



Internet File Management & HIPAA

*A Practical Approach towards
Responding to the Privacy Regulation of the Act*

The recent activation of the privacy requirement of the Health Insurance Portability and Accountability Act has forced all organizations which interact with patient health information to respond with improved methods for protecting and tracking this information. While most organizations have begun to address these requirements with respect to the transactional health information contained within their enterprise systems, many have not yet begun to apply compliance techniques to the unstructured file information that may reside within the many different storage locations spread throughout their enterprise.

This paper explores how Internet standards including HTTP, WebDAV and SSL can be used to provide the foundation for Internet file management based compliance solutions. In addition, it is intended to provide a basis for comparisons between traditional enterprise content management systems and today's web standards based applications so that organizations can more easily determine which solutions can best address their specific compliance requirements.

*A White Paper by James Till
Vice President of Marketing, Xythos Software, Inc.*

HIPAA's impact upon how common user data is accessed and stored may become the next significant compliance hurdle that organizations must address.

Although most healthcare organizations have already begun to respond to requirements related to the Health Insurance Portability and Accountability Act (HIPAA) with respect to patient information contained within their existing enterprise systems, many remain challenged to comply with the Act as it relates to much of their common, or unstructured file information. This information is typically not stored in enterprise databases, but instead resides in locations scattered about the enterprise, having been created by individual user applications such as word processors, spreadsheets, and email programs. Due to its decentralized nature, this information is often not secure when it's stored (consider a researcher's laptop computer for example). In addition, when this information is normally exchanged via email, it is typically unprotected or encrypted, exposing it to even greater potential risk.

The Privacy Requirement of the Act which became mandatory on April 14, 2003 will mostly be addressed through systematic improvement of an organization's information protection standards and policies. However, researchers have identified (4) areas associated with its requirements that directly impact how organizations must manage their IT infrastructure and all unstructured files containing Protected Health Information (PHI):

- User authentication and role-based authorization
- Disclosures requiring revocable authorization and logging
- Requests for copies of PHI
- Requests to amend PHI

The Act does not prescribe exactly how organizations which handle PHI must respond to these requirements, but states clearly that organizations must make substantive efforts to comply or may face penalties up to and including discontinuation of business. In an effort to assist its client's efforts to comply with the Act, Gartner Research has recommended they focus upon the following technology areas specifically related to complying with PHI security requirements:

- Centralized user authentication – typically via directory services
- Improved transport security over standard protocols
- Integrated document archive and retrieval systems – to control and audit PHI access

User Authentication

Directory services have become a commonplace mechanism for IT administrators to centrally manage user's system access, passwords, and group affiliations and typically also control their access to enterprise applications. However, directory

services have not been effective at governing access to unstructured file information stored on users systems or individually managing system access beyond the LAN environment, due primarily to user storage behavior and the absence of permission-based security protocols on the Web. Virtual private networks (VPNs) are often required for secure remote system access, but are typically deployed to manage application access instead of controlling networked file systems. The result is that unstructured PHI related files can often be inaccessible beyond the boundaries of an organization (usually the LAN) and difficult to track and audit when users resort to alternative means of exchanging this information, such as using email attachments.

Traditional document management applications are designed to utilize directory services and manage file system access at a much more granular level, but can also introduce greater system complexity and cost more than a HIPAA compliance solution may require. A simpler method to improve information access control would be to leverage an organization's standard directory services while providing secure remote file management functions, including auditing as part of the organization's own file management system. A working example may already exist in the new Internet file management protocol called Web Distributed Authoring and Versioning (WebDAV). The WebDAV extensions to HTTP (the Internet's primary language) provide a foundation for remote system access control and can simplify the challenge of managing unstructured file information throughout the organization. In fact, when WebDAV is combined with a web server's file logging and tracking capabilities the combination can provide the foundation for quite sophisticated compliance management systems.

