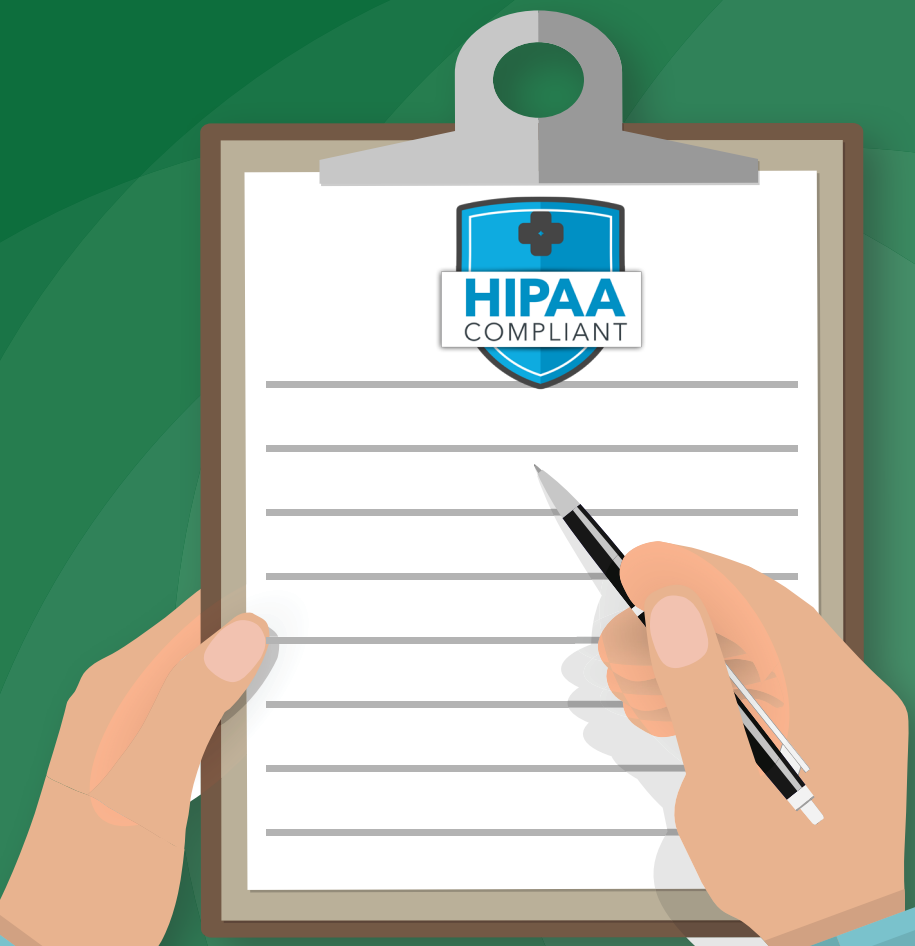

MEETING HIPAA COMPLIANCE WITH DOCUMENT MANAGEMENT SOFTWARE

Ademero
software

FOR MORE INFO VISIT US ONLINE AT
WWW.ADEMERO.COM

MEETING HIPAA COMPLIANCE
WITH DOCUMENT MANAGEMENT SOFTWARE

When it comes to healthcare, privacy is rule number one. It's such an important rule that in 1996 the US Department of Health and Human Services created HIPAA, the Health Insurance Portability and Accountability Act. If you handle protected health information, (PHI or ePHI for "electronic" data), you probably already know about being HIPAA compliant. In fact, the one thing you're most aware of is that if you fail to meet compliance you'll be facing hefty fines, criminal charges, or even jail time... so getting this right is your top priority.

COMPLIANCE

Generally speaking, there are 4 rules to consider for meeting compliance, but not all of these are considerations for the software you choose.

1. HIPAA Privacy Rule
2. HIPAA Security Rule
3. HIPAA Enforcement Rule
4. HIPAA Breach Notification Rule

To start, we'll look at the features your next document management system must have. The first thing of note is what's 'required' versus what is annotated as 'addressable'. Those specifications labeled 'required' must be implemented or it will be deemed an automatic failure to comply with the HIPAA Security Rule. Conversely, those labeled 'addressable' must be implemented if, after a risk assessment, the covered entity has determined that the specification is not reasonable and appropriate. If you decide this and choose to not implement the specification, you must document your rationale for that decision and either:

A

Implement an equivalent alternative that is reasonable and appropriate, or

B

If you choose to not implement either, then you must also document the rationale for this decision

There's a catch though. Even if you document your decision and you are audited, the auditor can decide that they do not agree with your decision, and you are the one that faces the penalty. If you are in doubt, it's probably best to go ahead and implement the 'addressable' specifications since most of them are best practices anyway.

HIPAA SECURITY RULE

Remember those four rules for meeting compliance I mentioned? Well, when it comes to software-related items in that list, you're really only concerned with the Security Rules when looking at what DMS to buy.

Let's start with the Security Rule which is made up of 3 parts.

