripts for automating batch file transfer functions, containing numerous commands that have to be executed in order to connect with their partners. As more trading partners are brought into the fold, these scripts become increasingly unmanageable. In some cases, these providers may use the legacy FTP protocol to transfer bulk data with their partners, despite the lack of security and management features inherent in that process.

Hospitals and other healthcare organizations have recognized the need to move away from being dependent on programming resources to enable the secure and convenient transfer of files among their trading partners. They want to build these transfers quickly as they add new partners, without intensive programming, and in a manner that provides maximum security and control.

Healthcare organizations need a manageable, affordable way to transfer files while also providing the security and audit trail required under HIPAA, HITECH and the ACA. They must be able to control the transfer of all sensitive files at every step so that patient data can be shared with outside physicians, government organizations, insurance companies, pharmacies and other entities. File transfers must also be fully auditable, preferably in an automated fashion to reduce the complexity and labor-intensive processes. A secure and simplified file transfer process can reduce costs and free up administrative and programming staff to focus on other critical tasks.

Emerging managed file transfer (MFT) solutions can provide the security, control, and visibility that can help the healthcare industry address the current challenges related to the electronic transfer of patient files. This white paper will outline the ways in which MFT can help address the security compliance requirements now faced by healthcare providers.

What is Managed File Transfer (MFT)?

"A secure and simplified file transfer process can REDUCE COSTS and free up administrative and programming staff to FOCUS ON OTHER CRITICAL TASKS."

Managed file transfer is a software solution that securely transfers data from one computer to another, and provides reporting, auditability, global visibility, scheduling automation, performance metrics and monitoring. MFT is an alternative to decentralized file transfer tools and programming scripts, and it provides a greater degree of organizational control, visibility, and security.

MFT solutions utilize standard protocols such as SFTP, SCP, Open PGP or FTPS for encrypted file transfers. Some MFT solutions also include support for other protocols, such as SMTP, AS2, Web Services, HTTPS etc. A centralized management solution is overlaid on these technologies, providing a standardized system for all file transfers within an organization.

These solutions provide full audit trails so that companies know who transferred each file, where it went, and when the transfer occurred. Most MFT systems also provide automation capabilities, so that managers can be alerted if there are problems with a transfer, or jobs can be executed automatically

when certain files arrive in specific locations. For example, the MFT solution could initiate file conversions, database, and distribution activities.

Each transfer in MFT is assigned a unique tracking number, providing a complete audit trail that is stored for each activity. The solution tracks which user initiated the transfer and the date/time the transfer occurred, and users can immediately receive warnings and error messages via a central reporting system.

Five Ways MFT Can Improve HIPAA and HITECH Compliance

Under the HIPAA/HITECH rules, healthcare providers and their trading partners have to follow strict guidelines for managing ePHI. Those guidelines (found in the HIPAA Security Rule, section 164.312) include a number of access, encryption, integrity, authentication and auditing requirements for protecting patient data.

Using an MFT solution can provide significant advantages when it comes to meeting these requirements. The alternative in many organizations is a loosely controlled series of ad-hoc file transfers that can jeopardize sensitive patient data, and generate severe penalties for non-compliance.

In ad-hoc scenarios, files can be sent via unsecured FTP with very little documentation or tracking. Individual employees may send files from their desktop to outside parties using free tools like FileZilla, and a hospital or physician practice may have no record of that transfer. That not only makes the type of compliance and auditing required under current healthcare regulations nearly impossible, it also makes it difficult for organizations to confirm critical files were sent to trading partners, or that they arrived intact.

Employees may send files via e-mail or through services like DropBox because it is easier than getting IT to develop new scripts for different partners. An MFT solution can simplify transfers for employees, while also making these transfers fully trackable and auditable, as well as more secure.

Below are five key ways that an MFT solution that can help meet HIPAA/HITECH requirements, while making the file transfer process more efficient and effective for employees.

"Using an MFT solution can provide SIGNIFICANT ADVANTAGES when it comes to meeting these (HIPAA/HITECH) requirements."

Automated Processes

Although automation is not expressly required under HIPAA, automating regular batch file transfers to trading partners (such as laboratories or insurance companies) can help meet access control requirements of the HIPAA law. By automating these transfers using an MFT solution, providers can eliminate the type of unsecured, ad hoc file transfers that may occur within the organization, and replace them with an effective assortment of batch transfers. In this way, they can reduce the number of staff members that have to access the solution, which improves access control and security.

