OPEN TEXT
The Content Experts™

HIPAA: Healthcare Transformation to Electronic Communications

Open Text Fax and Document Distribution Group
May 2009

Contents

Executive Summary

The Health Insurance Portability and Accountability Act (HIPAA), enacted by U.S. Congress to improve efficiency of the healthcare system and safeguard confidential personal health information, has had a profound impact on how healthcare organizations handle personal health information. Many traditional document handling processes do not comply with HIPAA regulations for privacy and security. As a result, healthcare organizations are re-evaluating their technology systems and processes to address security and data integrity issues. One of the technologies healthcare organizations can implement to support their HIPAA compliance initiatives is LAN-based enterprise faxing and electronic document delivery. Enterprise faxing solutions provide a centralized hub for electronically sending, receiving and tracking confidential personal health information.

This white paper provides a brief overview of HIPAA regulations and how healthcare organizations are using technology to assist with compliance. It discusses network faxing, explores some of the advantages of implementing a network fax solutions to support HIPAA compliance initiatives, and introduces Open Text Fax Server, RightFax Edition as a flexible tool for improving the security and overall efficiency of document transmission processes.

PART ONE: An Introduction to HIPAA Regulations

Born as an e-commerce catalyst, experts anticipate that the 1996 Health Insurance Portability and Accountability Act (HIPAA) will transform the healthcare industry in a manner similar to ATM's transformation of the banking industry. Congress enacted HIPAA to improve the healthcare system's efficiency and effectiveness and to protect electronic health information. HIPAA calls for sweeping changes to the ways the healthcare industry uses an individual's health information and the manner in which such information is handled and transmitted.

HIPAA requires a large number of healthcare entities, including many hospitals, doctors, nurses, health plans, labs, pharmacies, and billing and claims agents, to protect the privacy of a patient's health information, particularly when communicating electronically. Healthcare organizations are likely to rely heavily on software and IT solutions to become HIPAA compliant. As one indication of the trend toward electronic transmission, on October 16, 2003, the United States Department of Health and Human Services (DHHS) required that Medicare claims be submitted in an electronic form, subject to exceptions for statutorily-defined small healthcare providers and in other limited situations.

HIPAA is impacting healthcare organizations very much like Y2K impacted other industries. Unlike Y2K, noncompliance with HIPAA requirements will result in known legal consequences. Noncompliance penalties for covered healthcare entities start at less than $100 for each noncriminal violation. Penalties escalate to $250,000 and/or 10 years in prison for criminal violations.

DHHS has regulatory oversight of HIPAA and its implementation. The Office for Civil Rights at DHHS has the enforcement authority for the privacy portion of HIPAA. The Centers for Medicare and Medicaid Services (CMS) has HIPAA enforcement authority for the security, electronic transaction standards, and code sets. HIPAA mandates the implementation of administrative and technical rules (standards) in five areas: electronic transaction standards, standard code sets for information, unique health identifiers for employers and providers, security and digital signatures, and privacy of individually identifiable health information.

So far, two pieces to the HIPAA puzzle have been finalized; transactions and code sets and privacy. Compliance for the transactions and code sets became effective in October 2002. Privacy regulation compliance was due in April 2003. In addition, DHHS has finalized standards on the unique employer identifier. Other DHHS regulatory pieces on HIPAA (i.e., security regulations, unique health identifiers for providers, and electronic signature standards) have been proposed, but are not yet finalized.

A Catalyst Toward Increased Use of Technology

Transactions and Code Sets

Federal law required all large U.S. health plans (i.e., more than $5 million in annual revenue), covered healthcare providers and healthcare clearinghouses to conduct certain administrative transactions via Electronic Data Interchange (EDI) in a single standard using uniform implementation guides by October 16, 2002 (with an extension to defer compliance until October 16, 2003). Small health plans had until October 16, 2003 to comply, even without obtaining an extension.

The law does not require information to be electronically submitted. However, if you send or receive any one of eight administrative and financial transactions electronically, HIPAA requires that you do so in a defined, standardized format. Consequently, a healthcare entity may turn to technology as a cost-effective means of addressing HIPAA requirements.

The specific types of electronic information transactions that must be transmitted by EDI standards include the following:

- Healthcare claims or equivalent encounter information
- Healthcare payment and remittance advice
- Healthcare claim status
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Coordination of benefits
- Health plan premium payments
- Referral certification and authorization

Privacy Regulations

By far the most controversial element, HIPAA covers the privacy of medical information, directly covering most providers, healthcare plans, and clearinghouses. Its protection scope follows the data through a business associate contract. Its intent is to bind agents, contractors, and business partners who receive medical information from the covered entity in order to perform functions for the covered entity. Although business associates are contractually bound to act consistently with the regulations as they are specified in the business associate contract, liability under HIPAA ultimately rests with the covered entity if it had actual knowledge of a breach and did nothing to remedy it.

