The Role of Document Management in Complying with HIPAA's Security Rule

A Guide for Small- and Medium-Sized Businesses

EPSON®
EXCEED YOUR VISION

Contents

Executive Summary

Executive Summary

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 has been one of the most influential pieces of legislation on the healthcare industry. HIPAA's initial purpose was to anticipate the digitization of healthcare data and communications by codifying standards for electronic transactions. It eventually expanded to require healthcare entities to protect patient privacy (i.e., the Privacy Rule), secure patients' protected health information (PHI) (i.e., the Security Rule), and to notify patients in the event of a breach of PHI (i.e., the Breach Notification Rule). HIPAA is therefore not a single law or rule, but a "suite of regulations" that apply to two types of organizations: covered entities (CEs) and business associates (BAs), which HIPAA carefully defines.

HIPAA's Security Rule applies equally to CEs and BAs. It requires the implementation of administrative, physical, and technical safeguards in order to maintain the confidentiality, integrity, and availability (CIA) of patients' PHI. CEs and BAs are greatly aided in complying with the Security Rule by implementing a document management solution (DMS). A DMS is a hybrid software-hardware solution that assists in the creation, storage, transmission, and security of electronic health records (EHRs). EHRs often contain PHI, such as patient medical records and billing information, in electronic format. Common DMS features map to the Security Rule's safeguards. In turn, the administrative, technical, and physical controls or safeguards contribute to the CIA of patient PHI.

This paper aims to:

- Summarize HIPAA's privacy and security regulatory requirements, define who must comply, and outline how to comply – with a focus on the Security Rule
- Introduce the Security Rule's required safeguards and how they enable the CIA of patient PHI
- Explain how common DMS features map to the Security Rule's safeguards and therefore aid in compliance
- Provide guidance on evaluating DMS features and planning for DMS deployment

Part 1

HIPAA: An Old Law Now as Important as Ever

In the mid-1990s, managing documentation was a primary challenge in the healthcare industry. It was clear to industry experts and regulators that the future of healthcare documentation and communication would be digital. Within this context, the U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The original legislation's goal was to "modernize the flow of health information" by "creat[ing] a set of uniform electronic healthcare transaction codes" [1]. Even in HIPAA's nascent stages, patient privacy and the security of patient data were primary concerns of those crafting the legislation, yet how to mandate and regulate the privacy and security of healthcare data was controversial [1]. It would take the U.S. Congress another four years to pass the Privacy Rule and another seven years to pass the Security Rule. Significant updates to the legislation, including stricter enforcement provisions and the Data Breach Notification provision, were passed in 2009.

Today, managing documentation in a way that protects patients' privacy and ensures data security is still a primary challenge industry-wide. The difficulty is illustrated by an endless flow of news stories about data breaches inflicting the healthcare industry. Multiple, large-scale breaches of protected health information (PHI) have impacted several major providers within the past year. (Refer to Figure 1 for a summary of recent major healthcare-related breaches.) Privacy Rights Clearinghouse reports that 361 healthcare industry data breaches have been reported publicly from January 2014 to June 1, 2015 [2]. Many of these smaller breaches still involved thousands or tens of thousands of records containing patients' PHI. In some cases, the total number of records stolen, lost, or destroyed is still unclear. Together, these breaches have affected millions of healthcare providers, support businesses, and patients, yet these are just the breaches that have been discovered and reported. These breaches serve as a constant reminder of the importance of implementing the proper security and privacy safeguards mandated by HIPAA.

Figure 1. Recent Major Breaches Involving Health-Related Data

Source: Privacy Rights Clearinghouse

As with many complex laws, understanding HIPAA's regulatory requirements, who must comply, and how they must comply can be challenging. HIPAA is not one law or rule, but "a suite of regulations" that affect two primary types of entities [3]. HIPAA is comprised of three primary rules that mandate privacy and security requirements, which include the following [3].

- ***Privacy Rule*** – protects patients' PHI
- ***Security Rule*** – outlines national standards for securing electronic PHI
- ***Breach Notification Rule*** – requires entities to notify patients following a breach of PHI

Two types of healthcare entities are required to comply with HIPAA's three privacy/security rules. These include the following [3].

- ***Covered Entities (CEs)*** – Defined by HIPAA as any healthcare provider that bills electronically, in addition to administrators of health plans and health clearinghouses. Examples of CEs include doctors, clinics, hospitals, nursing homes, and pharmacies.
- ***Business Associates (BAs)*** – Defined by HIPAA as any entity or individual not employed by a CE, but who has access to PHI. Examples of BAs include health information organizations/ exchanges, e-prescribing gateways, other providers of data services that entail transmission of PHI, and subcontractors who access PHI.

