

# Compliance Brief: HIPAA



## Improve Medical Records Efficiency and Security

*The federal government issued the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, in 1996 to improve the security and efficiency of the healthcare system. HIPAA sets standards for the electronic exchange of healthcare data, regulates the security and privacy of personally identifiable healthcare information and requires providers to use national identification systems for healthcare patients, providers, payers and employers. HIPAA rules were designed to encourage adoption of secure Enterprise Content Management (ECM) practices in the healthcare industry.*

### Applicability

About 545,000 entities make up the healthcare industry. Healthcare providers, insurance companies and anyone who handles medical information must comply with HIPAA regulations. This includes employers and everyone who collects or has access to Protected Health Information (PHI).

### Healthcare Impact

Healthcare providers must adopt national standards for electronic healthcare transactions. The Privacy Rule requires companies to protect and track disclosures and remove PHI from records before they are shared. The Security Rule outlines administrative, physical and technical safeguards for electronic PHI. Although the most burdening deadlines passed in 2003 and 2005, recent reports state many companies are still struggling with compliance. Noncompliance can result in civil penalties of up to \$25,000 per violation and criminal penalties of up to \$250,000 and 10 years in prison. Consequently, healthcare IT priorities continue to concentrate on:

- Data security for patient privacy and confidentiality.
- Compliant disclosure processes.
- System activity monitoring and disaster recovery.

*If HIPAA compliance is not news per se, the need for security and streamlined healthcare communications definitely is, according to the Health Information and Management Systems Society and the Phoenix Health Systems. In fact, their U.S. Healthcare Industry HIPAA Compliance Survey results state any hospital director of information systems, medical records or the business office will tell us today that HIPAA, as a facilitator of information security and efficient electronic transactions, is an increasingly significant factor in everyday healthcare.*

### ECM Enables HIPAA Compliance

ECM technology provides document and system security that acts as a means for unified compliance and operational efficiency. Many hospitals, doctor's offices and other companies use Digitech Systems' solutions to address HIPAA privacy and security regulations. PaperVision® Enterprise, on-premise ECM, and ImageSilo®, our on-demand ECM service, are affordable, easy-to-integrate systems that also help healthcare companies reduce records management costs and enhance productivity.

The following PaperVision Enterprise and ImageSilo capabilities assist healthcare providers in building and maintaining HIPAA-compliant practices, while saving money and time.

### Data Security for Patient Privacy and Confidentiality

Healthcare providers must ensure the confidentiality, integrity and availability of all electronic PHI created, received, maintained or transmitted. ECM systems must be protected from intrusion, and companies must create procedures for clearly identifying those who need access to protected information. Both ImageSilo and PaperVision Enterprise provide the tools to address these compliance concerns.

- 256-bit AES data encryption can occur both during transmission and while data is stored, protecting PHI at every step.
- Login security settings require all session activity to come from the original login, and additional security protects the flow of information over public networks.
- Extensive security settings allow you to restrict access by project, document and index field to ensure doctors and billing processors view only the information necessary for the task.

### Compliant Disclosure Processes

HIPAA regulations require healthcare providers to track and document all disclosures of PHI to any internal or external party. De-identification requires companies to strip all PHI from a document before it can be shared. Healthcare providers use Digitech Systems' disclosure tracking technologies to enforce strict policies and procedures for sharing patient information.

- Redaction hides PHI to de-identify records and protect patient privacy when a document is shared.
- Enhanced auditing restricts information sharing to a pre-approved list of recipients and records every disclosure, including who received information, when and how.
- Document grants allow secure, temporary, web-based information access for external parties, such as insurance providers and outside practices.

### System Activity Monitoring and Disaster Recovery

HIPAA requires companies to identify data backup methods and review operations routinely to identify potential security violations. Healthcare providers must ensure information has not been changed or erased in an unauthorized manner. Extensive security settings, system reporting features and disaster recovery tools can be included with ImageSilo and PaperVision Enterprise and enable HIPAA compliance.

- The system tracks all user activity, including successfully completed, attempted or suspicious activities, such as trying to open protected records without security clearance.
- Unalterable logs show who accessed which pieces of information and provide documented evidence of HIPAA controls.
- Backup processing and data replication ensure information availability.