Federal law specifies how covered healthcare companies can use a patient's medical records, to whom they can disclose those records and when and how patients can have access to their own healthcare records. The rule covers personally identifiable data in oral, electronic, and written form.

HIPAA does not preempt more stringent state privacy laws. Therefore, covered entities need to regularly review state law requirements. A covered entity may find compliance more efficient and effective though the use of electronic technology. The HIPAA privacy rule determines who should have access to protected data. Its intent is to protect medical records so that they are seen only by people who need that specific information and who have authority to see it.

There are several elements to the privacy requirements, including

- Permitting patients to inspect and copy their protected health information
- Designating a privacy official and training employees on safeguarding health information
- Developing methods for disclosing the minimum amount of protected information necessary to achieve a given purpose
- Establishing procedures so that only personnel with a legitimate business reason have authority to access protected health information
- Developing and using contracts that require business associates to protect the privacy of protected data
- Adopting written privacy policies and procedures
- Obtaining patient authorizations when required for the use and disclosure of health information
- Establishing boundaries on medical records use and release
- Creating and disseminating a notice that explains a covered entity's privacy practices; how health information will be used and disclosed and an individual's rights with respect to their health information
- Documenting activities with respect to health information and the measures taken to protect its privacy

Information that does not specifically identify a patient is outside HIPAA's scope. This exclusion provides a unique incentive for providers, health plans, and their business associates to assess whether personally identifiable data is needed for a particular purpose.

Security and Electronic Signature

Once DHHS takes final action, the third set of HIPAA regulations are expected to involve security and electronic signature standards. While privacy rules deal with how information is disclosed, the security rules dictate how that information must be stored and transmitted.

The anticipated rules provide a catalyst to move toward increased electronic handling of protected healthcare information. Technology can create numerous advantages for covered entities:

- Create login IDs and passwords,
- Create a more secure delivery method and verify that the message received matches the message sent,
- Create a verifiable transmission log,

- Encrypt and provide other protections for transmissions of sensitive information so that only the intended party can access the information,
- Create data backup, data restoration and continued operation of electronic data systems in the event of an emergency,
- Create one-to-one connectivity,
- Protect computer equipment from unauthorized physical access, tampering, or theft, and
- Be designed to operate from a user's computer desktop while ensuring that the computer is physically secure.

The HIPAA security provisions are designed to protect the privacy and confidentiality of patient medical information. Four security areas have been designated: administrative procedures, physical safeguards, technical security services, and technical security mechanisms. The proposed regulations also address the use of electronic signatures.

The following examples highlight how technology can change the security maze into e-commerce solutions, leading to improved business efficiencies. First, a covered entity may want to electronically send its "Notice of Privacy Practices" and obtain an electronic confirmation that the notice was received. Technology can achieve this goal. Second, a covered entity will need to protect electronically maintained health information. Yet, technology can make this information easily retrieved when it needs to be amended. Third, technology can recognize electronic signatures, allowing a covered entity to obtain authorizations through electronic means. While the proposed rules would not require the use of an electronic signature, a covered entity would be required to meet three standards when using electronic signatures:

- Assure the unaltered transmission and receipt of the message from the sender to the intended recipient,
- Contain strong evidence of the signer's identity and message integrity, and
- Verify the claimed identity of the entity using the electronic signature.

The proposed security provisions would also require covered entities to obtain a certification that the appropriate security measures have been implemented. As part of implementing its security plan, a covered entity may need to not only assess its technological systems, but also change certain practices with respect to its use of electronic transmissions. For instance, a hard copy document containing protected health information that is left on a fax or computer printer may be seen by unauthorized persons. However, if that same information were transmitted electronically, there is the potential for increased protection of that information because security measures such as login IDs or passwords would be needed to access it. Electronic transmission of information may also provide covered entities with a greater ability to direct information to the intended recipient, thus limiting the exposure of that information to unauthorized persons before it reaches its destination.

Conclusion

Given the large volume of protected information in electronic form, HIPAA privacy requirements implicate the security and integrity of technological systems and processes. Technology security will become increasingly important as covered entities use their electronic systems to comply with HIPAA regulations. Security measures can be adopted and adapted for use in the healthcare industry and will grow more relevant as the trend toward electronic storage and maintenance of protected healthcare information continues.[1]

[1] The first section of this document was created with the assistance of Cynthia Thomas, President of TriDimension Strategies, LLC and Lisa A. Genecov, a Partner with Locke Liddell & Sapp LLP.

