

A HEALTHY PRESCRIPTION FOR SECURE AND COMPLIANT FILE TRANSFER

GREG SHIELDS

Resident Editor, Realtime Windows Server Community

Contributing Editor, Redmond Magazine, Virtualization Review Magazine, & MCP Magazine

SPONSORED BY IPSWITCH FILE TRANSFER

ABSTRACT

With medicine, the right prescription improves your quality of life and your health. It restores strength, vitality, and a feeling of security in your future. The same holds true for your business and file transfer and record management. With a secure, reliable, and compliant file transfer solution in place, you will have confidence in your organization's ability to safeguard patient information and comply with regulatory requirements.

For healthcare organizations, data security is both an operational and regulatory imperative. A hospital or billing office that fails to protect a patient's medical records faces the threat of losing customers — whether they are patients, doctors, or other healthcare organizations — along with a tarnished reputation and the loss of competitive advantage. With increased government regulation and oversight in the form of mandates such as the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), no company that deals with patient or medical records can afford to ignore the very real challenge of ensuring data security, integrity, and privacy.

In this paper, learn more about the issues of data security, secure data transfer, and the impact of regulatory compliance to the medical industry. Only through the implementation of best practices and effective file transfer solutions can you simultaneously protect your critical patient data while fulfilling the requirements dictated by government regulations like HIPAA.

A HEALTHY PRESCRIPTION FOR SECURE AND COMPLIANT FILE TRANSFER

With medicine, the right prescription improves your quality of life and your health. It restores strength, vitality, and a feeling of security in your future. The same holds true for your business and file transfer and record management. With a secure, reliable, and compliant file transfer solution in place, you will have confidence in your organization's ability to safeguard patient information and comply with regulatory requirements.

For healthcare organizations, data security is both an operational and regulatory imperative. A hospital or billing office that fails to protect a patient's medical records faces the threat of losing customers — whether they are patients, doctors, or other healthcare organizations — along with a tarnished reputation and the loss of competitive advantage.

HIPAA requires that companies prevent unauthorized access, alteration, deletion, and transmission of electronically stored and transmitted health information.

With increased government regulation and oversight in the form of mandates such as the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), no company that deals with patient or medical records can afford to ignore the very real challenge of ensuring data security, integrity, and privacy.

HIPAA establishes U.S. standards for electronic healthcare transactions, including preserving the privacy and security of personal health records. HIPAA requires that companies prevent unauthorized access, alteration, deletion, and transmission of electronically stored and transmitted health information. Companies must be able to track and report on the access, transport, and integrity of this information.

THE RISKS OF INSECURE DATA TRANSFER

With the increasing popularity and ease of electronic storage and transfer, interest in the safety and integrity of this sensitive data is at an all-time high. Healthcare organizations have traditionally relied on a combination of FTP, email, and even instant messaging to move data among offices and business partners. While these methods are convenient, they fail to deliver security, efficiency, or reliability — all of which are critically important to today's healthcare organizations.

Although FTP, email, and IM are widely used, none of these data transfer and storage methods are appropriate for today's healthcare organizations. Standard FTP does not include strong authentication or encryption capabilities, which opens the door to the potential for data disclosure. While email and instant messaging lack scalability and use server resources inefficiently, the larger problem with these methods involves their lack of encryption and data integrity. In addition, following the receipt of records, neither email nor IM have processes for workflow, data integrity verification to make sure the entire transmission arrived untouched and uncompromised, or the ability to enforce business rules to control access to those records.

A BETTER WAY TO ENSURE PATIENT CONFIDENTIALITY

To operate effectively, healthcare organizations must replace ungoverned file transfer and storage methods with secure, reliable, and compliant information exchange processes that assure data integrity. These processes help healthcare organizations move confidential patient data between locations in a secure, accurate, controlled, and documented manner that addresses the full range of evolving legislative and regulatory mandates. These locations can be remote offices, such as hospitals, medical clinics, billing and claims agencies, insurance companies, and doctor's offices.

A secure file transfer solution enables healthcare organizations to send data more securely with return receipts and extensive tracking and auditing capabilities to ensure compliance with the FDA and HIPAA.

