

Security Solutions for HIPAA Compliance: How WS_FTP Can Help

Whitepaper

HIPAA (The Health Insurance Portability and Accountability Act of 1996) was enacted to establish guidelines within the health care industry to ensure the privacy of patients and the physical and technical security of their medical records. This paper primarily deals with 142.308(c) and 142.308(d) of the Act. These sections deal with the technical security of patient information, and can be a difficult section to find solutions to.

A Matter of Size

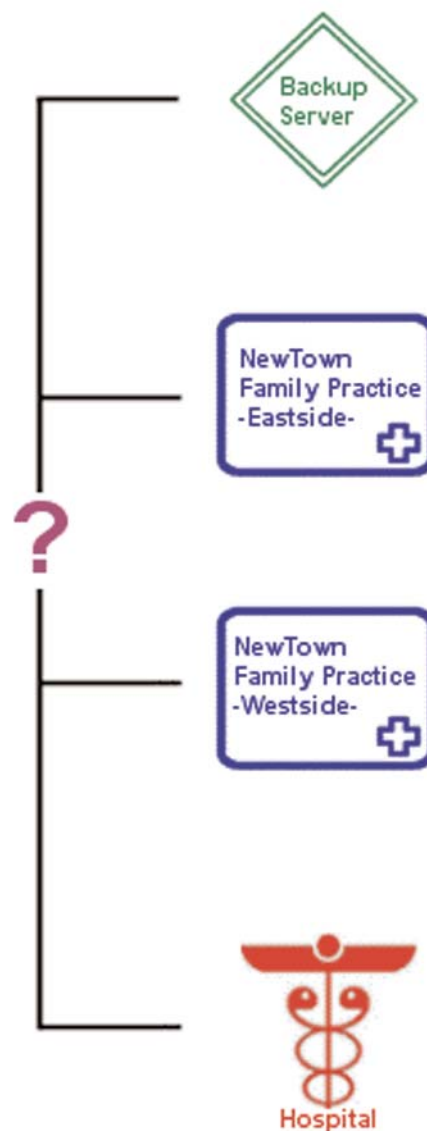
The health care industry is a large arena where many different players have to work together to serve the needs of their patients. No matter the size or organizational structure, all parties involved must follow the rules set forth by HIPAA to ensure the privacy and confidentiality of the patient's records and information. In this arena, it is the smaller practices, the smaller health plans, and community hospitals that have the greatest need for information on a cost-effective means to stay in the game. Therefore, this paper will focus on the needs of smaller businesses and private practices, and not the large HMOs and medical conglomerates.

Real Problem

In this paper, we will look at the business needs of NewTown Family Practice and their IT Manager, James. James has been assigned the duty of overseeing all of the security standards in the office as mandated by HIPAA. After seeing to and documenting the procedures for the physical security of the office, he is having trouble finding solutions for three key parts of the requirements:

Off-site back up and storage

James needs a way to electronically back up and archive all patient records for the practice. The server needs to be in a location separate from the physical files and the server for each individual office. Furthermore, James has to find a way for the files to be encrypted during the transfer from the office to the backup server, and has to have an internal audit of the transfer. Finally, these files must be readily accessible by any of the offices in the practice. This poses quite a problem, since the office only has an open internet connection between the offices and the server.

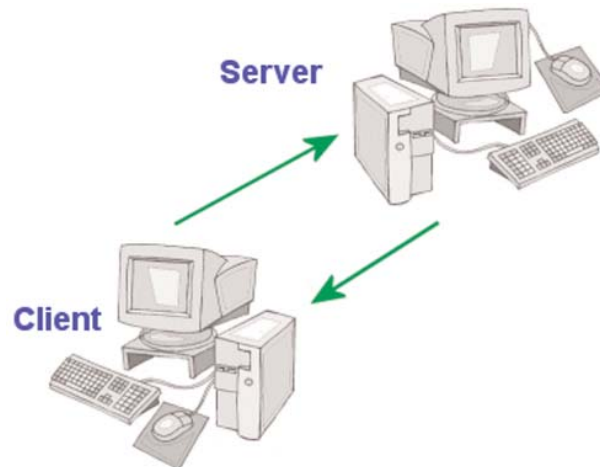


Remote access between offices and backup server

Since the two offices in the practice are located on opposite sides of the city, they need a way to quickly pass patient information back and forth between the sites. To do this, they need something that will encrypt the data, force 'entity authentication' and create an audit trail for all transactions. User authentication is making sure that the person who is accessing the secure data is who they say they are, and are authorized to access that data. James also knows that this procedure and application would be the main means of accessing the data on the backup server from remote locations.

Access control for all electronic information

In the office, there are different types of data that has to be accessed by the office personnel. Some are authorized to handle only billing and insurance information, while others need to access the complete medical records for patients. James must figure a way to put in place controls so that the different types of data can be accessed quickly, securely, and by the entity who is authorized to access a given type of information.



Real Solutions

These problems are only a part of the Security Standards of the HIPAA regulations, but they illustrate a need for software that is both flexible and affordable for the small to mid-size entity within the medical services field. Ipswitch's WS_FTP® family of software (WS_FTP Professional client and WS_FTP Server) is a long-trusted brand that has this flexibility, and if properly implemented, can solve many problems that have arisen by the HIPAA regulations, especially when used together.

Product Definitions



WS_FTP Professional

WS_FTP Professional is the market leader in Windows-based FTP (file transfer protocol) client software.