Table 1 summarizes each type of entity's compliance requirements by HIPAA rule. However, fully detailing these requirements is beyond the scope of this paper. For more information, readers are referred to the U.S. Department of Health and Human Service's publication entitled "Guide to Privacy and Security of Electronic Health Information," which is cited at the end of this paper.

Table 1. Summary of Who Must Comply with HIPAA's Privacy/Security Rules

	Privacy Rule	Security Rule	Breach Notification Rule
Covered Entities (CEs)	Yes	Yes	Yes
Business Associates (BAs)	Yes, certain provisions	Yes	Yes

The remainder of this paper focuses on the Security Rule requirements for CEs and BAs.

Part 2

Diving Deeper into HIPAA's Security Rule Requirements

At its most basic level, HIPAA's Security Rule requires CEs and BAs to develop a security management program, documented security processes/procedures, and a demonstrable audit process. This entails implementing appropriate administrative, technical, and physical safeguards in order to protect the confidentiality, integrity, and availability (CIA) of PHI [4]. In addition, a central requirement is to perform risk assessments regularly to ensure security measures are effective [4].

The three safeguards are common in the field of information security and are defined by HIPAA as follows:

- ***Administrative*** – These safeguards include "administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations. Administrative safeguards involve the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of workforce members in relation to the protection of that information" [3].
- ***Physical*** – These safeguards include "physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion"[3].
- ***Technical*** – These safeguards include "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it" [5].

Table 2. Examples of HIPAA Security Rule Safeguards

Administrative	Physical	Technical
• Security Management Process • Information Access Management • Workforce Training • Evaluation	• Facility Access and Control • Workstation and Device Security	• Access Control • Audit Control • Integrity Control • Transmission Security

Source: Summary of HIPAA Security Rule

The goal of these safeguards is to achieve the CIA of patient PHI. CIA is a widely known model used to guide the development and implementation of security programs. The CIA triad represents guiding principles that all security programs should achieve [6]. Each component of the triad is defined as follows [6].

- ***Confidentiality of data*** – Prevents unauthorized disclosure
- ***Integrity of data*** – Prevents unauthorized modification
- ***Availability of data*** – Prevents the loss of access

The preamble of the HIPAA Privacy Rule provides an example of the complexity involved in implementing HIPAA's three safeguards to achieve the principles of CIA. HIPAA cites the American Health Information Management Association (AHIMA) in observing that "during the course of a typical hospitalization," an average of 150 people access a patient's full or partial medical records [1]. These 150 individuals work in roles ranging from doctors, nurses, and primary caregivers to support (e.g., x-ray technicians) and administrative (e.g., billing clerks) staff [1]. This scenario illustrates the difficulty in efficiently sharing patient information among diverse CE and BA staff, each with a different purpose in accessing full or partial records, while also protecting the patient's privacy and achieving the security safeguards mandated by HIPAA.

Faced with such a complex operations environment, CEs and BAs can benefit from a document management solution (DMS). A DMS is a hybrid software-hardware solution that assists in the creation, storage, transmission, and security of what HIPAA calls electronic health records

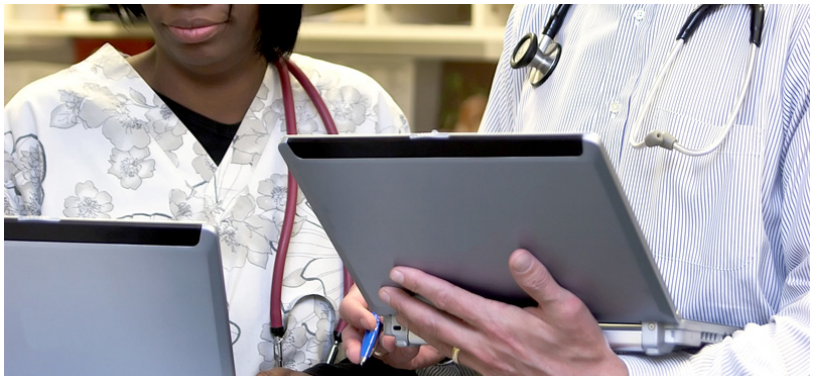
(EHRs). EHRs often contain PHI, such as patient medical records and billing information, in electronic format (ePHI). A DMS assists CEs and BAs in modernizing operations, while also helping to improve security by transitioning from a predominantly paper-based environment into one that uses EHRs and ePHI. When configured properly, the National Institutes of Technology and Standards (NIST) has observed that EHRs serve as a better protection of PHI than paper [7].

