SmartHIPAA!

7 Things You Must Know About

HIPAA Security

SmartHIPAA

Turnkey HIPAA compliance

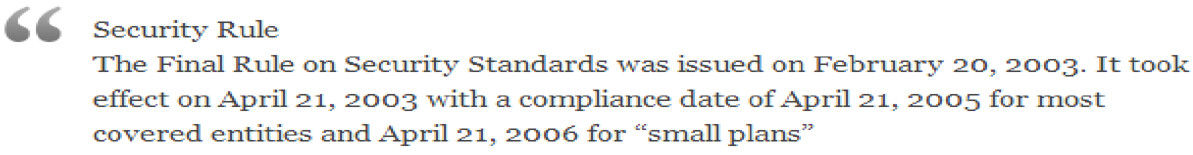
7 Things You Must Know About HIPAA Security

There is a lot to know about HIPAA and the HIPAA Security Rule. There are multiple steps and numerous security safeguards that need to be implemented. We know it can be overwhelming. This paper will highlight 7 things that will help you understand the HIPAA Security Rule and guide you to what you need to do to comply with HIPAA.

Although the process to comply with HIPAA might seem overwhelming, keep in mind that most organizations do not become compliant overnight. It is a process that takes time and effort. Each step that you take and each safeguard that you implement brings you one step closer to compliance. In fact the HIPAA Security Rule requires an iterative process for compliance. Let's take a look at 7 things that you must know about HIPAA security.

1. **HIPAA is not optional**

Many organizations feel they are exempt from the HIPAA regulations. This may stem from that fact that "small practices" were granted a 1 year extension to comply with the HIPAA Security Rule. According to Wikipedia

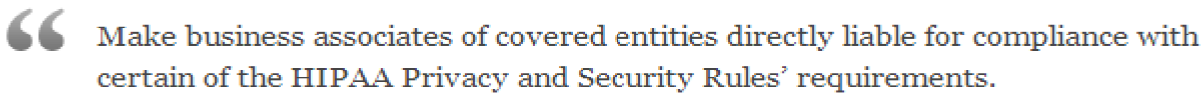


> Security Rule
> The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for "small plans"

So if you are a covered entity or healthcare provider, HIPAA regulations do apply to your practice or organization and MUST be implemented.

On the other hand, if you are a contractor or business associate of a covered entity you have been only loosely required to comply with the HIPAA Security Rule. Business associates were required to sign business associate agreements that contractually required them to protect patient information. That has now changed with the release of the HIPAA Omnibus Final Rule.

The new HIPAA rule makes business associates directly liable for compliance with the HIPAA Security Rule. Here is a quote from the Executive Summary of the HIPAA Omnibus rule:



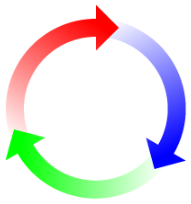
> Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.

As you can see, HIPAA compliance is not optional for covered entities or business associates.

2. **Iterative HIPAA Risk Management Process**

At the core of HIPAA security is a process called Risk Management. It sounds much more confusing than it actually is. So what is Risk Management?

Risk Management



Step A – Identify current safeguards and weaknesses

Step B – Implement additional security safeguards

Step C – Go back to Step A

Step A – Identify how you are currently protecting patient information and identify current weakness in your protection.

Step B – Implement additional security safeguards to better protect patient information

Step C – Go back to Step A

This an oversimplified definition of Risk Management but it illustrates that the process is one that must be repeated over and over.

3. You must perform a Risk Assessment

The HIPAA Security Rule and HIPAA Omnibus Final Rule mandates that all covered entities and business associates perform a Risk Assessment to determine how electronic protected health information (ePHI) is being protected and to recommend additional safeguards. A Risk Assessment is the foundation of the HIPAA Security Rule. By performing a Risk Assessment, an organization is forced to analyze where ePHI is stored and how it is currently protected. The output of a Risk Assessment provides valuable insight into vulnerabilities to ePHI and how ePHI can be better protected.

For a much more in-depth look at what a HIPAA Risk Assessment is, download our free guide to Understanding a HIPAA Risk Assessment.

If an organization were to be audited by the Department of Health and Human Services (HHS), one of the first questions is going to be “where is a copy of your latest Risk Assessment?” You don’t want to respond “we don’t have one” or produce something which is outdated or incomplete.

4. Encryption is your friend

Encryption is one of those technical terms that people have trouble understanding. While the process of encryption is very technical, there is no need to concern yourself with the technical details. Think of encryption as “an unbreakable password”. Information that is encrypted is safe and secure and cannot be accessed without the encryption password.