1. Technical Safeguards
2. Physical Safeguards
3. Administrative Safeguards

All 3 parts include implementation specifications for using software, but do not necessarily mean that the DMS you choose would logically have a hand in everything that is required here. Hosted or cloud solutions will need to cover areas in the Physical Safeguards section that other solutions will not. Some policies and procedures that are requirements for compliance fall on users or admins in your company, so you'll need to understand the requirements and how DMS can help you meet compliance.

TECHNICAL SAFEGUARDS

The Technical Safeguards focus on the technology that protects PHI and controls access to it. Security standards were designed to be technology neutral, so as to cover a broad spectrum of software solutions. There are 5 standards listed in this section. When you are implementing your DMS you'll be looking at how features in the software meet these 5 standards.

1. Access Control
2. Audit Controls
3. Integrity
4. Authentication
5. Transmission Security

1. ACCESS CONTROL

Software features that help prevent unauthorized access to ePHI fall in this category. The software must verify the user's identity before allowing access to documents and information and automatically log users out of the program after a set amount of inactivity. The covered entity, (that's you), is responsible for establishing emergency access procedures to allow the use of a special password by the Security Official for your company/office/etc. to have full access to ePHI during emergency situations. So, you're looking for these features in your DMS

1. Unique User Identification (*required)
2. Automatic Logoff (*addressable)
3. Emergency Access with full access (*required)

2. AUDIT CONTROLS (*REQUIRED)

Covered entities are required to have in place audit controls to monitor activity on software systems that contain ePHI. The ability to monitor

1. Login and logoff activity
2. File access
3. Updates
4. Edits
5. Any Security Incidents

are the main features you're looking for in your software to meet compliance, and must be as close to real time as possible to be useful. You will also need a policy in place within your company/office/etc. to regularly monitor using tools provided in the software; tools like

Document History

including updates, edits, etc.

Event Logging

including user access, incidents, etc.

Tools and features could be named differently depending on your software solution, but must cover these basic needs outlined above.

3. INTEGRITY
- MECHANISM TO AUTHENTICATE ePHI (*ADDRESSABLE)

This can be aided by your software, but the standard itself is about ensuring the ePHI has not been altered or destroyed in an unauthorized manner. If your software has event logging and document history, then you have the features you need to meet this goal with whatever policy or procedure you put in place.

4. AUTHENTICATION (*REQUIRED)

If the software features password protection and automatic logoff mentioned in section 1 above; Access Control, then the software includes whatever tools you need to meet this standard.

5. TRANSMISSION SECURITY
- INTEGRITY CONTROLS (*ADDRESSABLE)

Designed to ensure that security is in place for the ePHI, measures must be taken to guard against unauthorized access to ePHI that is being transmitted over any electronic communications network. This solution can vary, but ultimately boils down to things like firewalls and intrusion detection systems which fall in the wheelhouse of the facility maintaining your network; see Physical Safeguards below for more info.

6. TRANSMISSION SECURITY
- ENCRYPTION AND DECRYPTION (*ADDRESSABLE)

For the sender of ePHI, encryption converts the message in a file or document from a readable to an unreadable format. Decryption is the reverse. While not annotated as required, under HIPAA, every breach of unencrypted ePHI requires you to provide time-bound notifications to affected patients, the Secretary of HHS, and/or prominent local/state media outlets which would put you at risk for fines, lawsuits, bad PR, and more. The good news is that under the Breach Notification Rule, ePHI that is encrypted is not considered breached because it cannot be read or otherwise used without the key(s) required to decrypt it. So, though this one's not required, it's a best practice to have this feature included in your software to protect any data being sent across your network, or 'in transit'.

PHYSICAL SAFEGUARDS

The next set of rules and guidelines focus on the physical access to ePHI. Physical Safeguards like data backups and facility security plans are applicable for whomever is managing your server; the machine that's housing your data and the DMS software.

There are 4 standards in this section

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

When it comes to the physical protection of data, there are many requirements from backup power generators to video surveillance, and beyond. Sensitive healthcare information and documents must be kept secure from both human and environmental threats. Most cloud-based systems are often already located in facilities that meet this level of physical safety as well as the requirements below.

1. FACILITY ACCESS CONTROLS

Your Security Official is responsible for ensuring that this specification is implemented and in place, whether it's being handled by your hosting company or in-house. There are 4 parts to this specification below

Contingency Operations

(*addressable)

Establishing procedures to restore ePHI should it experience a disaster or an emergency related to its physical location.

Facility Security Plan

(*addressable)

Establishing procedures that safeguards the facility and equipment from unauthorized physical access, tampering, and theft.

C

Access Control & Validation Procedures

(*addressable)

Establishing procedures to control and validate a person's access to facilities based on roles and functions.

D

Maintenance Records

(*addressable)

Establishing procedures to document repairs and other maintenance to the physical components of a facility.

2. WORKSTATION USE (*REQUIRED)

This safeguard requires policies and procedures to protect ePHI on the workstation level; ensuring that they are used appropriately, used properly, and in what physical environment access to ePHI is permitted.

3. WORKSTATION SECURITY (*REQUIRED)

This standard is centered around the implementation of physical safeguards for all workstations that have access to ePHI to restrict access to authorized users. The solution is dependent on the covered entity's risk analysis and risk management process, so it can cover a variety of solutions to meet your specific needs.

