White Paper

DIGITECH AND HIPAA COMPLIANCE

April 2004

As HIPAA compliance becomes mandatory, Digitech Systems continues to proactively address the unique needs of the Health Care market. PaperVision® Enterprise is an affordable, easy to use document and content management solution that provides powerful tools to help the healthcare provider address the concerns of a HIPAA-compliant environment. These compliance benefits are also available with ImageSilo® our online document and content management system.

Digitech Systems

Overview

When Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996, they set forth various provisions for the privacy of protected health information (PHI) during diagnosis, treatment, and billing for medical issues. As a result of this regulation, the U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to guide healthcare providers through the implementation of HIPAA-compliant processes and procedures.

Digitech Systems offers a comprehensive document and content management solution that assists healthcare providers in building and maintaining HIPAA-compliant practices within their organizations. Digitech's PaperVision Enterprise and ImageSilo include powerful disclosure tracking, de-identification, and document security features to ensure the privacy of health-related information. With PaperVision Enterprise or ImageSilo, HIPAA-compliant procedures can be quickly and easily integrated into the normal routine.

The Market

A sizeable opportunity

First Consulting Group, in a study prepared for the American Hospital Association, estimates that the Health Care industry will spend up to $22.5 billion on electronic document and content management solutions between 2001-2005. As clarifications continue to emerge regarding HIPAA , the HHS Privacy Rule and the HHS Security rule, which extend the protections of the Privacy Rule to electronic transmission of health information, experts expect that spending will continue to increase.

ARMA International has stated, "Most healthcare organizations must comply with HIPAA's Privacy Rule by April 14, 2003, but many other organizations, including a large number of employers, also will be affected by this rule. In fact, HIPAA's Privacy Rule will impact, at least indirectly, all organizations in some way." (www.arma.org) Whether through increased security on electronic transmission of health-related information (Security Rule compliance required by April 21, 2005) or policy changes affecting how information is processed, organizations that deal with protected health information in any form, will be impacted by HIPAA. These organizations are looking for a document and content management solution that will best address the concerns identified by the Privacy Rule.

In addition to protecting confidential patient information, the Privacy Rule was designed to encourage adoption of secure, effective electronic document and content management practices in the Health Care industry. As these systems are implemented, healthcare providers will realize tremendous benefits including all of the following.

- Reduces costs associated with filing and retrieving patient information.

- Improves efficiency as documents can be automatically routed through any organizational process including admissions, billing, collections, and interactions with insurance providers.

- Enhances security because of electronic audit tracking—no more paper documents which are susceptible to misplacement and loss

- Protects patient privacy resulting in improved patient confidence

> *"…HIPAA's Privacy Rule will impact, at least indirectly, all organizations in some way."*
>
> *~ARMA International The Association for Information Management Professionals*

- Speeds Explanation of Benefits (EOB) and collections processes through real-time access to electronic records and information, providing significant improvement in cash flow through reduced days payable
- Helps healthcare provider avoid fines and litigation associated with noncompliance.

In addition to the benefits that come from HIPAA compliance, the healthcare provider can realize tremendous cost savings, streamline organizational processes, and improve document security and storage through the use of an effective document and content management system. Clearly, there is tremendous motivation to adopt document and content management, and the pressure is on as the April 2005 deadline looms. In fact, AHANews indicates that improving security to comply with HIPAA is one of CIO's top two priorities in 2004. ("CIOs rate security, patient safety as top priorities for '04, HIMSS survey finds," *AHANews.com* Feb 23, 2004)

Selecting the best solution

With all of this potential, healthcare providers will take care in selecting the best electronic document and content management solution for their organization. Five key areas of concern include disclosure tracking, protected disclosure, de-identification of protected information, patient disclosure authorizations, and generally protecting the security and privacy of personally identifiable electronic health information as it routes through the processes of diagnosing, treating, and billing individuals for health-related issues.

Disclosure tracking—HIPAA regulations require that the healthcare provider track disclosures of personally identifiable health information to any internal or third party. This includes doctors, insurance providers, billing and claims processing, and all other entities that might have reason to view the information.

Protected Disclosure—The Privacy Rule allows for certain types of disclosures that do not require authorization from the patient. These include 1) to the individual, 2) treatment, payment, and health care operations, 3) disclosures with the opportunity to object, 4) incidental use, 5) public interest and benefit activities, and 6) release of a limited data set. There is specific information that must be captured for each disclosure, and, in some situations, only a subset of the patient's record may be disclosed.

De-identification—There are no restrictions on the use of de-identified health information, and much of this type of information is used by the government, researchers, and health organizations in compiling statistics. De-identification requires the user to strip all personally identifiable information (i.e., patient name, identity number, address, etc.) from the health document before it is passed on.

Patient Authorization—A healthcare provider may not disclose PHI outside the scope of the HIPAA regulations without written authorization from the patient. This authorization must be obtained, recorded, and then maintained for a period of at least six years. In general, authorizations should be specific as to the information being disclosed, the person disclosing and receiving the information, expiration, etc., so a separate authorization is often required for each disclosure.

Security—The Security Rule portion of the HIPAA regulations applies to the transmission of electronic protected health information (EPHI). The healthcare provider is to ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits.

Digitech's Solution

HIPAA-enabling functionality

PaperVision Enterprise and ImageSilo are flexible document and content management solutions that will significantly assist any healthcare organization in attaining HIPAA compliance. With their powerful feature set, PaperVision and ImageSilo address the specific concerns brought to the forefront by the Privacy Rule changes in the Health Care industry. The table below matches key features and benefits provided by PaperVision Enterprise and ImageSilo with the specific HIPAA concerns they help to address.