Transport Security

HIPAA does not identify specific transmission protocols for PHI transport. However, as organizations migrate from more expensive dedicated and dial up solutions to Internet enabled solutions it is imperative that they take additional precautions to protect file information as it travels across public networks. File Transfer Protocol (FTP) is probably the best recognized method of file exchange used on the Internet today, yet it has recently been identified as the "culprit" in several well publicized security break downs. FTP implementations do not uniformly address file logging or ensure file delivery, while managing FTP servers is also notoriously problematic. The greatest risk related to the use of FTP is its relative unfamiliarity among the general user community. Its popularity among the data center crowd has never translated to general user adoption, probably due to the absence of any wide-spread GUI standard. As a result, untrained use of the system can easily lead to inaccurate and multiple transmissions of PHI, obviously defeating HIPAA compliance objectives.

Due to the inherent weaknesses of FTP, researchers such as Gartner have recommend that organizations select file transfer solutions based upon HTTP and Secure Sockets Layer (SSL) that can be accessed from within almost any desktop application or Web browser and can substantially limit security intrusions.

The use of these protocols permits pre-authentication of user identities as well as support for digital signatures and more advanced authentication schemes, if necessary. When combined with LDAP and WebDAV services, Internet enabled file transport not only permits improved system authentication and file encryption, but also improves the system's auditing functions, allowing for remote file access control, file access logging, and even automatic status change notification with certain vendors products.

Integrated Document Archive & Retrieval Systems

Vendors have been touting the benefits of enterprise document management systems (EDMS) to ensure information compliance for more than a decade, so selecting one to address HIPAA requirements would appear to be a natural choice. However, the advent of Internet standards such as WebDAV may provide organizations with greater flexibility to respond to the Act at a potentially significant cost savings when compared to traditional EDMS.

As an example, until recently organizations that needed to track large quantities of documents and control access to them to support collaborative work environments essentially had two options: either purchase an EDMS application from a commercial developer or deploy a team of experts to develop their own solution. Whichever choice they made, the core of these solutions always included a set of "library services" designed to control and monitor access to a central document or unstructured file repository. The key functions performed by these services are highlighted below:

Traditional "Library Services"

- File locking/un-locking
- File check-in/out
- File version control
- File logging
- Advanced access control
 - (read, write, delete, administer) permissions
- Automatic change notification
- Commenting/Discussions

While the demand for these core services has persisted, the traditional document management vendors have continued to add scores of new features to their applications, creating added complexity typically coupled with higher license costs. Coincidentally, the WebDAV standard has evolved to provide most of these same library services, which have now been identified by researchers as necessary to respond to the security compliance requirements associated with HIPAA.

The Xythos WebFile Server & Client and HIPAA

So, does all this mean that a WebDAV enabled file system can be used to successfully manage an organization's unstructured file information and allow it to become compliant with HIPAA privacy requirements? Probably not just by itself. A WebDAV, or Internet file management system is just a part of a complete HIPAA remediation plan to address all organizational interaction with PHI. However, an Internet file management system can be a particularly cost effective component of an enterprise wide HIPAA remediation plan when it is used to manage an organization's unstructured file information in combination with structured data management solutions and a compliant records management and file storage process.

The Xythos WebFile Server (WFS) has already been deployed by medical research teams, university hospitals and life sciences software developers and is a good example how an Internet file management system can be used to address compliance objectives. Below, we'll explore how it can be used to address key compliance requirements related to user authentication, file security and auditing.

Managing PHI Access Control

Like traditional document management systems, the WFS also can integrate with an organization's existing directory services to perform user authentication and maintain group definitions. However, the WFS takes access control management several steps further, providing comprehensive directory to single file level control for all access rights including *read*, *write*, and *share*. This permits file collaboration to take place within a securely protected environment between organizations and safely over the Internet.

Access to the WFS' file management functions can also take place entirely from within the existing applications that researchers or health care providers are already familiar with, minimizing costly training or integration requirements. In addition, web browser based system access is also provided, permitting secure access to PHI even while system users are away from their primary computer.

