WHITE PAPER

HIPAA: Health Care Transformation to Electronic Communications

A White Paper Commissioned by Captaris,Inc.
By Cynthia Thomas and Lisa A. Genecov*

TABLE OF CONTENTS

INTRODUCTION

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

HIPAA requires a large number of health care entities, including many hospitals, doctors, 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, beginning on October 16, 2003, the United States Department of Health and Human Services (DHHS) will require that Medicare claims be submitted in an electronic form, subject to exceptions for statutorily-defined small health care providers and in other limited situations.

Some have referred to HIPAA as Y2K on steroids. Unlike Y2K, noncompliance with HIPAA requirements will result in known legal consequences. Noncompliance penalties for covered health care entities start at not more than $100 for each non-criminal 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 takes effect in October 2002. Privacy regulation compliance is due 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 requires all large U.S. health plans (i.e., over $5 million in annual revenue), covered health care providers and health care clearinghouses to be able to conduct certain administrative transactions via electronic data interchange (EDI) in a single standard using uniform implementation guides by October 16, 2002. An extension may be obtained to defer compliance until October 16, 2003. Small health plans have 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 health care 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:

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Health care 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, health care 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 health care 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 health care 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 health care information. Technology can create numerous advantages for covered entities.

Technology can:

- 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 a one-to-one connectivity
- Protect computer equipment from unauthorized physical access, tampering or theft
- 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 the integrity of the message
- 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.

CONCLUSIONS

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 health care industry and will grow more relevant as the trend towards electronic storage and maintenance of protected health care information continues.

Cynthia Thomas is the president of TriDimension Strategies, LLC, a public policy consulting firm. Lisa A. Genecov is a Partner with Locke Liddell & Sapp LLP, a corporate and commercial law firm.

Legal Disclaimer: This paper is for general informational purposes only and does not represent legal advice or a legal opinion. Because of its generality, it may not be applicable to your specific situation. For legal advice, you should consult with legal counsel regarding your own particular legal needs. This paper is current as of October 1, 2002.

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 health care industry. The challenge is to find affordable solutions to electronically transfer documents. Health care organizations should ask the following questions to determine the best approach to secure the transfer of patient information:

- Does your organization believe that it will exchange more and more information electronically between physicians, hospitals, insurers and patients?
- Does your organization believe that consumers 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. Lab results are handled by many people before it is even received by the patient's physician.

RightFax e-Document Delivery Solution:

When doctors send their patients to hospitals for blood tests or x-rays, the results pass through a radiology or lab system, the forms are converted into a TIFF file and can be emailed directly to the doctors' offices. Patient information is kept confidential as access to the information is encrypted through RightFax SecureDocs. RightFax sends test orders with electronically logged-in samples, combining data from the verification of results into one report and then electronically transfers test results. The test results can be disseminated and delivered much more quickly, thereby providing doctors and their patients with better service, faster results and, potentially greater peace of mind.

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 and 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 physically track down the paperwork.

RightFax e-Document Delivery Solution:
RightFax receives prescriptions from the doctor's office through its fax server system and then routes to the mainframe order processing system at the pharmacy. RightFax then converts all prescriptions into standard TIFF format, which can be stored, retrieved or transferred electronically to another entity quickly and accurately. This process ensures that the orders are confidentially received and processed and provides the pharmacy with a record of all transactions. Thus, paper is eliminated and data tracking is improved.

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.

RightFax e-Document Delivery Solution:
Forms are scanned for image archiving and sent to an archival database for electronic routing, preventing documentation loss. RightFax integrates to the forms processing database and routes the claims to the desktop email. The process now tracks when claims are sent to physicians and hospital administrators. When a claim needs to be pulled for review, instead of searching through paper files, the image can be quickly located and routed by RightFax to a printer.

ADVANTAGES OF AUTOMATING THE ROUTING OF PRIVATE HEALTH CARE INFORMATION (PHI)

The advantages of network faxing are numerous for health care operators: a more secure delivery method than email, verifiable transmission log, one-to-one connectivity and ease-of-use from the user's computer desktops.

Captaris solutions assist health care operators with HIPAA compliance by streamlining document delivery from point of origination to final destination using authentication and certification technology to secure data. RightFax centralizes resources across multiple systems to improve operational efficiency. RightFax 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 desktop for anyone to see. HIPAA security regulations will require faxes to be tracked carefully, especially those sent to third party entities. The regulations will require verification of the identity of the person receiving the fax 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, a 1999 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 health care information is more likely to occur internally rather than beyond the walls of the health care 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 CAPTARIS RIGHTFAX WORKS TO AUTOMATE DOCUMENT FLOW

RightFax 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, RightFax acts as an intelligent scanner and captures data in multiple formats including text files, Java and XML
- During Phase 2, RightFax assembles the information into a customizable form
- In Phase 3, RightFax distributes the new document that has been assembled to email addresses, fax machines, PDAs and multi-function copiers
- In phase 4, RightFax generates document traffic reports detailing every step in the document routing process

When documents are sent with RightFax, the SecureDocs module keeps information private and secure.

Encryption and Certified Delivery of Sensitive Documents with RightFax

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 RightFax SecureDocs certified delivery Web site. The recipient receives an email message that indicates that a certified document is available with a link to the SecureDocs Web site.

All first time visitors to the SecureDocs certified delivery 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.

RightFax 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. Adobe Acrobat, the program used to view PDF files, will prompt the recipient for this password each time the file is opened.

Receiving Encrypted Documents

For a recipient to open any PDF file, he or she must have Adobe Acrobat Reader installed on his or her computer. This application is available for free at the Adobe Web site.

For encrypted PDF files sent via certified delivery, the recipient must log on to the SecureDocs Web site and then 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 e-mail, 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

RightFax 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, Word, Excel, TXT, RTF and e-mail through MAPI/Exchange
- Generate graphs and/or lists of fax information

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

Whether supporting single departments or your entire organization, RightFax can be configured to work with back-office applications like CRM, ERP, host, legacy, document management and imaging systems to meet your unique requirements. It is fully expandable, with an upgrade path to a wide range of current and future products. Because RightFax can support your HIPAA initiatives, your technology is protected well into the future, all with seamless integration into your operation, all at a level of optimum cost-efficiency.

RightFax is certified with companies including Microsoft, Lotus/IBM, SAP, Oracle, FileNet, Siebel and Xerox. With over 35,000 installations across the globe and the largest share of the market at 24% (source: IDC 2001), RightFax is installed in 80% of the Fortune 100 companies.

FOR MORE INFORMATION

Captaris is a leading provider of unified communications and mobile business solutions and home to some of the most recognized product brands in the business communications industry including RightFax, CallXpress, MediaLinq and Infinite. Captaris gives you the freedom to conduct business at anytime, from anywhere and the control to manage the information you need, when you need it. Captaris keeps business within your reach. For more information please contact us at: **www.Captaris.com** or 1.888.320.7778. Outside of the U.S. please call +1 520.320.7000.