HIPAA Concern	PaperVision Enterprise/ ImageSilo Feature	Advantage/Benefit
Disclosure Tracking	Enhanced Auditing	Force user to track critical information about every disclosure including a general purpose disclosure reason.
Disclosure Tracking	Manual Disclosures	Patient data released during a phone call or in office consultation can be tracked quickly and easily
Disclosure Tracking	Document Grants	Documents can be posted to a secure, web-accessible location combined with password security for disclosure to out-of-office parties.
Protected Disclosure	Email Auditing	Emails sent from the system are recorded in the system reports and the system can be configured to force a disclosure reason to be entered prior to sending the email.
Protected Disclosure	WorkFlow	Can restrict security levels to allow individuals to only see only the portions of a patient's information that they need to perform their function.
Protected Disclosure	Document-level Security	Specific records can be filtered for viewing by specific individuals only.
De-identification	Redaction	User-level settings control whether or not a user can turn off redactions to reveal PHI.
De-identification	Redaction	Set redaction colors and styles so de-identified portions of a document blend seamlessly

PaperVision Enterprise and ImageSilo quickly and easily address major areas of compliance concern including disclosure tracking, de-identification, and the security of protected health information.

		into the background.
De-identification	WYSIWYG Email and Printing	Redactions remain in place when emailing and printing
Patient Authorizations	Imaging and Retrieval	Scan and store every copy of a patient's disclosure authorization form in a readily-accessible format from any location, anytime, anywhere.
Security	System Operations/Queries and Utilization Reports	Tracks each activity performed by any user accessing the system. See this information displayed by user or by date/time stamp.
Security	System Operation/Queries	Tracks not only activities successfully completed by the user, but all activities they tried to perform such as looking up a patient record. Allows the administrator to audit individual user activity for anything that is suspicious.
Security	User-level Security	Setup user accounts to restrict the functions users have access to, such as email, printing, or annotations.
Security	Document-level Security Audits	Perform security audits for individual documents. Provide a full listing of every access to and operation performed on the document.
Security	Back-end Patient Data	Secure, airtight document storage can easily be configured to allow access to the database and electronic document storage only through 128-bit encrypted caching technologies, so your database and document storage are never fully exposed to an end-user.

In addition to these HIPAA-specific features, PaperVision Enterprise and ImageSilo are robust, scalable, feature-rich document and content management systems that will simplify document management needs in any organization while saving them money. Powerful search and retrieval capabilities allow a user to access any document in the system, from any workstation, at anytime. An Application Programming Interface (API) toolkit, included at no extra cost, allows the system to easily integrate with other business critical systems already in place. Additionally, the basic system can be deployed in a

matter of hours—not days or weeks like many other electronic document and content management systems. PaperVision Enterprise and ImageSilo not only enable HIPAA compliance, but also can save a healthcare organization time and money.

Vocabulary and Terminology

Authorization

Written permission from a patient that allows a healthcare provider to disclose PHI in a manner not covered by HIPAA. The authorization must be in plain language and specific to the reason for the disclosure, the receiving party, and should include an expiration date.

Covered Entity

Under HIPAA, this is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

De-Identification

The removal of personally identifiable health information from a patient record.

Disclosure

A release of information out of the document and content management system to a third party through email, document grants, export, print, or fax.

Electronic Medical Record (EMR)

The Electronic file containing all of a patients medical documents.

Explanation of Benefits (EOB)

Used by an insurance provider to clarify and explain the covered and non-covered benefits provided during a claim.

Health Care Clearinghouse

A public or private entity that does either of the following 1) Processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; 2) Receives a standard transaction from another entity and processes or facilitates the processing of information into nonstandard format or nonstandard data content for a receiving entity.

HHS OCR

United States federal government's Department of Health and Human Services' Office for Civil Rights. Has authority for overseeing and enforcing the Privacy Rule.

HIPAA

A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and

employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191.

Privacy Rule

A set of national standards for the protection of protected health information; a subset of HIPAA. Addresses the use and disclosure of individuals' health information by organizations. Sets standards for each individual's right to understand and control how their health information is used.

Protected Health Information (PHI)

Individually identifiable health information. Also Electronic Protected Health Information (EPHI)

Security Rule

Applies to electronic protected health information, however it is transmitted or stored; a subset of HIPAA.

Digitech Systems

ABOUT US

Digitech Systems, Inc. is a recognized leader in the development of software and services in the document management industry. We are committed to bringing the prospect of *any document ✆ anywhere ✆ anytime™* to an affordable reality. Digitech Systems, Inc. is headquartered in suburban Denver, CO. The software products provide affordable document and content management to organizations of any size. Three primary products include PaperFlow™ for image capture, PaperVision® Enterprise for document and content management, and ImageSilo® for secure off-site electronic document and content storage and retrieval. The line can be purchased as a fully integrated suite, or as process specific components. Ease-of-installation, extensive functionality, architectural flexibility, low price points and legendary toll free customer and technical support distinguish Digitech in the marketplace. For more information, or to obtain a free software demo CD, visit www.digitechsystems.com.

CONTACT INFORMATION

Digitech Systems, Inc.
8400 East Crescent Parkway, Suite 600
Greenwood Village, CO 80111
Tollfree: 866.374.3569
Email: Sales@digitechsystems.com
www.digitechsystems.com

Digitech Systems