SmartHIPAA!

Understanding a HIPAA Risk Assessment

SmartHIPAA

Turnkey HIPAA compliance

Understanding a HIPAA Risk Assessment

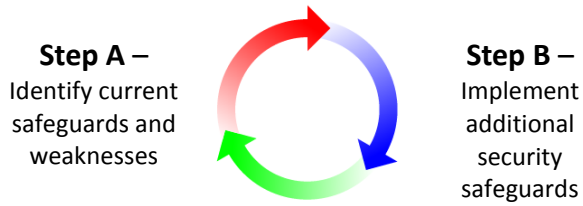
In order to protect patient information it is important to understand the risks to the information. A HIPAA Risk Assessment will help you answer the following questions:

1. Where is patient information stored, accessed, created or modified?
2. What are threats to this information?
3. How likely are these threats?
4. What is the impact of these threats?
5. What additional security measures can be implemented to protect the information?

Iterative 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 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 is repeated over and over.

Risk Assessment

How do you identify how you are protecting patient information and your weaknesses? The HIPAA Security Rule and Meaningful Use requirements call for all organizations to perform a HIPAA Risk Assessment. Let's look at a simplified definition of a Risk Assessment.

Step 1 – Identify where patient information is stored (EMR, PACS system, email, etc)

Step 2 - Identify threats to patient information (employee loses a laptop with patient information, fire destroys your EMR, a patient is sent another patient's test results, etc.)

Step 3 – Assess how you are currently protecting patient information (backing up your EMR on a nightly basis, using secure email to send patient information, using anti-virus to protect your systems from viruses, etc.)

Step 4 – Determine your risk for each of the threats that were identified in Step 2. You determine your risk by looking at how likely something is to happen and the impact if it does happen. Let's look at an example to better explain risk.

Risk of a fire destroying your EMR

How likely is it that a fire will destroy your EMR? The risk is probably very low. Fires happen but the probability of a fire is low.

What is the impact of a fire destroying your EMR? Your first reaction might be "the impact would be huge!" There is no denying that a fire would impact your organization but you have to look at the impact more closely.

Let's look at the worst case scenario first. If a fire destroys your EMR and the data has not been backed up, all your patient information would be lost forever. You could not recover the information. Months or even years of patient records would be gone. You would have no history of any of your patients. This scenario could put your practice out of business and even jeopardize the health of your patients. It is hard to argue that the impact would not be great.

Let's look at another scenario where the impact would not be as severe. If your EMR data is backed up on a nightly basis and stored offsite, a fire would not have the same impact as in the first scenario. Yes your server would be destroyed and your patient information would be inaccessible but it would not be lost forever. You could purchase another server from Dell or HP. You can have your IT staff or company setup a new server. You can have your EMR vendor reinstall the EMR software. You can restore your

EMR data from backup. It may take some time but you would eventually have your EMR and patient information up and running and accessible once again.

The impact of the second scenario is obviously much less severe than the impact of the first scenario where all your patient information data is lost forever.

Step 5 – Determine additional protections to lower the risk. Using the previous example, if you determined the risk of a fire would be high because you are not backing up your data then implementing a nightly data backup would lower your risk.

Again, these 5 steps are an oversimplified explanation of a Risk Assessment but hopefully it gives you a better understanding of the process. The key is to identify the risks that could have major impact to your organization and identify additional protections that could lower the risks.

Conclusion

Hopefully you have a better understanding of the HIPAA Risk Management process and the benefits of performing a HIPAA Risk Assessment. Risk Assessments should be performed once a year (or at most once every two years) or when major changes to systems occur (i.e. implementation of an EMR or Digital X-ray system).

Our SmartHIPAA service offers a streamlined yet extremely comprehensive Risk Assessment process which absolutely minimizes the time you will need to spend providing information. We have studied the HIPAA regulations and based upon them designed the initial questions which need to be asked, as well as the appropriate follow-ups based on your responses. The results of your assessment will be documented in an understandable format which includes actionable recommendations to better protect your patient information. All of this service and protection comes at a very affordable price. If you would like to discuss a HIPAA Risk Assessment or learn more about our comprehensive SmartHIPAA, feel free to contact us at office@smartpathtech.com .