eFileCabinet

HIPAA Regulations for Software:

How eFileCabinet Can Help You Meet HIPAA Compliance Standards

Erin Swan

July 2015

Overview

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, was established to protect the privacy of citizens who receive healthcare. Under this act, any organization that handles healthcare information must comply with a set of strict standards regarding how that information is gathered, stored, and transmitted.

If you work in the healthcare industry, you are likely quite familiar with HIPAA regulations for document security. However, it is not only healthcare providers who must comply with HIPAA regulations; if your organization is involved in any aspect of providing healthcare to individuals, you must be HIPAA compliant.

When you give a new employee a form to sign up for healthcare through your business, you are collecting health-related information. Though you may not be a "covered entity" under HIPAA, your company is still responsible for protecting your employees' healthcare information, and must therefore comply with HIPAA's regulations. Failing to do so can lead to high fines, and in some cases, criminal charges and jail time.

To ensure that employee information is protected and handled in compliance with HIPAA's standards, many companies turn to electronic document management software, like eFileCabinet.

It is important to note, however, that software alone cannot make you HIPAA compliant. The bulk of the responsibility rests on your company in the way that you handle and access the information. To be fully HIPAA compliant, you must follow proper procedures, including facility security measures, accessibility of information, and other factors. However, the right software can be an integral part of becoming a HIPAA-compliant facility.

> The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.
>
> Specifically, covered entities must:
>
> 1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
> 2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
> 3. Protect against reasonably anticipated, impermissible uses or disclosures; and
> 4. Ensure compliance by their workforce.
>
> -HHS.gov

HIPAA has provided a checklist for such software to ensure that security and storage standards are up to par in order to protect citizens' electronic protected health information, or e-PHI. The checklist is divided into three sections: Access Control, Physical Safeguards, and Administrative Safeguards. We'll go through these sections and address the requirements listed in each one, assessing how eFileCabinet meets HIPAA's regulations for document management software.

Access Control

Access Control refers to the software's ability to prevent unauthorized access to information. This means that the software should have certain security measures in place to protect documents.

Unique User Identification

To meet this requirement, document management software must have a way to verify who the user is before providing access to documents and employee information. This can take the form of a simple PIN or password, or can be as complex as facial or voice recognition.

All versions of the eFileCabinet software require users to have a unique username and password to gain access to documents contained in your company's cabinets. The password requirements for access can be adjusted by a system administrator. This means that you can adjust your level of security by requiring more complicated passwords from users, making their passwords more difficult to crack.

Automatic Logoff

To be HIPAA compliant, software must have an automatic logoff feature. If someone accessing the information becomes inactive in the program, they should be automatically logged out of the system after a set amount of inactive time. This prevents unauthorized personnel from accessing the software should an employee forget to log out of their user profile.

The eFileCabinet software is set to log you out after a certain amount of inactivity. You can adjust the preset amount of time before the program logs you out, customizing your level of security. Once you've been timed out, you will be required to log back in using your user credentials. For the mobile app, you can use a PIN to access the software again.

Encryption and Decryption

HIPAA requires data to be properly encrypted before being shared across a network, whether that network is public or private. This prevents unauthorized persons from intercepting and interpreting the data that is being shared.

> Encryption is one method of rendering electronic PHI unusable, unreadable, or indecipherable to unauthorized persons. The successful use of encryption depends upon two main features: the strength of the encryption algorithm and the security of the decryption key or process.
>
> - HIPAA.com

eFileCabinet encrypts the data on your network when it is both in transit (being shared with other users) and at rest (stored on your drive or in the cloud), ensuring that your information is protected at all times. This software uses 256-bit encryption, which gives the highest level of security possible. Data is only decrypted when it is being accessed by an authorized user.

Physical Safeguards

To be HIPAA compliant, businesses must have certain physical safeguards in place to protect employee healthcare information. This responsibility extends to the database server your document management software uses. These are the physical barriers that prevent theft or loss of information, either through malicious intent or natural disasters.

Data Backup and Storage

HIPAA requires document management systems to have automatic data backup and storage in order to achieve compliance with their standards. This usually means backing up all information to a remote location, such as a "cloud" system. This prevents data from being lost in the event that your facility is damaged or destroyed by a fire or other natural disaster.

eFileCabinet Online operates solely through the internet, which means no documents are stored at your business location, negating the threat of losing data should your business network be damaged or destroyed. The desktop version of eFileCabinet has an auto-backup feature, which you can activate in order to meet this HIPAA requirement. Your data will then be automatically backed up to the cloud, which is hosted by Amazon Web Services (AWS).

