

HIPAA COMPLIANCE

South River Technologies

CASE STUDY: SRT'S WEBDRIVE AND Cornerstone MFT HELP MEDICAL TRANSCRIPTION COMPANY BECOME HIPAA COMPLIANT

INSIDE THIS ISSUE:

South River Technologies
HIPAA Compliance
Statement 3

- 128-bit SSL encryption
- Information Access Control
- Security Configuration Management
- Termination Policy
- Internal Audit
- OTP MD5 Passwords
- Disaster Recovery

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) outlines minimum standards which need to be met to ensure the confidentiality, privacy and security of health care information in the Internet environment. HIPAA requires that health organizations that store or transfer patient data over the Internet be HIPAA compliant as of April 13, 2003.

Case Study: Med Tran, a Medical Transcription Company contacts SRT to help them initiate an effective and affordable method of satisfying government guidelines set forth by HIPAA.

Med Tran receives patient information from doctors and hospitals and out-sources part of their business to an offshore location, where the transcriptions are completed and returned to Med Tran. Med Tran then sends these files to a "verifier" who checks them and returns them to Med Tran. Med Tran then returns the files

to the individual doctor or hospital.

All of this information is being sent electronically and must have the highest level of security to protect the patient's private medical information.

SRT recommends that Med Tran install WebDrive and Cornerstone MFT to help them meet the requirements of HIPAA.

WebDrive is installed on the computers sending the patient data at the hospitals or doctors' offices. They map a drive to the directory assigned to them on the Cornerstone server at Med Tran. Once the drive is mapped, the users are working with their familiar Windows Explorer interface with no new software to learn.

The offshore transcribers also have a directory assigned to them at Med Tran where they map a drive with their WebDrive and download the assigned patient files. When they have completed their task

they transfer the files via their mapped drive back to Med Tran.

WebDrive is also installed on the Verifier's computer and a secure drive is mapped to the Cornerstone MFT server at Med Tran.



Finally, Med Tran enters the completed files in the directory assigned to the doctor or hospital for scheduled download. With patient files being sent to multiple locations, file encryption during data transfer is critical.

WebDrive and Cornerstone fully support the highest level of security (**128-bit SSL encryption**), which is mandated by HIPAA.

(continued on page 2)

CASE STUDY: SRT'S WebDrive AND Cornerstone MFT HELP MEDICAL TRANSCRIPTION COMPANY BECOME HIPAA COMPLIANT



“Cornerstone MFT is the first commercially available MFT solution for Windows that fully supports SFTP and FTPS.”

Cornerstone MFT is the first commercially available MFT server for Windows that fully supports SFTP (SSH's Secure File Transfer Protocol) and FTPS (FTP over SSL). The key benefit to SFTP is its ability to handle multiple secure file transfers over a single encrypted “pipe” or tunnel. Using a single pipe means less holes in your corporate firewall and less opportunities for unauthorized access.

Secure access to data as mandated by HIPAA can be accomplished by using the MFT server's wizard driven setup. The Administrator can easily create domains, servers, groups and users as well as configure all security options. To comply with HIPAA's requirement to **implement information access control** and for **security configuration management**, South River Technologies' WebDrive and Cornerstone MFT solution provide for:

1. *Timeout* after a selected amount of minutes from the time of the user's last activity to prevent unauthorized users viewing personal data should the authorized users leave their workstation.
2. *Account Disable* after a chosen number of incorrect passwords to prevent unauthorized users from hacking passwords.

3. *OTP MD5 encryption* for added security when using FTPS.
4. *Locking Users* in their home directory preventing them from viewing or accessing data that they are not authorized to view.
5. *Create * User groups* and granting permissions on a group basis only allowing users access to data that they are authorized to view.
6. Requiring all users to logon with their username and password by *disabling anonymous access*.
7. *128-bit SSL Security and SFTP on the server*.
8. *Require Secure Connections* refusing non-secure communication attempts.

With the Administrator feeling more confident about complying with the security requirements of HIPAA, the question of termination procedures is addressed. HIPAA requires that companies dealing with patient information have a **termination policy** in effect. With Cornerstone, the administrator can quickly disable or delete the user's account in the Account Manager or simply right click the user's name and select delete. This action will cause the user to be immediately kicked from

the system. In addition, a user's account can be set to expire on a set date.

The mandate for **Internal Audit** is met by the administrator during server setup by simply enabling *logging to file* on the Logging tab. The log will produce an audit trail displaying the user ID, the date and time of activity and the activity performed.

With the security issues resolved, the administrator sets up directories on the Cornerstone server for the offsite offices and instructs the offices which directory to map their drive to from their WebDrive client. The offices can now easily and securely transmit data back and forth.

The final issue of disaster recovery is addressed by suggesting that Med Tran contract with an independent ISP backup company to which they could map a drive using WebDrive and transfer their files securely. Not only would this meet the mandate to have outside storage of data but it would virtually eliminate the necessity of in house tape backups.