Although encryption is not a requirement under the HIPAA Security Rule, it does provide a “safe harbor” in the event of a security incident. If a device (laptop, desktop, USB drive, DVD, etc.) that contains ePHI (electronic protected health information) is lost or stolen and the device is encrypted, the covered entity or business associate is not required to report the breach. Encryption dramatically reduces the liability of storing ePHI on desktops, laptops and portable devices. Just remember to keep the encryption password separate from the device. In other words, don’t put the password on a sticky note on the laptop or DVD.

5. **You must train your employees on HIPAA Security**

The HIPAA Security Rule and HIPAA Omnibus Final Rule also mandate that covered entities and business associates setup a security awareness / training program and all workforce members (employees, contractors, etc.) go through security training. Training is not optional. The only way employees will understand how to protect ePHI is through training.

In addition, the HIPAA Security Rule requires that employees be provided with ongoing security reminders. In other words, all workforce members must receive training and after training they need reminders on security so they are aware of how to effectively protect ePHI. HIPAA Secure Now! provides free security reminders.

6. **You must have written policies and procedures**

The HIPAA Security Rule requires written policies and procedures which describe how ePHI is to be protected. Policies and procedures are important so that every employee knows what they need to do to protect patient information. In addition, it is important to ensure that your HIPAA training reinforces your policies and procedures.

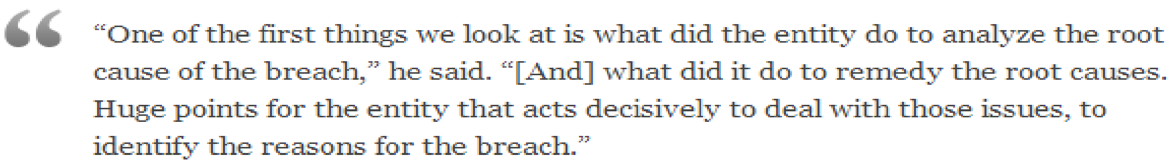
A few things to take into consideration here is that the policies and procedures need to be written. It is not good enough to have policies and/or procedures that are generally used but not written down. Policies and procedures must be documented. Another important aspect is that the written policies and procedures must be distributed and enforced by your organization. Just having a binder with written policies and procedures that sits on a practice administrator’s or head of operations bookshelf and has never been read will not satisfy the HIPAA requirement.

7. **You must have an incident response plan**

To be compliant with the HIPAA Security Rule and HIPAA Omnibus Final Rule, you must have a security incident response plan (SIRP) in place. A SIRP is a predefined plan that guides an organization through the steps which must be taken in the event of a security breach or incident. Here is an example of the high-level steps in a security incident response plan:

1. **Define the incident** – What happened? When did it happen? Who was involved? When was it discovered?
2. **Stop the incident** – if a smartphone is lost, take the steps to disable the access; if a breach is found take the steps to prevent further access, etc.
3. **Document the incident** – fill in all the details of what occurred from step 1 (define the incident) and step 2 (steps taken to stop the incident). Clearly document all aspects of the incident.
4. **Determine who has been affected by the incident** – which patient records have been affected?
5. **Perform a risk assessment** – a risk assessment will determine if the breach has led to disclosure of ePHI. The outcome of the risk assessment will determine next steps including any required notification steps.
6. **Notification** – notify appropriate individuals / agencies. The amount of patient records affected is a key determining factor of what notification steps are needed. Breaches affecting over 500 individuals require significantly more notifications. Individual patients and Health and Human Services (HHS) will need to be notified. In addition, local media may need to be notified as well.
7. **Provide guidance to prevent the incident from occurring again** – an important aspect of a security incident response plan is to ensure that the same incident does not happen in the future. Recommendations to increase security and reduce the risk of an incident are essential.

Leon Rodriguez, director of the Office of Civil Rights (OCR) at the Department of Health and Human Services, stated in an interview that having a SIRP will help organizations that experience a security breach. Rodriquez made it clear that organizations that have a SIRP in place and act quickly and decisively about large breaches will receive less severe or no monetary penalties. But organizations that do not act or correct issues related to a breach will receive much higher monetary penalties.



> “One of the first things we look at is what did the entity do to analyze the root cause of the breach,” he said. “[And] what did it do to remedy the root causes. Huge points for the entity that acts decisively to deal with those issues, to identify the reasons for the breach.”

Conclusion

Hopefully you now have a better understanding of some of the things you need to do to comply with the HIPAA Security Rule. Remember, the process to comply with HIPAA is an iterative process. Each item that you address or implement gets you a step closer to being compliant.