Two common security protocols that help secure and increase the reliability of data transfer are Secure Sockets Layer (SSL) and Secure Shell (SSH). Both are specifically designed to encrypt file transfers as well as the associated administrative network traffic. SSL and SSH enhance the security and reliability of file transfer by using encryption to protect against unauthorized viewing and modification of high-risk data during transmission across open networks such as the Internet.

Data must also be protected when it is in storage or at rest. Combining SSL and SSH security with OpenPGP provides an additional level of protection for data at rest. OpenPGP encrypts files in storage through the use of cryptographic key pairs that authenticate users and data. Receivers need to use the corresponding private key in order to decrypt the file.

MAKING SECURE FILE TRANSFER A REALITY

An effective data transfer solution must be able to ensure end-to-end security and reliability throughout the file transfer process, and provide management visibility over the process via integrated, application-level security, compliance reporting, auditing, workflow monitoring, and automation. Important features to look for in a data transfer solution include the ability to:

- Reduce the risk of providing access to healthcare data while complying with regulations such as HIPAA.
- Simplify file transfer processes to better understand, monitor, and respond to changing requirements without compromising patient confidentiality.
- Protect file transfer communications through embedded security.
- Provide robust data management, monitoring, and scheduling that includes tracking, auditing, and guaranteed delivery.

MEETING THE HEALTHCARE COMPLIANCE CHALLENGE

Many healthcare organizations are concerned about the cost of compliance. A comprehensive, proactive approach to compliance management can help reduce these costs and make it easier to manage compliance across your organization. An effective process for managing compliance should include:

- An inventory of your current data transmission and storage systems, processes, and platforms.
- Documentation of all regulated file transfer and storage processes.
- Efficient monitoring of file transfers with the ability to take corrective actions
- The ability to measure and report on results.

HIPAA compliance requires four general categories of security: confidentiality, integrity, availability, and

THE FILE PROTECTION TRIO

Confidentiality

Information that is considered to be confidential must only be accessed, used, copied, or disclosed by persons who have been authorized to do so, and only when there is a genuine need to do so. A breach of confidentiality occurs when confidential information has been, or may have been, accessed, used, copied, or disclosed to, or by, someone who was not authorized to have access to the information.

Integrity

In information security, integrity means that data cannot be created, changed, or deleted without authorization. It also means that data stored in one area is in agreement with related data stored in another area.

Availability

The concept of availability means that the information the computing systems used to process the information and the security controls used to protect the information are all available and functioning correctly when the information is needed.

Source: Wikipedia.

auditing. Each category can be specifically addressed through the right secure data transfer solution.

Confidentiality

HIPAA rule 164.132 establishes technical safeguards for authentication, access control, and privacy. You can meet these challenges with requirements for unique user IDs, automatic logoff, and strong password policies that include encryption and auto-expiration. Multiple levels of access control and administrator privileges allow access only to those people or entities that have been granted access rights. 256-bit AES cryptography and OpenPGP encryption will help to safeguard the confidentiality of health information as it's transmitted and stored electronically.

Integrity

HIPAA rule 164.132 also addresses concerns over data integrity. Health information must be protected from improper alteration or destruction and mechanisms must be in place to authenticate data integrity. The SHA-512 protocol ensures uncompromised data transfer while SSH and 256-bit AES SSL encrypt client connections to ensure that all the data sent was received without alteration or compromise. Non-repudiation takes data security to the highest level currently available by adding digital certificate management to secure delivery and data encryption. SSL certifications and SSH keys ensure that received data was sent by someone who possesses the private key corresponding to the signing certificate.

Availability

HIPAA rule 164.308 requires administrative safeguards for data backup and disaster recovery plans. Load balancing, clustering groups, and robust logging capabilities can ensure data retrieval and quick response in the event of a disaster. Also, client side, programmatic retries, checkpoint-restart, and auto-reconnect capabilities add to end-to-end high availability.

Audit

HIPAA rule 164.312 sets standards for audit controls, requiring you to implement hardware, software, and/or procedural mechanisms to record and examine activity related to the transfer of protected health information. Strong system logging that includes client-server, administration, and syslog support ensures auditable records to protect your organization.

