COVIANT Software

YOUR GUIDE TO HIPAA COMPLIANT FILE TRANSFERS

COVIANT SOFTWARE

Coviant Software supports leading healthcare organizations with their secure managed file transfer (MFT) solutions. MFT solutions are designed to help healthcare organizations maintain HIPAA compliance by automating the encryption of electronic protected health information (ePHI) when in transit and at rest.

Contents

01 **Overview**

02 **Designing Your Hipaa Compliant File Transfers**

03 **Meeting Hipaa Updates**

04 **Summary**

Overview

If you are in the healthcare industry, you need a file transfer solution that is secure, easy to use, and scalable to handle your largest and most complex jobs. And you also need it to support your efforts to operate in compliance with the Health Insurance Portability and Accountability Act (HIPAA).

In 2025, significant updates to HIPAA are set to reshape how healthcare organizations handle sensitive data, including personally identifiable information (PII) and electronic protected health information (ePHI) in transit and at rest. The proposed changes aim to protect patient privacy, and healthcare organizations should be proactive and adapt to a changing 'digital healthcare environment' or face strengthened penalties for non-compliance. Some of these penalties include additional sanctions for repeat violations or breaches resulting from negligence.

Good business practice dictates data protection for you, your customers, and your business partners – including data in-motion. But even the best security practices do not alleviate the need to demonstrate compliance with a variety of changing regulations and standards that can carry high contractual, civil, and criminal penalties. Plus, the indirect loss of faith of your customers or business partners can have an incalculable impact on your bottom line. The key here is to keep learning and evolving the technology used in your organization.

HIPAA 2025 changes require regulated entities to identify their information systems that create, receive, maintain, or transmit ePHI and all technology assets, including hardware, software, electronic media, information, and data, that may affect ePHI.

Popular secure protocols, such as SSL or SSH, are used when data is transmitted outside the corporate firewall to customers, business partners, or other departments. These protocols support a secure and compliant file transfer process, but they are not enough to ensure security and compliance goals are met. Delivering security and compliance with your file transfer process requires a **managed file transfer solution** with a full complement of security features to ensure that your data is always protected.

Overview

Coviant Software offers Diplomat MFT, a suite of **managed file transfer solutions** that has the security features, automations, and simple operation needed to keep your sensitive data secure at rest and in motion, minimize risks associated with human error, and keep your staff more efficient when complying with HIPAA, no matter what the upcoming changes look like. Diplomat MFT brings together the security and workflow management features that IT and security professionals need, in an easy to implement, cost- effective managed file transfer solution, for automating your secure file transfer process.

This paper offers a step-by-step guide to creating a framework for a HIPAA compliant file transfer system, that you can implement in your organization today when built with a secure, managed file transfer solution, that has the scalability and flexibility necessary to accommodate your needs as your organization grows, necessary for the revised HIPAA compliance in 2025 and beyond.

Step 1: Create A Secure Configuration

Secure file transfer requires a solution that spans the corporate firewall. One part of the solution, such as a secure FTP or web server, is located outside the firewall and acts as a temporary repository for files being transferred between business partners or other entities. Another part of the solution, such as a managed file transfer solution, resides in a secure location inside the corporate firewall and manages file transfers to and from the FTP server. Secure FTP servers are popular among business partners that want to standardize on non-proprietary solutions. To ensure file transfer security, only the secure FTP server should be outside the internal firewall and a managed file transfer solution, such as Diplomat MFT, must be safely inside the internal firewall.