Part 3

How DMS Features Help to Comply with HIPAA's Security Rule

A DMS aids in HIPAA compliance because many common DMS features map to the Security Rule's technical safeguards. In turn, the technical safeguards enable CEs and BAs to achieve the guiding security principles of CIA in the following ways:

- *DMS features that aid in the confidentiality of data*



  - ***Encryption*** – Converts readable data into gobbledygook that cannot be meaningfully deciphered without a secret mathematical key; even if someone (with or without permission) can view the encrypted data, say a patient's credit card number, that person cannot make sense of the data without first decrypting it.

  - ***Access control*** – Enables central system administrators to allow/disallow CE employees and BAs access to ePHI; the most common type of access control is role based, wherein an administrator allows access to full or partial medical or billing records based on the individual's job role and purpose for accessing the data.

  - ***Authentication*** – Ensures that a person (or another IT system) attempting to access data is who they say they are; the most common type of human authentication is the password, but other, stronger authentication schemes include two-factor and three-factor authentication.

- *DMS features that aid in maintaining the integrity of data*

  - ***Digital signatures*** – A type of authentication that, unlike passwords, helps maintain the integrity rather than the confidentiality of data; digital signatures use a complex cryptographic process to ensure that electronic communications actually originated from the individual who claims authorship.

  - ***Checksums*** – A mathematical method to ensure that data has been in no way modified, intentionally or by accident, during storage and/or transmission between a sender (e.g., BA) and a receiver (e.g., CE).

- *DMS features that aid in maintaining the availability of data*

  - ***Data backup*** – A critical functionality that enables organizations to recover from and continue operating in the event of a disaster, ranging from severe weather

(e.g., hurricanes) and accidents (e.g., unexpected power loss) to malicious activities (e.g., computer hacking); some DMSs offer the option of on-site backup as well as off-site backup via cloud computing technology. (This is discussed in more depth in the next section of this paper.)

Table 3, below, summarizes how common DMS features enable organizations to achieve the principles of the CIA triad.

Table 3. How Common DMS Features Enable CIA

Confidentiality of Data	Integrity of Data	Availability of Data
• Encryption • Access control • Authentication	• Digital signatures • Checksums	• Data backup (on-site or off)

In addition to significantly aiding in compliance with HIPAA's Security Rule, DMSs also enhance and improve upon aspects of CE and BA operations by providing the following:

- ***Cost savings*** – Transitioning to EHRs and ePHI to manage documentation introduces numerous opportunities for cost savings, from decreasing the physical space required to store paper records to automating tedious tasks.
- ***Process efficiencies*** – DMSs help to eliminate many repetitive manual tasks required to maintain paper documentation (e.g., advanced workflow integration), in turn freeing staff to focus on patient care and quality.
- ***Improved patient/client relations*** – DMSs help to be more responsive to patients and clients (e.g., faster communications), which improves the overall quality of service.

Part 4

Planning to Deploy a DMS

Transitioning from a predominantly paper-based documentation system to one that achieves the full benefits of EHRs and ePHI management can be challenging. Although a DMS's relative advantages to paper-based systems are clear and the benefits attractive, many CEs and BAs hesitate to adopt one because of the perceived complexity and additional work required. In fact, as in any job, the right tool (or technology) simplifies a complex process. With a solid plan and a phased approach, an orderly and efficient transition is entirely possible.

The first consideration in planning DMS deployments is the organization's business model and its requirements to comply with HIPAA's rules. As mentioned in Part 1 of this paper, CEs and BAs are both required to comply with HIPAA's rules, but the specifics vary, especially in regards to the Privacy Rule. However, most requirements for complying with the Security Rule apply equally to CEs and BAs. As outlined in Part 3 of this paper, many common DMS features aid in fulfilling HIPAA's technical safeguards. Following are some considerations when evaluating DMS features:

- ***Encryption*** – The encryption used should be strong enough to withstand malicious individuals' attempts to brute-force crack it. Brute-force cracking involves attempting to guess every possible combination of the mathematical key used to encrypt the data in order to decrypt it. Brute-forcing cracking requires intensive computational processing,

which is readily available to criminals in the form of low-cost, on-demand cloud computing services. To ensure the confidentiality of data, even following a successful breach, DMSs should offer the Advanced Encryption Standard (AES) with a minimum key length of 128 bits. Using AES with a 192-bit or 256-bit key is preferred.