PART TWO: Leveraging Enterprise Fax and Electronic Document Delivery to Assist with HIPAA Compliance

Introduction

One way that healthcare organizations can support their HIPAA compliance efforts is with enterprise faxing technologies. Network faxing solutions provide integrated electronic document delivery features that allow authorized users to securely and efficiently send, receive, and track confidential personal medical information from desktop, email, and back-office medical applications. This helps healthcare organizations eliminate time-consuming, error-prone, and unproductive paper handling procedures and limits exposure of personal healthcare information to unauthorized access or alteration. Using enterprise faxing technologies, healthcare organizations gain better control over workflow processes while enhancing information security and tracking through a centralized communications hub on the network.

Assessing Document Routing Inefficiencies

Dealing with large amounts of sensitive information such as patient treatment information, lab results, medical claims forms, and drug prescriptions is common in the healthcare industry. The challenge is to find an affordable solution to electronically transfer documents. Healthcare organizations should ask the following questions when choosing a solution:

- Does your organization believe that it will exchange more and more information electronically between physicians, hospitals, insurers, and patients?
- Does your organization believe that clients care more about privacy than they used to?
- How will HIPAA regulations affect the way in which your organization shares information?

After assessing how your organization routes documents, it may be surprising to find that your organization is still relying on costly manual processes such as those described below.

Scenario One: Traditional Method of Transferring Lab Results

Over the years, laboratories have tried a myriad of delivery methods to get test results to their clients. Many are costly and complex systems, but the most common method still used today is manual fax or postal mail. Manual fax may not keep patient information private and it is not a secure method of delivery. Many people handle lab results before they are even received by the patient's physician.

Scenario Two: Traditional Method of Filling and Rewriting Prescriptions

For a mail service pharmacy to fulfill a prescription, paperwork moves manually from one production area to another, from work bin to work bin, handled and re-handled by pharmacy technicians and pharmacists. When a customer or physician calls about an order during the fulfillment process, staff needs to physically track down the paperwork.

Scenario Three: Traditional Method of Processing Medical Claims Forms

Medical claim forms are received by mail, opened, date stamped, sorted, and batched by physician specialty. The forms are then keyed into a claims database and filed. The system then performs adjudication to determine the validity and proper payment of the claim and using its own logic, generates an exception report. These claims would then be manually pulled from the paper files and manually faxed to a review panel consisting of many physicians, all with different fax numbers. These claims are often routed to wrong fax machines, or claims appear illegible and have to be re-faxed and it is not uncommon to lose claims in the paper shuffle.

Automating the Routing of Private Healthcare Information (PHI)

The advantages of network faxing are numerous for healthcare organizations: a more secure, tamper-resistant delivery method, verifiable transmission log, one-to-one connectivity, and ease-of-use from the user's computer desktops.

Open Text Fax Server, RightFax Edition assists healthcare organizations with HIPAA compliance by streamlining document delivery from point of origination to final destination using authentication and certification technology. Fax Server centralizes resources across multiple systems to improve operational efficiency. It provides a cost-effective solution that acts as a central data hub for all patient billing, radiology, lab results, and standard fax traffic for the entire network, enabling hospitals and other HIPAA impacted entities to exchange documents quickly and accurately.

Hospitals, clearinghouses, and physician offices know that faxing is the most common cause of confidential information ending up at the wrong place or in the wrong hands. Think about how often patient information is left at the fax machine or sitting on a desk for anyone to see. HIPAA security regulations require faxes to be tracked carefully, especially those sent to third-party entities. The regulations require verification of the fax recipient's identity and provide ongoing monitoring of fax security practices.

While firewalls, encryption, and other technologies have made some headway in addressing security breaches from outside attackers, many internal holes still exist within organizations. Internal security breaches occur far more often than most organizations realize or are willing to admit. For example, an FBI and Computer Security Institute study found that internal data theft is far easier, more common, and presents a much greater threat to organizations than outside attacks.

Unauthorized access by insiders rose for the third straight year to more than 60 percent. Unauthorized access to protected healthcare information is more likely to occur internally rather than beyond the walls of the healthcare operator. The American Health Information Management Association (AHIMA) estimates that an average of 150 people, from doctors and nurses to lab technicians and billing clerks, may access a patient's medical record during a hospital stay.