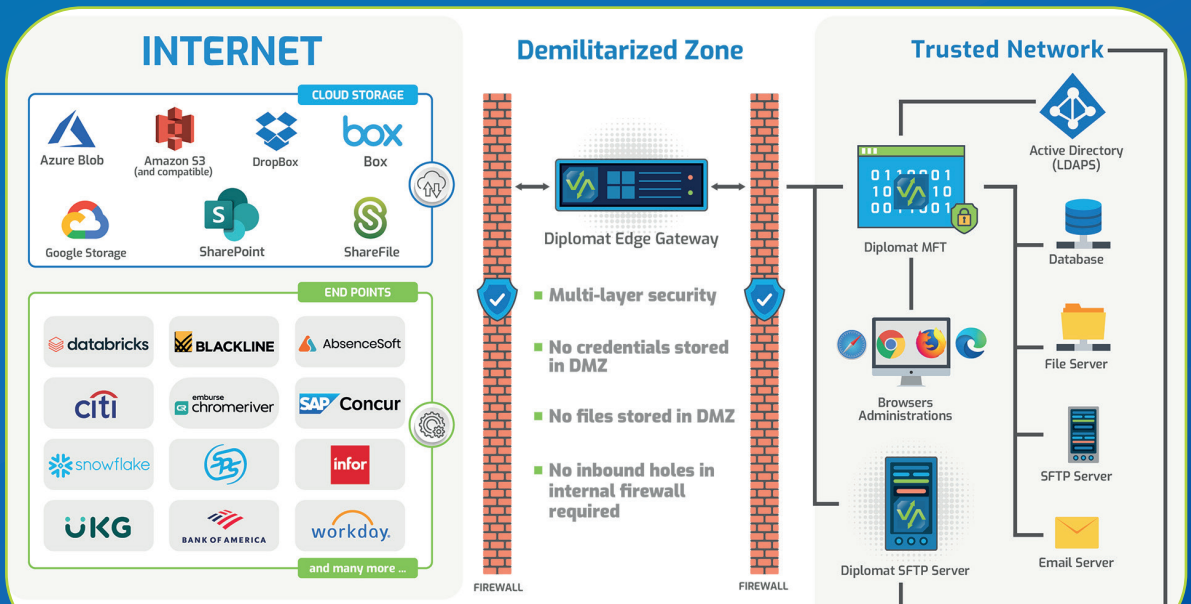

FIG. 1 – SECURE FILE TRANSFER CONFIGURATION

Step 2: Control Access

Control access to your file transfer solution. Both the FTP or web server and the managed file transfer software must be designed and implemented to limit and monitor access when setting up file transfers and when file transfer jobs are run. Limiting users, tasks, and data accessibility prevent unintended errors and makes it more difficult for outsiders to successfully breach your file transfer solution.

Set up access controls during the implementation of your managed file transfer solution to:

Protect internal communications: Most administrative consoles for FTP or web servers and managed file transfer software use client connections to communicate when setting up file transfer tasks. These client connections should be encrypted with SSL or other secure protocols.

Encrypt access data: File transfer solutions should always encrypt sensitive data at rest and only decrypt it as needed, such as when the application is started or when file transfer jobs are executed. Encryption of user IDs such as (2FA)/Multi-factor authentication (MFA), accounts, passwords, and encryption pass phrases prevents unintended use of the access information. Be careful to avoid file transfer applications that store data in plaintext, such as batch files or registry entries.

Create unique user accounts: Any user uploading or downloading files from your FTP or web server needs to be uniquely identifiable with a user ID and password. Disable anonymous connections. Require complex alphanumeric passwords that must be updated at least every 90 days. Having individual accounts for each of your business partners or other internal groups means you can swiftly shut down accounts in the event of a possible security breach. LDAPS authentication and TOTP Authentication are features that can support secure User ID access and maintains the requirements of the proposed HIPAA changes.

Limit privileges on accounts: Each new FTP or web server account creates a potential point of access to your secure file transfer solution. When setting up new accounts, strictly limit privileges based on the precise needs of each user. Restrict access to only one default directory for each account. Restrict read, write, and delete privileges based on whether the user will be sending or receiving files from your server. If possible, restrict access to a limited set of IP addresses.

Terminate inactive sessions: Each unattended administrative logon and each FTP or web session can create easy access to secure file transfer management software, as well as to data on FTP servers. Each logon should be set to automatically terminate after a specified period.