- ***Access Control*** – Of the numerous types of access control models, the most common in non-military organizations is role-based access control. This method enables a central system administrator to allow/disallow individuals to access full or partial EHRs and ePHI based on their roles (e.g. doctors, billing clerks, etc.) and purpose. From a security administration standpoint, this is probably the most efficient type of access control to implement. Some DMSs provide Microsoft Active Directory Sync, which is an efficient way to implement and administer access control based on existing policies and technologies.

- ***Authentication*** (for data confidentiality) – Single factor authentication is compliant with HIPAA and remains one of, if not the, easiest and most affordable authentication schemes. However, authentication can be made more secure by implementing what is known as two-factor authentication. This scheme requires humans to authenticate themselves by providing something they know (e.g., password) in addition to something they possess, such as a time-sensitive code sent to their cellphone or an organization-issued token. This second factor – requiring something users possess – significantly complicates the task of imposters, especially those outside of the organization. DMSs that support two-factor authentication schemes therefore provide stronger protection than those that support only single-factor authentication.

- ***Authentication (for data integrity)*** – Some DMSs support digital signatures for both the transmission of data and to facilitate authentic electronic signatures. This feature adds a layer of security to a business process that can significantly improve the efficiency of a common task.

- ***On-site versus cloud backup*** – This continues to be one of the hottest topics of debate in the security community and a vexing question across industries: Is data safer when stored on site or in the cloud? The truth is, each method has its inherent advantages and disadvantages, and effectiveness depends on the security model in place to protect the data, regardless of where it is stored. A security and risk management assessment, which is required by HIPAA, can provide some insight for each organization [3]. Selecting a DMS that offers both options is prudent, even if both functionalities are not used initially. After all, businesses change, requirements evolve, and so forth. Selecting a DMS that offers both affords a degree of flexibility over the long term.

- ***Audit support*** – DMSs should provide adequate audit support features. Examples include audit tracking, which logs every modification to files made by users or the system, and document retention, which allows users to set an expiration date for storing files. Such features can reduce manual processes or fully automate tasks (e.g., deleting a file after its designated expiration date).

- ***Hardware (scanner)*** – All of the features above apply to the software piece of the DMS. Hardware, particularly the scanner, is an equally important aspect of the total DMS. In

evaluating scanners, consider the speed and quality of scanning, as well as its reliability and how easily it integrates with DMS software. Some DMS software vendors certify scanners that easily integrate with them. Selecting a certified, hybrid software-hardware solution affords a degree of confidence about compatibility and ease of integration.

In addition to choosing a DMS based on optimal features, the transition from a paper-based to EHRs/ePHI environment is often made smoother by the following:

- ***Think holistically about the business environment during planning*** – DMS is primarily a technological solution, but people and process impact its implementation. Consider how the deployment of a DMS will affect existing processes and how it will impact staff roles, responsibilities, etc. Organizations that evaluate their environments holistically, taking time to document the current state (without DMS) versus the future state (with DMS) operations, are more likely to select an optimal DMS and to achieve specific goals following its deployment. HIPAA requires comprehensive process and procedure documentation, so reviewing and updating this documentation as part of the DMS evaluation process serves a dual purpose[3].
- ***Develop a phased transition plan*** – The transition from paper to EHRs/ePHI can be implemented on a gradual basis during the course of day-to-day operations. The transition must not occur all at once. For example, a BA could lay out a plan to conduct batch conversions from paper to electronic records during the course of its regular billing cycle.

A CE could lay out a plan that involves converting patients' paper medical records to digital format following a visit. It could take one or two years for the CE to complete the transition at this pace, but the approach can be more efficient by integrating record scans into normal workflow activities, versus treating the activity as separate projects, per se. It would just require implementing a new post-visit process and perhaps modifying existing staff roles. Alternatively, the transition could be phased according to milestones or volumes rather than events. For instance, using a document scanner capable of scanning from 45 to 65 pages per minute (ppm), an organization can convert 4,500 to 6,500 records from paper to electronic format per day. Depending on the size and complexity of the business environment, such an approach could make more sense.