The Xythos WFS also provides a unique feature known as "tickets" which can allow managed access to health information between organizations where "named users" are not shared. Tickets can be used to control the number of times an outside participant may view a record and whether they can change it or simply have viewing privileges. Once users select access privileges, tickets are automatically generated by the WFS and embedded within email messages as secure links (URLs) further protecting the shared information for transmission within encrypted packets. As a result, tickets can be used as a simple method to improve the protection of PHI that is used by third parties, such as project based research teams or outsourced testing labs, where assigning permanent system IDs is not warranted.

Eliminating PHI Exposure Related to Email

Similar to FTP, email represents a significant point of HIPAA compliance exposure, particularly when it includes file attachments containing patient information. User names, passwords, and even file content are often exposed during email transmission making it virtually impossible for organizations to be certain how many times the information has been accessed or by whom. The privacy requirements of the Act now dictate that organizations must make a substantive effort to protect PHI which they exchange, as well as maintain an accurate record of all requests to access or change this information.

The key challenge in responding to this requirement of the Act is to leverage the familiarity and ubiquity of email while eliminating its inherent lack of security and auditing functionality related to email attachments. The Xythos WebFile Server begins to address this challenge by allowing file addresses to be automatically represented as URLs via access controlled sharing or its tickets function, thus protecting PHI file content. However, for users accustomed to attaching locally stored content from within their email clients such as Microsoft Outlook or Lotus Notes a more comprehensive solution is necessary.

The Xythos WebFile Client (WFC) was designed specifically to eliminate the need for users to have to send un-protected file information in the form of email attachments, even if that information does not reside within a secure file server environment. The WFC can operate transparently within an application on user's desktops transforming typical file attaching behaviors including inserting, pasting and "paper clipping" into secure file sharing behaviors. Best of all, the WFC can take full advantage of the complete list of access control functions provided by the Xythos WFS such as file-level *read*, *write*, *delete* and *administer* options providing a very high level of compliance flexibility. Just as important as being able to secure information access and transport, the WFC also performs the much needed house-keeping task of moving file information from department servers or client systems into the environments of centralized enterprise servers where information can be better protected, backed up, and uniformly managed with respect to both HIPAA compliance and an organization's records management requirements.

Improving PHI Auditing

A key component of the privacy requirement of the Act encompasses tracking and recording all requests for PHI access and any changes that are made to this information. Organizations must monitor document repositories and protect them against invalid requests as well as maintain comprehensive logs of all activity related to PHI for minimum seven year periods. Internet file management systems, such as the Xythos WebFile Server can be used to address much of these HIPAA information auditing requirements and when deployed in combination with enterprise storage resource management applications, such as those provided by EMC, IBM, and Veritas can help address the long term records management requirements of the Act as well.

The WFS itself provides integrated file logging and version control functions that can be applied to any type of health record including large scanned images. Administrators or users can set file version control to ensure that every saved version of a file is stored independently for future reference or audits. File logging permits system administrators or content originators to accurately monitor all access to a file or directory in addition to providing a record of all actions performed upon the file and at what date and time.