Step 3: Automate Transfers

Automate file transfers to reduce errors and limit access to sensitive information. A file transfer solution must allow you to run jobs on an automated schedule using the job scheduler of your choice. You need the flexibility to use an internal scheduler that comes with the file transfer solution, a system scheduler (e.g., Windows Scheduler), or a scheduler in a separate application to kick off file transfer jobs that integrate with your business workflow. Running jobs automatically means that you can eliminate the hit-and miss execution of file transfer jobs using a manual process. A scheduler will also streamline the compliance process by generating automated reports for file transfers. These reports can be used to demonstrate adherence to HIPAA's updated audit requirements and ensure timely reporting of incidents. Jobs run on time. Plus, the correct encryption key and logon information eliminate the possible introduction of a variety of security errors into the file transfer process.

Automated job execution means that users do not need to know sensitive access information, such as usernames, passwords, and passphrases. Each manual intervention required to complete a secure file transfer creates an opportunity for user error and for capture of sensitive passwords or passphrases. Look for file transfer solutions where access information can be entered once and used as needed at run-time.

Step 4: Authenticate Users and Process

Require user authentication. User authentication ensures that only a limited number of known users with unique privileges can access your file transfer solution. Linking authentication to each user's network or local log on identity both simplifies user authentication with a single sign-on and strengthens security by ensuring that only named users have access to file transfer set-up tasks.

Track all user activity. A file transfer solution must capture user activity data each time file transfer set-up data is changed. Knowing when file transfer set-up data was changed and who changed it provides an audit trail that simplifies the tracking and correction of problems.

Authenticate all processes making file transfer requests. When an automated process initiates a file transfer job, the process must be authenticated much like a user might need to log into an application to manually encrypt, sign, and transfer a file. Any file transfer solution needs to authenticate job processes that attempt to initiate file transfer jobs. A process that requests a file transfer job can be authenticated with a password, user ID of the process making the request, or other authentication methods.

Step 5: Encrypt Files

The updated HIPAA rules mandate stricter encryption protocols for both data at rest and in transit. Healthcare organizations must ensure all sensitive data, including electronic protected health information (ePHI), is encrypted using algorithms compliant with the National Institute of Standards and Technology (NIST).

Encrypt all files before they leave the corporate firewall. Data files should be encrypted in a secure area before transfer to an FTP or web server in the DMZ. Using secure transmission protocols only protects data in transit. As soon as files are at rest on a server in the DMZ, they are vulnerable to attack. Some FTP servers offer data encryption, but these solutions can create a security loophole by waiting until files are in an internet-accessible location before encryption.

Select a solid, widely used encryption standard, such as OpenPGP. OpenPGP is one of the oldest public key encryption technologies. Because of its popularity, many users spend time attempting to find vulnerabilities in it. And, when vulnerabilities are found, they are rapidly addressed.

Use good encryption practices. Strong encryption algorithms are important, but good encryption practices are equally valuable in decreasing the possibility of a file being breached. **Create the minimum number of keys required to meet your business needs.** If you select OpenPGP for file encryption, you have the option of using multiple encryption sub-keys with consecutive validity periods. Each new encryption sub-key provides the same security as creating a new key pair without the administrative hassle of sending a new public key to your business partners. When you create a new OpenPGP key pair, set up multiple encryption sub keys that are valid for short intervals, such as a year or less.

Step 6: Sign and Verify Files

Sign and verify files to ensure integrity and non-repudiation. Sign all outbound data files and check for valid signatures on all inbound files. Signing and verification are the best ways to guarantee nonrepudiation of origin and to ensure decrypted files are safe to process. Verifying signatures on every file ensures that the files you receive have not been altered during transit and confirms the identity of the sender.

With an encryption standard like OpenPGP, a signature is created and affixed to a file before it is encrypted in preparation for outbound transmission. The private key of the sender is used to create the signature. Without a signature, a recipient has no way to determine the sender of the file. When the file is received, the file is decrypted, and the signature can be examined before the file is processed.

Signatures are used to determine the sender of the file – as only the public key of the sender can successfully verify a signature. If the signature verification fails, then the file should not be processed. Signatures verify the integrity of files. Part of the signature contains a hash of the original file. As part of the signature verification process, the hash is recalculated using the decrypted file and compared to the hash in the original signature attached to the file. Matching hashes mean that the file has not been altered since the signature was attached. In other words, the integrity of the decrypted file has been confirmed, and it is safe to be processed.