- ***Plan for staff training*** – As mentioned in Part 2 of this paper, training the workforce to properly use privacy and security technologies falls under HIPAA's administrative safeguard requirement. Deploying DMS and implementing its use into daily workflow requires training. All of the DMS security features designed to help comply with HIPAA's Security Rule are useless if staff are untrained on how to properly configure and operate the technology. Evaluate DMS vendors' training, as well as ongoing technical support, as part of the buying process.

Through diligent product evaluation, careful organizational planning, and a logical phased approach, CEs and BAs can achieve an orderly and efficient transition from paper-based to EHR/ePHI environments.

Part 5

Conclusion

HIPAA compliance is difficult, tedious, and time consuming, but is also required for CEs and BAs. As healthcare-related data breaches continue to make news, HIPAA is unlikely to become less relevant. The best approach for CEs and BAs is to make compliance as easy and efficient as possible.

DMSs help organizations to comply with HIPAA by providing a set of features that map to the required technical, administrative and physical controls or safeguards in the Security Rule. In turn, these safeguards contribute to the principles of CIA, which serve as effective guidelines for any security program. DMSs also provide a set of broader business benefits, including the following:

- Decreased cost of compliance through process efficiency, task automation, and easier auditing.
- Improved patient/client relations by allowing staff to focus on quality care and responsive service.
- Enhanced risk mitigation facilitated by a detailed review of operations and documentation prior to DMS deployment, as well as a suite of technological features that, properly configured and operated, provide more security than paper-based systems.

One DMS that small and medium CEs and BAs can consider is eFileCabinet software with certified Epson scanners. The eFileCabinet DMS is easy to use, fully featured, secure, and value priced for small and medium CEs and BAs. Epson's WorkForce DS-510, DS-760, and DS-860 scanners deliver performance, reliability, quality, and value. Visit eFileCabinet and Epson online to learn more.

About

Epson

Seiko Epson Corporation is a global imaging and innovation leader that is dedicated to exceeding the vision of customers worldwide through its compact, energy-saving, high-precision technologies, with a product lineup ranging from printers and 3LCD projectors for business and the home, to electronic and crystal devices. Led by the Japan-based Seiko Epson Corporation, the Epson Group comprises over 70,000 employees in 108 companies around the world, and is proud of its ongoing contributions to the global environment and the communities in which it operates.

eFileCabinet

Founded in 2001, eFileCabinet Inc. began as a cutting-edge tool to digitally store records in accounting firms. Over time, eFileCabinet has evolved into a sophisticated but simple electronic document management solution designed to help organizations capture, manage, and protect their data regardless of their industry. Today more than 154,000 users (and growing) worldwide rely on eFileCabinet Inc. solutions to provide a simple but effective document management software solution. eFileCabinet provides cloud and client/server solutions, including: eFileCabinet On-Premise, an electronic document management software for storing and managing important business documents; eFileCabinet Online, a hosted DMS solution; SecureDrawer, a client portal/file sharing service to share and collaborate.

References

1. Daniel J. Solove (April 2013). "HIPAA Turns 10: Analyzing the Past, Present and Future Impact." Journal of AHIMA 84, no.4: 22-28. Retrieved from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050149.hcsp?dDocName=bok1_050149

2. Privacy Rights Clearinghouse (2015). Chronology of Data Breaches. Retrieved from https://www.privacyrights.org/data-breach/new

3. The Office of the National Coordinator for Health Information Technology (April 2015). Guide to Privacy and Security of Electronic Health Information, Version 2.0. [Electronic Resource] U.S Department of Health and Human Services. Retrieved from http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

4. U.S. Department of Health and Human Services (2015). "Summary of HIPAA Security Rule." [Electronic Resource] www.HHS.gov. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

5. Centers for Medicare & Medicaid Services (May 2005, Revised March 2007). "HIPAA Security Series: Security Standards -- Technical Safeguards, Vol. 2 Paper 4." [Electronic Resource] U.S. Department of Health and Human Services. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

6. Yusuf Bhaiji (July 2008). "Chapter 1: Overview of Network Security." [Electronic Resource] Cisco Press. Retrieved from http://www.networkworld.com/article/2274081/lan-wan/chapter-1--overview-of-network-security.html

7. Karent Scarfone, Murugiah Souppaya, and Matt Sexton (November 2007). NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices. [Electronic Resource] National Institute of Technology and Standards. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

Published: October, 2015

EPSON®
EXCEED YOUR VISION

Epson America, Inc.
3840 Kilroy Airport Way, Long Beach, CA 90806