RECOMMENDATIONS FOR SECURE HEALTHCARE FILE TRANSFER

Countless healthcare files are exchanged electronically every day. Insecure file transfer represents a significant risk to your healthcare organization. The ideal electronic file transfer solution should enable secure, reliable file transfer by providing integrated, strong security using SSL and SSH encryption along with the tools to effectively manage the file transfer process.

More importantly, focusing on security breaches distracts your organization from its core mandate of improving patient care. A reliable and secure file transfer process helps your organization safeguard patient information while complying with stringent regulatory requirements. This allows your organization to concentrate on patients, and not on data transfer.

IPSWITCH SOLUTIONS MEET THE FILE TRANSFER CHALLENGE

Ipswitch File Transfer solutions enable healthcare organizations to meet and exceed regulatory compliance and implement sound security policies by safely and reliably moving data across the Internet.

Safeguarding patient information

Ipswitch File Transfer solutions provide 256-bit AES encryption for transfers over SSL and SSH protocols — the highest commercially available encryption technology — making them the most secure solutions for healthcare organizations that require confidentiality when transferring patient information over the Internet. Ipswitch File Transfer solutions also leverage OpenPGP file encryption and SHA-512 integrity to ensure uncompromised transfers and non-repudiation.

Complying with stringent regulatory requirements

Ipswitch File Transfer's secure, automated, and reliable solutions track data access and security enforcement policies to enable a level of HIPAA compliance unrivaled by other file transfer methods. With the ability to create multiple hosts, define user access, and block IP addresses in real time, administrators can ensure that confidential data is accessible only to those with explicit permissions.

Increase ease of use and control IT operational and training costs

Ipswitch File Transfer solutions' intuitive graphical user interface is easy to configure and use, eliminating the need for expensive user and administrator training. Its secure web-based interface enables administrators to control access, define rules, and ensure enforcement from a single customizable dashboard. Silent installs and virtualization are also major cost-control mechanisms supported by Ipswitch solutions.

Improve patient care

Ipswitch File Transfer solutions' architecture scales to thousands of servers and clients — providing the server clustering and load balancing necessary to ensure the availability and performance of critical patient information and research data.

ABOUT THE AUTHOR:

Greg Shields is an independent author, speaker, and IT consultant based in Denver, Colorado. With nearly 15 years of experience in information technology, Greg has developed extensive experience in systems administration, engineering, and architecture specializing in Microsoft, Citrix, and VMware technologies. Greg is a Contributing Editor for both Redmond Magazine, Microsoft Certified Professional Magazine, and Virtualization Review Magazine authoring three regular columns along with numerous feature articles, webcasts, and white papers. He is also Resident Editor for Realtime Publishers' Windows Server Community at www.realtime-windowsserver.com.

Greg is a highly sought-after instructor and speaker, teaching system and network troubleshooting curriculum for TechMentor Events, a twice-annual IT conference, and producing computer-based training curriculum for CBT Nuggets on numerous topics. Greg is a triple Microsoft Certified Systems Engineer (MCSE) with security specialization.

ABOUT IPSWITCH FILE TRANSFER

Ipswitch File Transfer develops and markets a wide range of innovative secure and managed file transfer solutions. For over 15 years Ipswitch brands, WS_FTP® and MOVEit®, have delivered the world's most popular file transfer solutions to over 40 million users in the home, small office, home office (SOHO), small-to-medium business (SMB), mid-market and enterprise markets. **Visit www.ipswitchFT.com for more information on the Ipswitch File Transfer division and its range of products for any of your file transfer needs.**

ABOUT IPSWITCH, INC.

Ipswitch develops and markets innovative IT software that is easy to learn and use. More than 100 million people worldwide use Ipswitch software to monitor their networks with Ipswitch WhatsUp®, transfer files over the Internet using the market leading WS_FTP® and MOVEit® brands of secure and managed file transfer clients and servers and communicate via Ipswitch IMail™ Server. For product and sales information, write to info@ipswitch.com or visit <http://www.ipswitch.com>. Ipswitch values community involvement; visit <http://icare.ipswitch.com> to find out how to become involved.

Visit www.ipswitch.com for more information on the company.



Contact Ipswitch's File Transfer Division