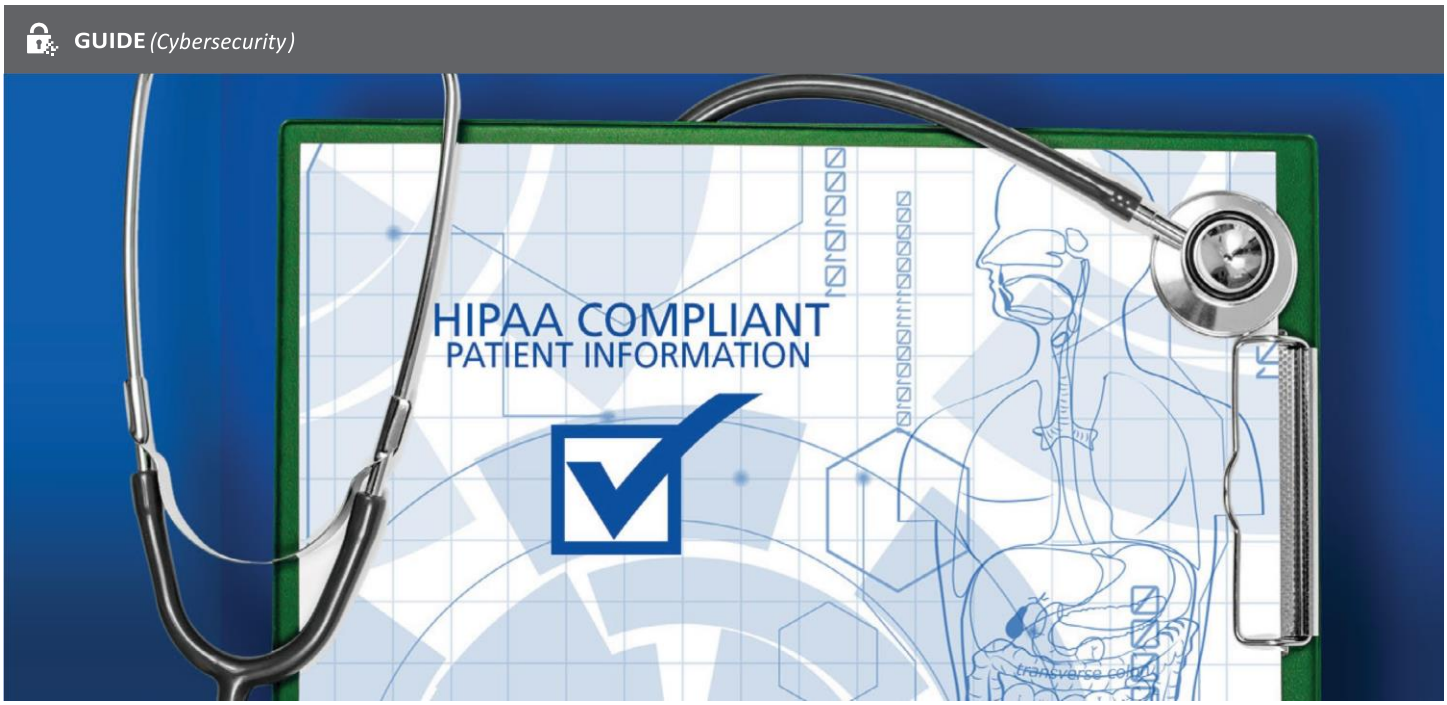
Managed File Transfer



How Managed File Transfer Addresses HIPAA Requirements for ePHI

INTRODUCTION

As the healthcare industry transitions from primarily using paper documents and patient charts to electronic health records, the need for a secure and reliable method of sharing electronic protected health information (ePHI) has increased. Both the Health Information Technology for Economic and Clinical Health Act (HITECH) and Health Insurance Portability and Accountability Act (HIPAA) include specific guidance and requirements related to the transfer of ePHI. Failure to follow these guidelines can result in potential privacy breaches and HIPAA violations.

These new requirements have effectively made traditional File Transfer Protocol (FTP) file sharing ill-advised, if not obsolete. Transferring electronic patient records requires strong security, tight administrative controls, and thorough audit reporting that is not possible using traditional, ad hoc methods.

A robust managed file transfer (MFT) solution can not only streamline and automate the movement of critical patient files for healthcare providers, insurance companies, vendors, and other stakeholders, it can also provide the security and controls necessary for HIPAA and HITECH compliance.

By eliminating the custom programming and complex scripting normally required for these transfers, MFT can also save time and money, improve the quality of and dependability of file transfers, and free up IT and administrative resources that would otherwise have to manage these processes.