Running these jobs automatically ensures that files are transferred correctly and on time. Automation also eliminates the need for individual users to manually enter sensitive passwords. Role-based access in an MFT solution can still allow approved users to run ad-hoc transfers as needed, but with the centralized controls and auditing needed for compliance.

Additionally, an MFT solution can convert data from internal health care information system into different data formats (like CSV or Excel) so the information can be shared with trading partners. Because the MFT solution can encrypt this data, sensitive data is not copied from a database into an unsecured format.

A robust MFT can also automatically alert supervisors and support personnel when a transfer fails. Since such a failure can indicate a security issue, it is imperative that proper staff members receive real-time updates on the status of ongoing transfers.

Access Control and Identification

HIPAA requires both limited access to patient data and the use of unique user identification, along with such capabilities as automatic logoff and authentication of users and entities that verify the identity of anyone accessing ePHI.

With an MFT solution, 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 will allow administrative users to access only authorized features, and folders and files can be authorized to user groups or individual users.

"HIPAA requires that healthcare organizations implement a mechanism to encrypt ePHI."

In order to log into the MFT, each user is required to have a unique ID. That allows the solution to audit all user file transfer activities, and store and report that information.

Folders and files can be restricted from edit/delete access by user and group. Data can be made available for read-only access or can be completely restricted. Encrypted transmissions may use hashing algorithms to confirm the integrity of data packets during transmission.

Data Security

HIPAA requires that healthcare organizations implement a mechanism to encrypt ePHI, ensure that information has not been altered or destroyed in an unauthorized manner, authenticate ePHI user access, and guard against breaches as the data is transmitted over an electronic network.

With an MFT solution, files and transmissions are securely transferred using SFTP, FTPS and HTTPS protocols, as well as encryption standards of AES and Open PGP. Procedures can be established to encrypt ePHI while it is at rest on internal servers, and to also encrypt the tunnels through which the files may travel.

Access to files and folders is restricted to authorized users, who must access the MFT solution with a minimum of a valid username and password, along with the added security of a key or certificate for authentication.

When working with outside trading partners, secure HTTPS links can provide access to files for external users for quick access. With an MFT, that external access can be monitored and controlled to authorized recipients. Additionally, the MFT solution can be configured to password-protect those download links, limit the number of downloads and expire the links after a certain period of time.

Establish an Audit Trail

A key component of the HIPAA/HITECH requirements is that all information related to ePHI file transfers be trackable and auditable. Using an MFT, establishing this audit data is simple to accomplish, and results in a data store that not only complies

with the regulations, but also provides highly granular visibility into file transfer activities for internal use.

Audit trails can document when unauthorized activities (e.g. invalid logins) are attempted in MFT, a requirement for ePHI authentication within HIPAA. The MFT solution can provide detailed information on each file transfer so that providers have a detailed history of security procedures used for each transmission. The MFT also tracks which individual users access the solution to ensure organizational accountability.

Organizations can be quickly alerted of any file transfer issues via email, SYSLOG or other messaging systems. At the same time, using this monitoring data, they can establish internal auditing processes that can help them establish best practices and continuous improvement programs. Finally, the data can be presented to external auditors to establish that all transfers are fully compliant.

Reduce the Cost of Compliance

An MFT solution can also cut the cost of compliance. By automating the file transfer process and limiting the number of PC-based and decentralized file transfers that occur within a healthcare organization, the cost of managing files and complying with regulatory requirements can be reduced.

By eliminating the use of complex FTP scripts and manual transfer processes, healthcare organizations can reduce the total number of man-hours dedicated to managing the movement of ePHI. For companies that still transfer physical files to their trading partners, having access to an automated, secure electronic transfer process can eliminate the cost of using an authorized courier service, along with the time required to prepare those files.

CONCLUSION

For healthcare organizations, the security of ePHI will be critical as the adoption of electronic health records continues, and pressure mounts to more effectively share data in a secure fashion. Meeting HIPAA, HITECH and ACA requirements using manual file management processes will be increasingly costly, time consuming, and ineffective. By deploying a managed file transfer (MFT) solution with robust encryption, authentication, automation, and auditing capabilities, healthcare providers can reduce the challenges associated with compliance while simultaneously making file transfers more efficient and ensuring the privacy and integrity of patient data.

See how easy it is to secure your patient data with GoAnywhere MFT.

Request a demo at
info.goanywhere.com/healthcare

HelpSystems
103 South 14th Street
Ashland, Nebraska 68003
(402) 944.4242
(800) 949.4969
goanywhere.sales@helpsystems.com
www.goanywhere.com

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.