Document Management and HIPAA:

Protecting Your Data, Your Employees and Your Organization

If your organization deals with any aspect of providing health care to individuals in the United States, then it is almost certain that you are affected by HIPAA security rules. Under the Health Insurance Portability and Accountability Act of 1996, better known as HIPAA, the United States Department of Health and Human Services (HHS) has established a very stringent set of rules for document and data security to protect the privacy of health care information.

Some organizations incorrectly assume that these rules only apply to doctors, health insurance companies and hospital administrators. However, any individual or organization that collects, stores, holds, processes or even has access to an individual's personal health information is responsible for protecting that information even if they're not considered a "covered entity" under HIPAA. Violations of the HIPAA rules can lead to very severe financial penalties, and in some cases even criminal charges and incarceration. Remember that application you give to all your employees when they sign up for health insurance? That qualifies as access to personal health information, and even though you may not be a "covered entity," it makes your organization responsible for protecting that information.

> *"... if an employer has any kind of health clinic operations available to employees, or provides a self-insured health plan for employees, or acts as the intermediary between its employees and health care providers, it will find itself handling the kind of PHI that is protected by the HIPAA privacy rule."*
>
> *Especially for Texas Employers, Texas Workforce Commission, 2012 Edition*

The objective of this paper is to identify how you can leverage your document management system to not only help protect confidential health care information, but also to help protect yourself and your organization from the penalties of non-compliance with HIPAA regulations.

HIPAA Overview

HIPAA security standards are categorized into three specific areas of "Safeguards": Administrative Safeguards[1] which deal with organizational policies and procedures; Physical Safeguards[2] which deal with the physical security of systems and information; and Technical Safeguards[3] that deal with the electronic security of systems and information.

It is important to note that it is not possible to create software that will automatically guarantee compliance with all HIPAA security requirements. Many of the Administrative and Physical Safeguards are focused on aspects of security that are simply not affected by systems and software. However, there are several areas, including data backup, and disaster recovery, where your Document Management System can help you avoid potential problems by ensuring security for personal health information and helping you comply with HIPAA regulations.

Data Backup

The HIPAA Administrative Safeguards require covered organizations to have a data backup plan in place to ensure that personal health information is secure and protected in the event of some kind of systems failure. Your document management system can help provide security and compliance in two ways. First, if you have all of your data on-site, many systems can help you implement secure, encrypted off-site backup that happens automatically according to your specifications. Second, with some suppliers, you can implement your entire document management system "in the cloud." With these systems, not only are your backups automatically taken care of, but you also gain the benefit of the enhanced physical security that most independent data centers provide.

"Annual data losses cost U.S. businesses $18.2 billion"

David M. Smith, PHD
Pepperdine University,
Graziado Business Review V6 I3

Emergency Operation and Disaster Recovery

Most employers are not sufficiently prepared for emergency operation or even disaster recovery. But consider this: What if one of your employees is injured in a major fire at your building, and it also happens to destroy the system containing critically important health care information for that employee? How are you going to get to that information? Because health care information is so important, HIPAA Administrative Safeguards also require covered entities to have a plan for secure access to personal health care information under emergency conditions, as well as a plan for recovery from a disaster situation. The best cloud-based document management systems will ensure secure access to your critical data in a disaster situation, and make it dramatically easier to plan for and recover from that disaster. Not only will it save you a lot of money in the event of a disaster, it will save your employee's personal information.

> *"Baylor University Medical Center in Dallas has budgeted $7.5 million over 5 years to pay for implementation of HIPAA"*
>
> *American Hospital Association*

Physical Safeguards

Think of the HIPAA Physical Safeguards as the physical barrier between your health care information and anyone or anything that threatens to physically destroy it or access it. For most small businesses, it can be quite expensive and often impractical to implement the level of physical security required to comply with or exceed HIPAA regulations. Imagine having to implement the following physical security capabilities to protect your systems that contain sensitive data:

- Power conditioning
- Strict environmental controls
- Redundant network connections
- Natural disaster protections
- Backup power generation systems
- Personnel access controls
- Intrusion detection
- Video surveillance
- Fire detection and suppression
- Offsite backup

However, as mentioned earlier, most cloud-based document management systems are hosted in facilities that provide state-of-the-art physical security and protection against anything from a natural disaster to a power outage. In the best situations, your supplier's data center may already have received HIPAA certification for their physical safeguards.

For organizations with on-premise systems, physical safeguards can be significantly more challenging. Some on-premise systems have very useful physical security features that tie in directly with their document management system. For example, a document management system that provides automatic backups to a cloud-based server will effectively provide two benefits. First, it fulfills the need for basic data backups, and second, it provides off-site storage for those backups.