4. DEVICE AND MEDIA CONTROLS

This standard requires policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility along with the movement of these items within the facility.

There are 4 specifications within this standard

A

Disposal

(*required)

Establishing procedures to address the final disposition of ePHI, and/or the hardware or electronic media in which it is stored.

B

Media Re-Use

(*required)

Establishing procedures for removal of ePHI from electronic media before the media is made available for re-use.

C

Accountability

(*addressable)

Establishing and maintaining a record of the movements of hardware and electronic media and any person responsible.

D

Data Backup and Storage

(*addressable)

Establishing a retrievable and exact copy of ePHI, when needed, before movement of equipment.

Ultimately, hosted solutions can be a great way to save on the expense of having to implement physical security solutions in-house; see hhs.gov for more information on implementing physical safeguard requirements.

ADMINISTRATIVE SAFEGUARDS

The final category of safeguards is centered around the security measures used to regulate and monitor access to your documents and information. The administrative components are very important with HIPAA compliance and outlay guidelines like assigning an in-house Privacy Officer, performing annual risk assessments, employee training, reviews of policies and procedures, executing BAA's, and more.

1. SECURITY MANAGEMENT PROCESS

1. Risk Analysis (*required)
2. Risk Management (*required)
3. Sanction Policy (*required)
4. Information Systems Activity Reviews (*required)

2. ASSIGNED SECURITY RESPONSIBILITY - OFFICERS (*REQUIRED)

3. WORKFORCE SECURITY - EMPLOYEE OVERSIGHT (*ADDRESSABLE)

4. INFORMATION ACCESS MANAGEMENT

1. Multiple Organizations (*required)
2. ePHI Access (*addressable)

5. SECURITY AWARENESS & TRAINING

1. Security Reminders (*addressable)
2. Protection Against Malware (*addressable)
3. Login Monitoring (*addressable)
4. Password Management (*addressable)
5. Response and Reporting (*required)

6. CONTINGENCY PLAN

1. Contingency Plans (*required)
2. Contingency Plans Updates and Analysis (*addressable)
3. Emergency Mode (*required)

7. EVALUATIONS (*REQUIRED)

8. BUSINESS ASSOCIATE AGREEMENTS - BAA (*REQUIRED)

The list of requirements in this section is extensive, but as it pertains to software there's just a couple of features that the software would need to include which are closely tied to requirements outlined in the Technical Safeguards section above.

1

Login Monitoring
(*addressable)

While the act of monitoring requires policies and procedures within your company, the software should provide tools for such a task.

2

Password Management
(*addressable)

The requirement specifically is calling for procedures to be in place at your company for password management, but the ability in the software that allows for password changes, creation, and protection are features that are needed in order to meet this standard.

3

Response & Reporting
(*required)

This standard mandates that security incidents must be identified, documented, and responded to in a timely manner. Software can help meet this requirement with features like document history and system event logging.

KEEPING IT SIMPLE

The hard part about HIPAA is knowing exactly what it takes to be compliant with whatever software you choose, but it doesn't have to be. It's actually pretty simple from the software side, which should help you narrow in on the one you want to purchase pretty quickly. When you boil it down, HIPAA is asking for 4 things with all these rules and regulations.

1. Put safeguards in place to protect PHI and ePHI.
2. Reasonably limit use and sharing of information to the minimum number of people necessary to accomplish your goal.
3. Have agreements in place (BAAs) to ensure service providers that perform covered functions for you do not disclose PHI and safeguard it appropriately.
4. Have procedures in place to limit access to PHI and a training program in place to train employees on protecting this sensitive information.

When it comes to picking a document management system, there's several features you'll need in order to meet compliancy. Individual software might call these by different names, but in the end you'll be looking for features that provide

1. Unique User Identification
2. Password Protection
3. Automatic Logoff
4. Transmitting Data Encryption & Decryption
5. Complete Electronic History of Documents
6. System Event Logging
7. Login Monitoring

If you're using your DMS provider to host your system on the cloud, then you'll also be looking for the requirements for Physical Safeguards like

1. Data Backups
2. Facility Access Controls (Physical Security)
    a. Disaster Recovery Plan
    b. Redundant Power Servers
    c. Video Surveillance
    d. Fire Suppressant
    e. Limited Access to Servers

When it's all said and done, you'll be looking for much more out of your DMS than just an electronic version of a file cabinet. You're looking for a robust and simple solution that meets all your needs at one low price. One that's fast to implement, has all the features you need, with a snappy user interface that's easy to use and understand.

Content Central will keep your office moving with features that do more than just help you meet HIPAA compliance. But don't just take our word for it, give it a try yourself.

Download a Trial

Download a free trial of our Document Management Software today to see just how Content Central works for meeting HIPAA Compliance.

Schedule a Demo

Schedule a personalized demonstration to see exactly how Content Central can help you meet HIPAA Compliance today.

More to Discover!

Learn more about Content Central and the rest of our paperless office suite of products with videos, brochures, help articles, downloadables, and more!

Ademero software

WANT MORE INFO?
VISIT **WWW.ADEMERO.COM**