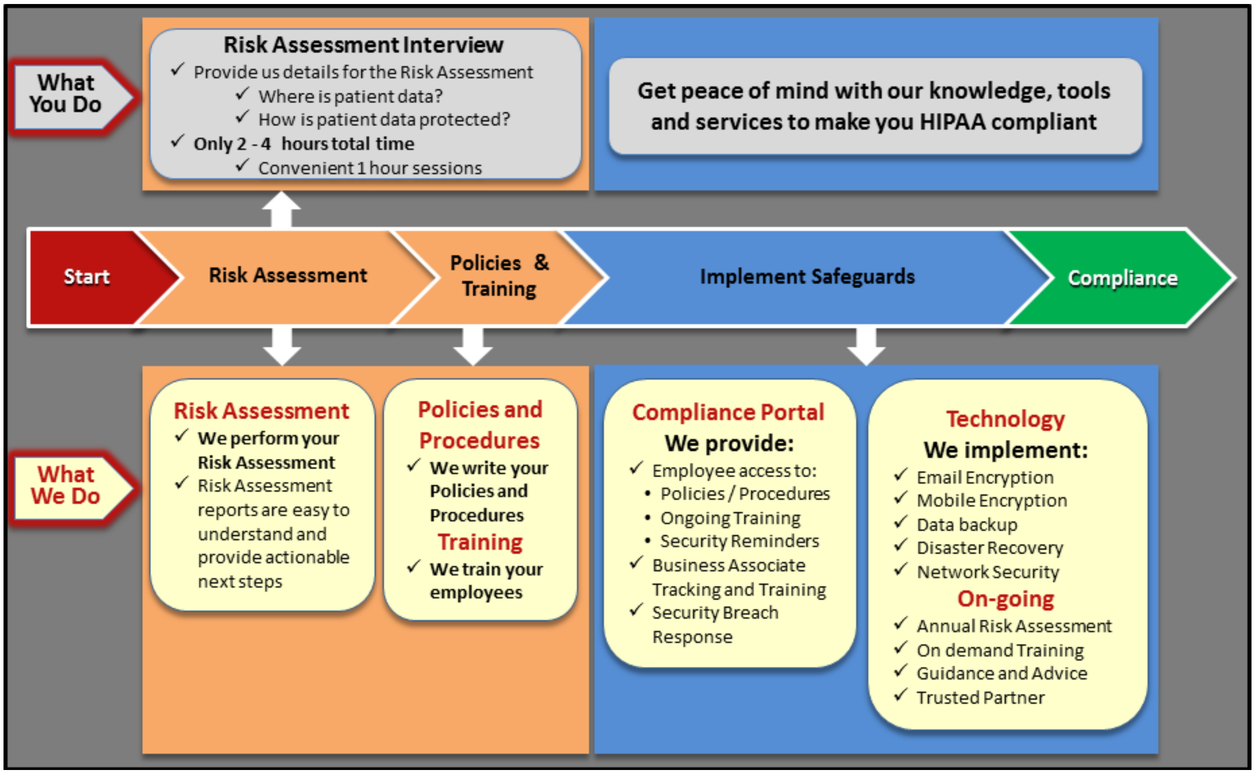
Our SmartHIPAA service can help you with your HIPAA compliance. Our comprehensive and affordable service can help you with:

- ✓ Performing a HIPAA risk assessment

- ✓ Writing your HIPAA security policies and procedures
- ✓ Training your employees and providing security reminders
- ✓ Implementing encryption to protect patient information
- ✓ Implementing a security incident response plan

And the best part is that we do all the hard work for you!

Take a look at our HIPAA Compliance Roadmap



What You Do

Risk Assessment Interview

- ✓ Provide us details for the Risk Assessment
  - ✓ Where is patient data?
  - ✓ How is patient data protected?
- ✓ **Only 2 - 4 hours total time**
  - ✓ Convenient 1 hour sessions

Get peace of mind with our knowledge, tools and services to make you HIPAA compliant

Start → Risk Assessment → Policies & Training → Implement Safeguards → Compliance

What We Do

Risk Assessment

- ✓ **We perform your Risk Assessment**
- ✓ Risk Assessment reports are easy to understand and provide actionable next steps

Policies and Procedures

- ✓ **We write your Policies and Procedures**

Training

- ✓ **We train your employees**

Compliance Portal

We provide:

- ✓ Employee access to:
  - Policies / Procedures
  - Ongoing Training
  - Security Reminders
- ✓ Business Associate Tracking and Training
- ✓ Security Breach Response

Technology

We implement:

- ✓ Email Encryption
- ✓ Mobile Encryption
- ✓ Data backup
- ✓ Disaster Recovery
- ✓ Network Security

On-going

- ✓ Annual Risk Assessment
- ✓ On demand Training
- ✓ Guidance and Advice
- ✓ Trusted Partner

If you would like to learn more about our comprehensive SmartHIPAA, feel free to contact us at office@smartpathtech.com .