DynaFile™ HIPAA Compliance Overview

Rev 9/20/2012

DynaFile
Your Documents. On Demand.

WWW.DYNAFILE.COM

Overview

Maintaining HIPAA and Joint Commission compliance is a challenge for all healthcare organizations. From maintaining privacy and security to guaranteeing record integrity, compliance involves a number of complex processes. But having the right technology can make compliance easier than you might think. The DynaFile™ document management system gives you the tools you need to enforce your compliance plan at every level of your organization.

Adopting an electronic medical record system is a great way for hospitals, doctor's office, clinics, or any other type of businesses in the healthcare industry to easily share information with each other. An electronic medical record system speeds up the process when dealing with insurance companies by allowing patients' medical records to be accessed securely through an online portal. Insurance companies do not have to call and wait for businesses to fax over important documents. Doctors can share patients' information such as scans, diagnoses, or medical records through the use of a high speed internet connection. A cloud based document management system such as DynaFile™ provides a virtual filing cabinet for doctors to cross reference and insurance companies to speed up the paperwork.

Protected Health Information

Both HIPAA and Joint Commission Management of Information standards specifically address information security, privacy and confidentiality in terms of Protected Health Information (**PHI**). DynaFile™ features multi-layered security that gives system administrators finely-tuned control over access to the system and patient records, as well as associated documentation.

- Maintain information security with password-protected access to the DynaFile™ repository.
- Assign user- or group-specific access rights to individual folders, files and metadata.
- Redact individual words or entire areas of documents to secure PHI such as patient name, address and Social Security number.
- Manage written or oral PHI in any format, from paper to e-mail to audio and video files.

Within DynaFile™, PHI records are stored as encrypted data to prevent any unauthorized access. All of our servers are diligently monitored by trained IT personnel. Furthermore, a documented disaster recovery plan is in place to ensure that important data can be recovered in case of an unexpected data center disaster

Comprehensive System Security

HIPAA security regulations dictate how to store, transfer and protect the privacy of electronic PHI. DynaFile's™ security and auditing tools help you enforce your administrative and technical PHI safeguards. And when it's necessary to access information for patient care, DynaFile™ ensures that only authorized personnel can do so.

- Log all attempts to view, delete, edit, move, e-mail or print documents and records.
- Options to affix a custom watermark or timestamp to printed documents.
- Ensure continuity of information with document versioning.
- Preserve complete patient records by restricting modification and deletion of documents.

Data Center Security

In today's global economy, service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. While SAS 70 utilized criteria that were defined by the data center provider, SOC 2 Type II and SOC 3 reports put stricter audit requirements in place and set a higher bar with a more meaningful audit standard. Because SOC 2 and SOC 3 independently verify the validity and functionality control activities and processes, customers can be assured that the highest level of internal controls and security are established and maintained. This not only ensures that our data centers have been through an in-depth audit to ensure adequate controls and safeguards are in place, but adds a further assessment layer by requiring an organization's management to attest in writing to the fair presentation and design of controls

The data centers that house the DynaFile™ system have completed a full audit for SOC 2 Type II and SOC 3 compliance. Through the use of a dedicated firewall to prevent network threats and unauthorized access to sensitive patients' health records, biometric fingerprint identification, multiple redundant backup mechanisms as well as training for our engineers and data center technicians you can ensure that your data is secure.

Tracking of All Activity

Joint Commission standards indicate that only designated, qualified staff accept and transfer information. HIPAA likewise states that organizations must establish policies and procedures regarding which individuals can access and distribute PHI. DynaFile™ tracks all repository activity, including who performed the action, which documents were involved and where, when and why the action took place.

- Monitor system activity, including individual user activities, repository searches and attempts to change documents or user information.
- Restrict information distribution at the user or group level.
- Quickly identify security threats with custom web-based reporting.

Conclusion

With electronic document management, you not only reduce costs and increase profits, but you also streamline your compliance processes. Comprehensive security measures protect your documents from unauthorized access in a way file cabinets cannot, enabling you to monitor user activity, protect documents from alteration or loss and prevent accidental release of confidential information.

In an increasingly demanding regulatory environment, an electronic document management solution both improves your organization's profitability and helps limit exposure to civil and criminal liability. With a solution such as DynaFile™, a compliance program no longer has to complicate your business processes and consume large amounts of time and money. Instead, your organization can use your compliance program to streamline workflow and ultimately improve client service and profitability.