WS_FTP Server

WS_FTP Server is a full-featured securable FTP server for Windows systems. The WS_FTP Server lets you create an FTP site that makes files and folders on your PC available to other users and customers. Users can connect (via the Internet) to your site, list folders and files, and (depending on permissions) download and upload folders and files.

SSL encryption

(Secure Sockets Layer) is a way to make a secure connection from a client to a server with SSL capabilities. When an SSL connection is established, all commands and data (optionally chosen by the client) passing from one side to the other will be encrypted and can be decrypted only by the parties involved in the transfer of data.

Client? Server? What's the difference?

FTP is based on the client-server model of communication between computers: one computer runs a server program "serving up" information to other computers. The other computers, or systems, run client programs that request information and receive replies from the server. The system running the server program is an FTP server.

To access an FTP server, users must be able to connect to the Internet, Intranet, or local area network (via a modem or local area network) and an FTP client program.

An FTP client-server session establishes two connections: a control connection that stays open for the entire session and a data connection that opens and closes to transfer data such as folder listings and files to or from the server as requested by the client. Normally, the control connection occurs on port 21.

The FTP server runs continuously in the background and listens to port 21 for a connection request from an FTP client. When an FTP client requests a connection, the FTP server verifies the logon user ID and password and, if valid, it listens to this channel (control channel) for the next command.

After a user logs on, their access to the FTP host's file system is determined by permissions assigned to directories and folders.

Putting it All Together

So let's revisit the problems James has identified and determine how WS_FTP Professional and Server can be used to solve those problems.

Off-site backup and storage

James did his research and found that WS_FTP Professional and WS_FTP Server offers the highest level of security (128 bit encryption) available on the market, at an affordable price. He was able to install WS_FTP Server on their backup server, and after the initial setup, use the Server Manager to manage the operation of the server from his office several miles away. He was then able to purchase a license for twenty copies of WS_FTP Professional to install on all of the computers that were going to be accessing the patient records stored on the server.

After the installation of the server and clients, James performed the following tasks to make sure the employees could access the information they needed, that the information was encrypted, and that data they were not authorized to use was hidden from them.

Set up Site profiles. For each of the employees, James created a site profile in WS_FTP Professional that made connecting to the server quick and easy. The site profile contains the user information, the server information, and a series of options that tell the client to connect using SSL and to timeout, or log out after a certain amount of idle time. The network time out is a necessity for HIPAA compliance.

Create virtual folders. In WS_FTP Server, James created virtual folders to reference, or 'point to' folders on the backup server where the different types of patient data are stored. He was then able to set permissions on those folders to allow only certain users to gain access to those folders. He did this by setting up User Groups that the individual users were placed in. In James's case, he made a group called Insurance, and placed in it, all employees who were authorized to access insurance information but nothing else.

Establish encryption level. In both the Client and the Server, James selected the options **Use only 128-bit SSL for secure connections**. By doing that, he ensured that no client would be able to connect to the server with anything but the highest available encryption.

Internal Audit. A key part of HIPAA compliance has to do with audits of who accessed what data, and when. Through WS_FTP Server, this is done with the logging system. Once logging has been turned on, server events for all FTP hosts are logged to a file named FSyyyyymmnn.log where yyyy is the year, mm is the month, and nn is the day. This log is created daily in the Log directory specified in the Local System properties. If this option is selected, you can also select the Debug Msgs option, which will add more detailed information to the log.

Furthermore, WS_FTP Server contains a Log Analyzer that lets you parse logs for specific types of information to provide a comprehensive analysis of transfer data.

Remote access between offices and backup server

James's setup of the WS_FTP Professional clients solved the access between the server and the offices, but he needed the individual offices to share data between each other. The way the offices were previously set up, patient information was stored at the office that the patient had first visited. To be able to visit a different location of the same doctor, the patient had to wait three days for the files to be copied and hand-delivered to the office across town. This was inconvenient for both the patient and the office personnel. James's solution was simple; he purchased a copy of WS_FTP Server for each of the offices and set it up very much like he did for the backup server.

First, he set up user accounts for each of the authorized employees. Then, he set up virtual folders that pointed to the folders on the server where the data was stored. After setting permissions for those folders, he was able to limit which data was accessed by which employee. Finally, James set up new Site Profiles for each of the employees so they had only to click a link to connect to the correct server.

Access control for all electronic information

James will no longer have a problem with access control. Once he has set up WS_FTP Professional and Server as shown in the previous examples, the office will be in full compliance on all of the regulations set forth in this section of the HIPAA requirements. He has only to document each of the steps he took to ensure the security of the data and the computers used to access the data, then document the day-to-day procedures the employees must follow to remain compliant.

Just when James feels everything is ready, one of the physicians tells him that he would like to be able to access patient records from the hospital on his laptop. It doesn't take long for the IT manager to come up with a solution. He sets up a copy of WS_FTP Professional on the laptop and creates site profiles for the doctor to be able to access the information on any of the servers in their network. Now, the doctor is able to securely access patient files from anywhere he has an internal connection.

Problem Solved!

By using WS_FTP Professional and WS_FTP Server, small to mid-sized businesses can solve many of the problems presented by the HIPAA regulations in a cost-effective manner.

For information on purchasing our products, please visit our website at:
<http://www.ipswitch.com>

You may also send e-mail to sales@ipswitch.com or call (781) 676-5700