A well-designed MFT solution helps organizations meet the requirements of HIPAA and HITECH by implementing a managed and auditable solution. These solutions can centralize file transfer processes, automate workflows, monitor file transfers, provide detailed audit logs and enable file protection (through encryption) beyond the organization's firewall.

This white paper will provide an overview of how MFT solutions can help healthcare organizations meet the specific requirements of the HIPAA standards.

Meeting HIPAA Required Standards

Below is a list of HIPAA required standards related to the transfer of ePHI, along with a description of how an MFT solution can help meet those standards. All of the requirements are part of the HIPAA §164.312 Technical Safeguards.

"Transferring electronic patient records requires strong security, tight administrative controls, and thorough audit reporting that is not possible using traditional, ad hoc methods."

HIPAA § 164.312(a)(1)

Access Control: 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.

Using an MFT solution, users and passwords can be authenticated via 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 in a MFT solution allows administrative users to access only authorized features, and folders and files can be authorized to specific users and groups. Each user is required to have a unique ID to log into the MFT, and data can be made available for restricted access.

HIPAA § 164.312 (a)(2)(i)

Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.

Each MFT user must have a unique user ID and password to log into the solution. All activity for the user can be audited in a central database, including all file transfer activity. This audit information can be reported within the MFT and can additionally be sent to a central SYSLOG server.

HIPAA § 164.312(c)(1)

Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

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.

HIPAA § 164.312(d)

Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

MFT users can be authenticated using a variety of protocols including database, LDAP, AD, SSH keys and certificates. Digital signatures can be utilized in the data to confirm the sender's identity (non-repudiation).

HIPAA § 164.312(e)(1)

Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications 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.

HIPAA Addressable Standards

Within HIPAA, certain parts of the standard are listed as "addressable," and can be implemented in a slightly more flexible manner than other requirements. In meeting addressable implementation specifications, a covered entity can implement the specifications, implement one or more alternative security measures to accomplish the same goal, or choose not to implement the specification at all. MFT offers a simple, affordable way for covered entities to meet both the addressable and required specifications.

HIPAA § 164.312(a)(2)(iii)

Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

The session timeout with an MFT solution can be configured by the administrator so users are automatically logged out after being inactive for the specified length of time.

HIPAA § 164.312(a)(2)(iv)

Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.

Data can be exchanged securely using SFTP (SSH), SCP, FTPS (SSL/TLS) and HTTPS protocols using a managed file transfer solution. The files can be individually encrypted using the Open PGP and AES encryption standards. Additionally, procedures can be established to automatically encrypt ePHI while it is at rest on internal servers, and to encrypt the tunnels through which the files may travel during transfer.

HIPAA § 164.312(b)(1)

Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

MFT solutions can capture required audit data and provide a mechanism to monitor all file transfers. All user activity is tracked and audited in a central database, providing complete visibility. Any unauthorized activity can also be tracked using the MFT system. Providers can maintain a detailed history of security procedures associated with each transmission, as well as individual user access history since all users are uniquely identified. Any unauthorized transfers or transfer failures can trigger alerts via e-mail, SYSLOG, and other messaging systems. The data can also be used by internal auditing programs.

HIPAA §164.312(c)(2)

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.

Audit trails will document when unauthorized attempts are made to access the MFT system. The combination of unique user identification and the ability to limit file access by individuals and groups can further prevent unauthorized changes.

HIPAA § 164.312 (e)(2)(i)

Integrity Controls: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Using an MFT solution, files and folders can be restricted by individual users and group profiles. Through standard hash algorithms, data packet checksums can verify that the data sent matches the data received. As mentioned earlier, the system also tracks all user activity centrally and can generate alerts based on customized parameters and triggers, creating another layer of protection against data tampering.

"MFT offers a simple, affordable way for covered entities to meet both the addressable and required (HIPAA) specifications."

HIPAA § 164.312 (e)(2)(ii)

Encryption: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Files transferred via MFT can be encrypted and decrypted using the Open PGP and AES encryption standards. SSL and SSH standards are utilized for encrypting tunnels between systems. Data can be automatically encrypted on internal servers at rest.

CONCLUSION

Managed file transfer, as outlined above, can help healthcare organizations and their trading partners more securely exchange ePHI and meet both the required and addressable specifications of the HIPAA standard.

An MFT platform protects against data breaches for both internal and external transmissions. Using rigorous access control and automated transfer processes—complete with encryption— such solutions can provide the comprehensive management controls that HIPAA and HITECH regulations require.