" System Owners must develop, document, implement and test a Contingency Plan that includes (1) A Backup Plan (2) An Emergency mode operation plan; and (3) A Disaster Recovery Plan. "

–Yale University HIPAA Policy 5100 – Jan. 13, 2012

However, on-site systems will still require significant effort to develop internal policies and procedures to physically protect sensitive information. Things like uninterruptable power supplies and personnel access controls are a good place to start, but be prepared for additional investments. A more in-depth analysis of physical security concerns can be found in our white paper titled “Crucial Document Management Security Concerns - Online and On-Premise”

Access To Information

HIPAA regulations define Technical Safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."[3] In other words, Technical Safeguards are the measures you take to protect sensitive health care information when it is inside your system or being transmitted to or from your system. The good news is that the best cloud-based services have processes in place to address many of these issues. Some on-premise systems from the best suppliers also cover many areas fairly well. However, if you have home-grown systems with highly sensitive information, you may have to keep up with this fast-moving area of security on your own. In order to meet or exceed the HIPAA requirements, you will want to make sure your system includes most, if not all of the following capabilities:

- **Proper user ID and password administration** capabilities that help you ensure that all users are uniquely identified and that their passwords are sufficiently secure and periodically changed.
- **Role-based account access** and security will help ensure that only those individuals with proper authorization can access certain kinds of sensitive information. The best systems will allow you to implement multiple levels of access depending on the role of the user.
- **Group-based access management** will allow you to define groups of users and grant differing levels of access by group.
- **Data redaction capabilities** can dramatically increase usability by providing the ability to redact individual words or sentences in documents. This capability allows users with lower levels of clearance to view and work with a particular document while preventing them from viewing more sensitive areas of that document.

- **Emergency access procedures** ensure that information can still be securely accessed in an emergency situation.
- **Automatic logoff** capabilities help secure your sensitive data in case someone leaves a workstation unattended.
- **Data encryption and decryption** capabilities ensure that sensitive information cannot be viewed or interpreted without the correct encryption keys. The best systems use 256 bit encryption.

Audit Trails

Clear audit trails are another provision of the HIPAA regulations. Proper audit controls will record all activity pertaining to sensitive data, and particularly any activity which changes or captures information. In some cases, the logs generated by your document management system's audit controls can be used directly for HIPAA compliance reporting. In addition, proper audit controls are extremely important when investigating potential security violations. Solid audit controls is something that should be included in all good document management systems, whether on-site or cloud-based.

" Encryption of e-mail messages merits special attention because e-mail is so common. Many patients enjoy direct online communications with their physicians via e-mail. The problem, of course, is that e-mail is the digital equivalent of a postcard. Anyone handling the message can easily read its contents. "

David C. Kibbe, MD, MBA - Fam Pract Manag. 2005 Apr;12(4):43-9

Data Integrity

HIPAA requires that policies and procedures be put in place to ensure that sensitive information is protected from improper alteration or destruction as a result of intentional or unintentional actions on the part of workers, or from technical causes such as media errors. Your document management system will need to have mechanisms in place to help identify

or discover such errors when they happen. The best systems have electronic mechanisms that include elements such as check sum verification, digital signatures, or other electronic verification tools to automatically check for data integrity whenever the data is accessed or transmitted.

Identity Authentication.

Under HIPAA, the organization must have procedures to verify that a person or entity seeking access to sensitive information is in fact who they claim they are. This can be as simple as a password or pin, some kind of card or key, or in some cases, it might be as sophisticated as the facial recognition or other biometric methods. Some of the best document management systems will provide in-depth authentication mechanisms within the software, in addition to easily allowing the integration of third party authentication hardware.

Security During Data Transmission

HIPAA requires that the organization implement security measures to prevent the unauthorized interception of or access to sensitive information that is being transmitted over a network, whether it is an internal network or public network like the internet. As mentioned above, steps need to be taken to ensure that data is not corrupted (data integrity) during transmission, and nearly all document management systems handle this in the proper fashion.

The other aspect of data security during transmission deals with encryption and decryption. Unless data is properly encrypted prior to transmission across a network, it can often be intercepted and interpreted. Sophisticated encryption algorithms can prevent the data from being interpreted even if it is somehow intercepted. The best document management systems use 256 bit encryption algorithms.

Summary

If you deal with personal health information, even if it is just for your own employees, it simply makes good business sense to ensure that the information is secure. If you are a "covered entity" as defined by HIPAA, you are required to comply with HIPAA Security Standards. The failure to implement proper security in either case can have extremely serious consequences for your employees or customers, and could potentially result in very damaging civil penalties or even criminal charges. In today's environment, threats to your sensitive data are increasing rapidly. By ensuring your document management system can comply with HIPAA requirements, you can dramatically reduce the level of risk your company has to bear while providing confidence for your customers.

References

1 - Security Standards: Administrative Safeguards, HIPAA Security Series, US Dept. Of Health and Human Services

2 - Security Standards: Physical Safeguards, HIPAA Security Series, US Dept. Of Health and Human Services

3 - Security Standards: Technical Safeguards, HIPAA Security Series, US Dept. Of Health and Human Services