WebDrive and Cornerstone MFT solution working together effectively satisfy many of HIPAA's Security Standard requirements.

South River Technologies
2635 Riva Road
Suite 100
Annapolis, Maryland
21401
Tel: 410-266-0667
Fax: 410-266-1191
www.southrivertech.com

South River Technologies HIPAA Compliance Statement

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") outlines minimum standards which need to be met to insure the confidentiality, privacy and security of health care information in the Internet environment. HIPAA requires that health organizations that store or transfer patient data over the Internet must be HIPAA compliant as of April 13, 2003.

How are SRT's Products HIPAA Compliant ?

HIPAA requires that all health related data transferred over the Internet be done using industry standard 128-bit encryption technologies. The entire SRT product line, including WebDrive and Cornerstone MFT, fully support 128-bit SSL and SSH Public Key Encryption technologies.

WebDrive

Secure access to health care information across the Internet has become mandatory with HIPAA. WebDrive offers secure access and collaboration, without requiring users to learn a new application. WebDrive lets users access files in a way that they are already familiar with. Remote files are accessed as if they were local to the user's own workstation. Users can securely create or edit files within any Windows or DOS-based application and save them directly to the remote server. There is no separate 'upload' process required of the end user.

WebDrive helps with your HIPAA compliance by offering the following security and encryption features:

1. *FTPS (FTP over SSL)* – SSL, or Secure Sockets Layer, is a method by which an encrypted 'pipe' or tunnel is established between the FTP client and FTP server. Once the secure tunnel has been established (which is done using 128-bit encryption techniques), standard FTP is used to transfer data over the secure connection. WebDrive supports both Implicit FTPS and Explicit FTPS (AUTH SSL).
2. *SFTP (SSH's Secure File Transfer Protocol)* – Similar to FTPS, SSH's Secure File Transfer Protocol is yet another method for performing secure file transfers. One key benefit to SFTP is its ability to handle multiple secure file transfers over a single encrypted pipe (FTPS uses multiple pipes). By using a single encrypted pipe, there are less holes in your corporate firewall.
3. *S/Key OTP encryption* – WebDrive supports OTP (One-Time Password) features with MD4 and MD5 encryption.

Cornerstone MFT

Storage of electronic files and easy, secure access to those files across the Internet is a requirement for successful health care organizations. Cornerstone MFT provides the security and performance that HIPAA demands, with easy and precise configuration controls.

Cornerstone MFT helps with your HIPAA compliance by offering the following security and encryption features:

1. *FTPS (FTP over SSL)* – SSL, or Secure Sockets Layer, is a method by which an encrypted 'pipe' or tunnel is established between the FTP client and FTP server. Once the secure tunnel has been established (which is done using 128-bit encryption techniques), standard FTP is used to transfer data over the secure connection. Cornerstone supports both Implicit FTPS and Explicit FTPS (AUTH SSL). SSL's successor, TLS, or Transport Layer Security, adds an extra layer of security to the already secure SSL. Cornerstone MFT supports TLS for encrypted file transfers through Implicit FTPS and Explicit FTPS (AUTH TLS).
-

South River Technologies HIPAA Compliance Statement

2. *SFTP (SSH's Secure File Transfer Protocol)* – Similar to FTPS, SSH's Secure File Transfer Protocol is yet another method for performing secure file transfers. One key benefit to SFTP is its ability to handle multiple secure file transfers over a single encrypted pipe (FTPS uses multiple pipes). By using a single encrypted pipe, there are fewer holes in your corporate firewall. Cornerstone MFT is the first commercially available MFT server for Windows that fully supports SFTP and FTPS.
3. *S/Key OTP encryption* – Cornerstone MFT supports OTP (One-Time Password) with MD4 and MD5 encryption.
4. *Require Secure Connections* – Cornerstone also supports the ability to require all user connections to be secured. When this feature is enabled, Cornerstone will refuse access from any client that does not support FTPS or SFTP.
5. *No Anonymous Access* – Most FTP servers support the ability to have anonymous user connections. This is inherently unsecure since it becomes difficult to determine who is connecting to the server. Cornerstone features the ability to disable all anonymous access, forcing users to enter a valid username and password to securely access the server and transfer data.

The information contained in this document represents the current view of South River Technologies on the issues discussed, as of the date of publication. This White Paper is for information purposes only. SRT makes no warranties, express or implied, as to the information in this document. This White Paper may not be reproduced in any form without written permission from SRT.

Cornerstone MFT and WebDrive are U.S Registered trademarks of South River Technologies, Inc. All other trademarks are the property of their respective owners.



About South River Technologies

South River Technologies, headquartered in Annapolis, Maryland, develops file management software that is used for file collaboration, website management and shared access. SRT's unique client technology creates an instantly familiar interface by integrating seamlessly into the Windows Operating System. Founded in 1996, South River Technologies directly sells and markets Windows based utilities, and licenses its technologies to Software Publishers and Independent Software Vendors.



For more information about SRT's secure file transfer and management solutions, visit our website at <http://www.SouthRiverTechnologies.com>.