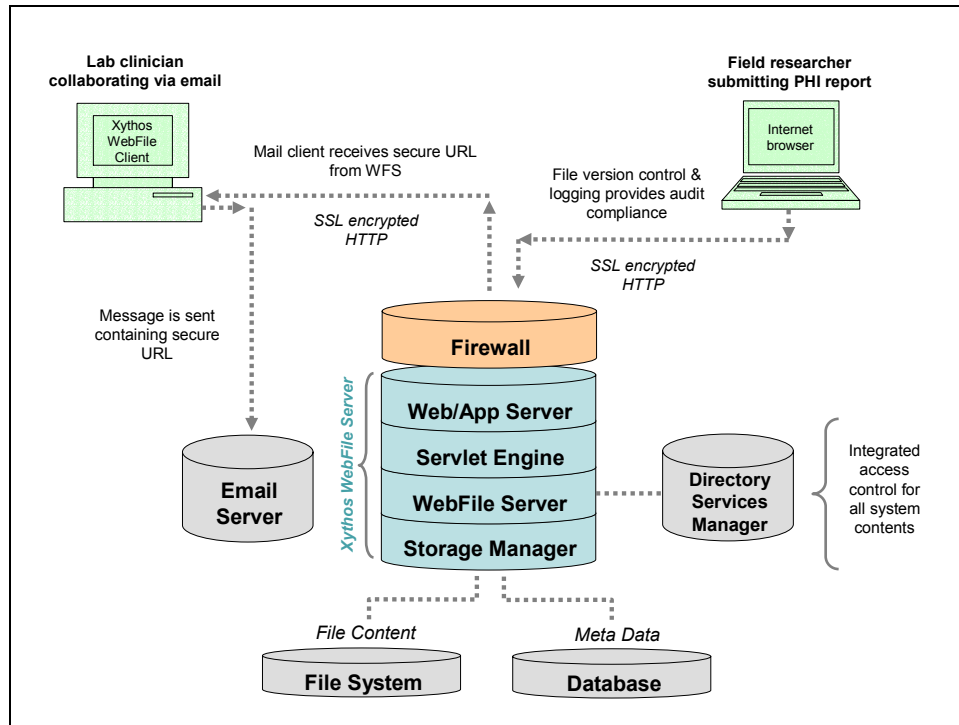
To improve system monitoring capabilities and support remote compliance management, the WFS supports automatic change status notification, providing email alerts for system administrators indicating when PHI has been requested, by whom and the exact disposition of any request. Participants can even use the integrated comments function of the WFS to discuss changes in the status of patient information, and the comments themselves can also become system alerts.

The WebFile Server System Architecture

Although HIPAA does not outline specific architectural designs for privacy compliance, organizations will want to carefully consider the impact that compliance related decisions will have upon their systems and users. A solution's ability to leverage existing investments in file server, storage and networking standards can help save substantial implementation costs. In addition, a solution's ability to scale to meet increased processing and storage requirements must be seriously considered as the size and number of PHI records continues to grow. The Xythos WFS is a practical choice for system integration due to its 100% J2EE architecture which permits it to be operated within almost any type of server environment. Its unique design also permits it to be deployed across any number of servers, allowing organizations to better utilize existing equipment and provide flexible load balancing as system demand grows.

Xythos' approach to storage management provides similar opportunities for cost saving and ease of integration. The WFS stands alone when compared to its competitors in supporting multiple database options including IBM, Microsoft, and Oracle products, essentially guarantying customers can continue to use their current database to address PHI file storage requirements. Similarly, the WFS can leverage any form of physical storage solutions including popular network attached storage (NAS) and storage area networks (SANs) to store unstructured file information. Most importantly, all of this technology remains practically invisible to system users, as it is simply integrated within their common email and desktop applications where it protects and monitors their file system use, as illustrated in the example below:

Secure file collaboration using email or direct WebFile Server connections



Conclusion

A practical plan to respond to HIPAA privacy requirements requires a systematic approach to identifying all protected health information throughout the organization so that business processes can be updated or developed to take the necessary steps towards compliance. Most healthcare organizations and associated institutions such as insurers and claims processors have already begun the necessary steps to protect their structured PHI contained within their transactional databases. However, significant areas of exposure remain related to many organizations' unstructured file information. In particular, processes related to research and development, clinical trials, and field studies should be reviewed carefully where patient information may be involved.

Organizations which adopt a standards based approach towards addressing HIPAA requirements are likely to achieve lower overall costs of compliance and minimize the disruption to their ongoing business processes. In addition, adopting an Internet standards based architecture for managing enterprise file information will better position them to respond to future security requirements, which will almost certainly evolve. The Xythos WebFile Server and Client products can provide a significant first step towards improving file system compliance with HIPAA, while eliminating the unnecessary cost and complexity associated with traditional enterprise content and document management applications.

Just as importantly, the Xythos solutions are designed to work closely together with the desktop applications and email products already used by most organizations, thus minimizing the time and costs associated with user introduction and training. For organizations planning a comprehensive response to the Act by better managing and protecting all of their enterprise information using standards based solutions, the Xythos WebFile Server and WebFile Client products are worth significant consideration.