> The covered entity must develop procedures to protect its facility and systems from "unauthorized physical access, tampering, and theft." These policies and procedures are outcomes of the covered entity's risk analysis pertaining to unauthorized access to its facility. Unauthorized access includes access to building exteriors and interiors, tampering, theft, intrusions, and deliberate impairment of systems, including computers and electricity supply.
>
> -HIPAA.com

Facility Security Plan

This requirement is not directly related to the software you use to store healthcare information, but rather, it refers to the measures the database server takes to protect the storage device itself. Your document management software should utilize a server that has ample security measures in place to meet HIPAA compliance requirements. The database server should have certain certifications indicating that they have met these requirements.

As already stated, eFileCabinet uses AWS to backup and host your documents in the cloud. AWS has received two types of certifications indicating they have met HIPAA compliance standards for facility security, and they employ a large number of security measures to protect the information they host:

- Redundant power servers
- Video surveillance
- Limited access to servers
- Fire suppressant
- Disaster recovery plans
- And many more security measures

The facility security plan at the physical database location ensures that your data remains safe in the cloud, and that you are able to access the information any time you need it.

Administrative Safeguards

The final category of HIPAA requirements is referred to as Administrative Safeguards; these are the security measures put in place to regulate and monitor access to the secured documents. These safeguards are designed to ensure there are no unauthorized changes to documents, and to further limit access to more sensitive documents.

Login Monitoring

To comply with HIPAA regulations, your document management software should allow you to monitor who is logging into your system and which documents they are accessing. This shows you which users are accessing documents and when they are being accessed, allowing you to monitor any suspicious or unauthorized access and activity.

If you have administrative capabilities in eFileCabinet, you can view a document's access history to see which users accessed a document, as well as what time it was accessed. The software will also monitor and record any changes made to your documents; if something is changed in a document that should not have been changed, you can see when it was done and who did it, so you can address the issue. These audit trails ensure that your documents are not tampered with, and they remain accurate.

> A covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.
>
> - HHS.gov

Access Authorization

HIPAA-compliant software should also have the ability to give different users different levels of access to the software. For example, a data-entry worker would have access to fewer documents and less information than the HR administrator. Another term often used in describing this requirement is limiting access and use to only the "minimum necessary"; this means restricting access to information based on the individual's role in the workplace, giving them the access they need to fulfill their duties and no more.

eFileCabinet allows you to create user groups with various levels of access. When you give an employee access to the software, their profile can be added to a group with the appropriate access levels. In this way, they can complete the tasks required of their position without you having to give them full access to sensitive healthcare information. As an administrator, you can alter this access at any time as needed.

Summary

If you are a “covered entity” as defined by HIPAA, you are required to meet HIPAA’s Security Standards, and your document management software must comply with the requirements outlined above. But even if you are not a “covered entity,” it is simply good business practice to follow these requirements, and ensure that your software is as secure as possible.

It is also important that your employees be properly trained on how to use the security measures within the software, and how to handle e-PHI according to HIPAA’s Security Standards. Proper business procedures and information handling are the cornerstones of HIPAA compliance; electronic document management software such as eFileCabinet can only be effective when all other business procedures are in compliance with HIPAA.

eFileCabinet has been carefully designed and structured to be easy to use, but with security measures that make it difficult to access without authorization. These features are customizable, and are only HIPAA compliant when you have activated and are properly using all of the available security features described above. If any security features are misused or inactivated, you are no longer in compliance with HIPAA.

However, when properly employed, eFileCabinet’s security measures and features meet the incredibly complicated compliance standards set forth by HIPAA for electronic document management software. By coupling this software with proper security measures and business procedures within your company, you can meet HIPAA compliance requirements, protecting both the sensitive healthcare information you handle and your business from liability.

Sources

1. Beer, Ken and Ryan Holland. Amazon Web Services. *Securing Data at Rest with Encryption.* November 2013. Web.

2. Amazon Web Services. *Creating Healthcare Data Applications to Promote HIPAA and HITECH Compliance.* August 2012. Web

3. HIPAA Security Series, U.S. Department of Health and Human Services. *Security 101 for Covered Entities.* March 2007. Web.

4. U.S. Department of Health and Human Services. *Summary of the HIPAA Security Rule.* Web.