By electronically routing PHI from the time it is received and then tracking the document through its life cycle, covered entities can limit the number of people handling and viewing sensitive information. Automating the routing of patient records reduces administrative costs and reduces the number of lost records, while keeping confidentially intact.

How Fax Server Works to Automate Document Flow

Fax Server utilizes a four-phase workflow process. This process captures any form of information, renders it into an electronic image, distributes the information via fax, email, or over the Internet, and creates customized reporting, including host notifications.

- In Phase I, Fax Server intelligently captures data in multiple formats including text files, print files, Java and XML.
- During Phase 2, Fax Server preprocesses the information into a customizable form with rules and delivery settings.
- In Phase 3, Fax Server distributes the newly assembled document to an email address, fax machine, PDA, or multifunction device.
- In Phase 4, Fax Server generates document traffic reports detailing every step in the document routing process.

Encryption and Certified Delivery of Sensitive Documents with Fax Server

Documents can be sent with Fax Server, using encrypted or certified delivery options that keep information private and secure.

Sending Documents via Certified Delivery

When a user sends a document via certified delivery, the document is not sent directly to the recipient. Instead, it is sent to the organization's Fax Server certified delivery Web site called Fax Server Secure Documents. The recipient receives an email message that indicates a certified document is available, with a link to the Fax Server certified delivery Web site.

All first time visitors to the Fax Server Secure Documents Web site must create a password upon access to the site. Each subsequent time recipients visit the site they must supply the password. Certified document recipients can change their passwords at any time.

Fax Server stores the history of each certified document so users can track when the document was sent, when it was retrieved by the user (or if it was not retrieved), and when each attachment to the certified document was viewed.

Sending Encrypted Documents

When an encrypted PDF document is sent, the recipient receives an email message with the document attached as a PDF file. Users can select to password protect the document so that the recipient is required to type in the password in order to open and view the document. The recipient will be prompted for this password each time the file is opened.

Receiving Encrypted Documents

For encrypted PDF files sent via certified delivery, the recipient must log on to the Fax Server Secure Documents Web site and download the file. The recipient must enter a password for the PDF file to gain the permissions established for the file.

For encrypted PDF files sent via email, the recipient receives the PDF as an attachment to an email message. The recipient must enter a password for the PDF file to gain the permissions that you established for the PDF file.

Document Traffic Reporting

Fax Server stores detailed information about each sent and received fax. The Fax Reporter administrative utility organizes and presents this information for reporting and billing purposes. With Fax Reporter you can:

- Create fax information reports from new and existing data sets.
- Save data sets as Microsoft Access (.MDB) files.
- Export reports to other file formats including HTML, Microsoft® Office Word, Microsoft Office Excel®, TXT, RTF and email through Microsoft MAPI or Exchange.
- Generate graphs and/or lists of fax information.

- Preview reports before printing.
- Create custom reports or use the standard report forms.

In addition, Fax Server provides advanced document-based notification options using Fax Server Production Fax, FaxUtil, FaxStat, and within Microsoft Office Outlook® and IBM Lotus Notes. These comprehensive notification features allow users to monitor their document delivery status and ensure that their documents are delivered to the right destination.

Conclusion

Whether supporting single departments or your entire organization, Open Text Fax Server, RightFax Edition can be configured to work with back-office applications such as Customer Relation Management, Enterprise Resource Planning, host, legacy, document management, and imaging systems. Fax Server is fully expandable with an upgrade path to a wide range of current and future products. Fax Server can support your HIPAA initiatives and seamlessly integrate into your network environment, making it an investment you can rely on to deliver long-term business results.

About Open Text

Open Text is a leader in Enterprise Content Management (ECM). With two decades of experience helping organizations overcome the challenges associated with managing and gaining the true value of their business content, Open Text stands unmatched in the market.

Together with our customers and partners, we are truly The Content Experts,™ supporting 46,000 organizations and millions of users in 114 countries around the globe. We know how organizations work. We have a keen understanding of how content flows throughout an enterprise, and of the business challenges that organizations face today.

It is this knowledge that gives us our unique ability to develop the richest array of tailored content management applications and solutions in the industry. Our unique and collaborative approach helps us provide guidance so that our customers can effectively address business challenges and leverage content to drive growth, mitigate risk, increase brand equity, automate processes, manage compliance, and generate competitive advantage. Organizations can trust the management of their vital business content to Open Text, The Content Experts.

http://faxsolutions.opentext.com

Sales: captaris.sales@opentext.com
+1-800-304-2727

Support: support@opentext.com
+1-800-540-7292