Step 7: Use Secure Protocols

Use secure transmission protocols to protect log on data and add an extra layer of protection to encrypted files being transferred. Secure protocols protect log on data during each user access. File encryption protects your data but does not protect the log on data used to access an FTP or web server.

Secure protocols establish a secure connection with an FTP or web server before sending the log on data used to authenticate a user, such as usernames, passwords, and keys. If attackers capture log on data, they can initiate other file transfer jobs and potentially transmit files with malicious content.

Without secure transmission protocols, an encrypted file can be captured intact during transit. Once the encrypted file is in their possession, attackers can work on decrypting the file at their leisure. Using a secure protocol provides an additional layer of encryption that must be penetrated before a file is compromised.

Step 8: Archive Encrypted Files

Encrypt data files with your own master key before archiving. Archived files can be an essential component in providing the business a record of information that has been transferred. These archived files need to be equally as secure as the files that were transferred. Archival of encrypted files provides protection in case of an internal security breach, but you must be able to decrypt the archived files when they are needed. Encrypting archival copies of files to your own master key before storing them in a secure location creates a repository of secure files that are safe and meet your business needs.

Don't keep archive files that you can't decrypt. When you are encrypting files to be sent to your business partners, you use their public key. You will not be able to decrypt these encrypted files unless you also encrypt them with your own master key.

Step 9: Capture Audit Data

Audits will now focus more extensively on data transfer processes, requiring healthcare organizations to demonstrate robust controls and comprehensive logging of all file transfers involving ePHI, in the proposed HIPAA changes.

Capture audit data to demonstrate regulatory and internal audit compliance. Audit data can be used strategically to demonstrate regulatory compliance or tactically to confirm to a business partner the encryption key and destination location used by a specific file transfer job.

Proving that you have a secure file transfer process can be an arduous task. Audit data needs to be both comprehensive and easy to analyze. Your file transfer solution **needs to capture extensive data in a standard format, such as an SQL database.** Two types of audit data are critical:

Job and file data: Detailed information on each file transfer job and each file transferred can demonstrate that secure procedures, such as encrypting files before transfer and use of secure transmission protocols, were used for each file transferred.

User activity data: Data on who accessed your file transfer solution is equally as important. If files were transferred incorrectly, questions of who may have set up or updated the file transfers may become critical.

The integrity of audit data must also be ensured. If you capture audit data into files, limit the user identities that are allowed to write, alter, or delete audit files. If you use database technology, such as SQL, limit write access to the audit tables to the identity used by the file transfer management software.

Step 10: Monitor File Transfers

Monitor file transfer jobs to rapidly identify potential security problems. Automating file transfer jobs does not guarantee that no issues will arise at run-time. Your file transfer solution needs to provide real-time information. A job not running on schedule or taking too long to complete may signal a security problem.

When a file transfer job fails, the support person responsible for the job needs to be alerted as soon as possible. Email and/or paging notifications need to be sent, including the information (e.g., log entries) needed to diagnose and correct the problem.

If a security breach occurs unrelated to a file transfer (e.g., an FTP server or encryption key has been compromised), the specific file transfer jobs affected may need to be suspended until the security breach has been corrected.

Meeting Hipaa Updates

Now that you have your framework for HIPAA compliant file transfers using a managed file transfer solution, you'll be able to assess its effectiveness against the latest HIPAA mandate to ensure your organizations compliance. The key HIPAA updates are as follows:

- **Enhanced Data Encryption Standards** The updated rules mandate stricter encryption protocols for both data at rest and in transit. Healthcare organizations must ensure all sensitive data, including electronic protected health information (ePHI), is encrypted using algorithms compliant with the National Institute of Standards and Technology (NIST).
- **Real-Time Incident Reporting** Organizations will now be required to report data breaches and other security incidents to the Department of Health and Human Services (HHS) within 48 hours. This is a significant reduction from the previous 60-day notification window.
- **Increased Emphasis on Vendor Management** Covered entities must verify that all third-party vendors, including those providing MFT solutions, adhere to HIPAA's updated security and privacy standards.
- **Broader Scope of Audit Requirements** Audits will now focus more extensively on data transfer processes, requiring healthcare organizations to demonstrate robust controls and comprehensive logging of all file transfers involving ePHI.
- **Strengthened Penalties for Non-Compliance** Financial penalties for non-compliance are increasing, with additional sanctions for repeat violations or breaches resulting from negligence.

By implementing the correct framework and choosing the correct managed file transfer technology, you'll be protecting your organization from potential threats, securing your patient data and maintaining your HIPAA compliance. For examples on how Coviant Software supports healthcare organizations with their managed file transfers and HIPAA compliance, visit our case studies for **Mass General Brigham, Molina Healthcare and Christus.**

Meeting Hipaa Updates

The following figure identifies the portions of HIPAA that affect file transfer security and how the 10 Steps to managed file transfer can meet those mandates.

10 STEPS TO SECURE FILE TRANSFER IMPLEMENTATION	a)(1) Access Control Allow access only to those persons or software programs that have been granted access rights.	a)(2)(i) Unique User Identification Assign a unique name and/or number for identifying and tracking user identity.	(a)(2)(iii) Automatic Logoff Implement electronic procedures that terminate an electronic session after apredetermined time of inactivity.	(a)(2)(iv) Encryption And Decryption Implement a mechanism to encrypt and decrypt electronic protected health information.	(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.	c)(1) Integrity Property that data or information have not been altered or destroyed in an unauthorized manner.	(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.	(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.	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.	(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.	(e)(2)(ii) Encryption Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
1. Secure configuration	✓										
2. Control access	✓	✓	✓								
3. Automate transfers	✓										
4. Authenticate users/ processes	✓							✓			
5. Encrypt files				✓							✓
6. Sign and verify files						✓	✓		✓	✓	
7. Use secure protocols										✓	
8. Archive encrypted files	✓			✓							
9. Capture audit data					✓						
10. Monitor file transfers					✓						

FIG. 2 – HIPAA §164.312 TECHNICAL SAFEGUARDS

The Health Insurance Portability and Accountability Act of 1996 established national standards for the security of electronic health care information with both civil and criminal penalties for non compliance by covered entitles, such as hospitals or physician practices. The HITECH Act of 2009 extended these penalties beyond covered entities to their business associates and established more rigorous enforcement policies.

The HIPAA Security Rule in §164.312 defines the technical safeguards required to protect and control access to patient data. FIG. 2. above identifies the relevant security standards in HIPAA §164.312 and the related specifications that are necessary to protect data-in motion. You can finds out more about HIPAA technical safeguards at **http://www.cms.hhs.gov/HIPAAGenInfo.**

Summary

Changes to HIPAA signal a new era in data protection for the healthcare industry. By adopting a robust managed file transfer solution, healthcare organizations can confidently navigate these updates, ensuring the secure handling of sensitive data and maintaining compliance with the latest regulations. Investing in the right managed file transfer technology is not just about meeting regulatory requirements — it's about protecting patients and fostering trust in a digital world.

Both security and compliance are essential to smooth operations and business continuity. Developing a managed file transfer implementation can also meet the key objectives that are critical for compliance with industry mandates. Focus on the step-by-step framework to meet your security and compliance needs.

COVIANT Software

ABOUT COVIANT SOFTWARE

Coviant Software delivers secure file transfer management products that secure data in transit and improve compliance with industry and government mandates. Built on open technologies, such as OpenPGP encryption, SFTP, and SQL, Coviant's Diplomat MFT platform is an easy-to implement, cost-effective solution for automating your secure file transfer process.

If you're interested in testing Diplomat MFT as managed file transfer solution for your HIPAA compliant file transfers, you can start here for a **free-trial.**

Phone: +1 (210) 985-0985
Phone: +44 20 3970 9742 (UK)
Email: info@coviantsoftware.com

Coviant Software LLC
5804 Babcock Rd, #151
San Antonio, TX 78240