SmartHIPAA!

5 simple and inexpensive tips to protect patient information

SmartHIPAA

Turnkey HIPAA compliance

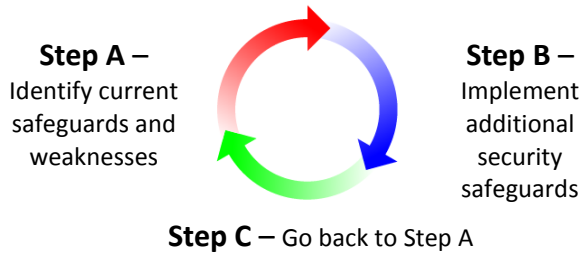
5 simple and inexpensive tips to protect patient information

HIPAA security guidelines can be confusing and compliance expensive. Yet there are simple and inexpensive tips you can take to secure patient information. The first thing to realize is that HIPAA security is a process and takes time to implement. No one becomes "HIPAA compliant" overnight. There is no magic product to purchase or book to read that will make your organization instantly HIPAA compliant.

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. This paper will focus on some of the things you can do for Step B but let's briefly look at Step A.

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.

By now you may be saying to yourself "Okay, I understand the concept of risk but where are the simple and inexpensive tips I can take to secure patient information?"

Simple and inexpensive tips to secure patient information

A majority of HIPAA related breaches to patient information happen due to lost or stolen portable devices. Portable devices include laptops, USB drives, CDs, DVDs, Backup tapes, Smartphones, etc. These portable devices can hold hundreds or thousands of patient records. There are a few simple and inexpensive ways of protecting portable devices to minimize the risk of losing patient information. Four of the tips will focus on portable devices and the fifth tip will look at how good password controls can protect patient information.

Tip #1 – Encrypt all laptops

We are not going to get into the details of data encryption and you don't need to fully understand what data encryption is to understand the benefits. The HIPAA Security Rule states that if patient data is encrypted and the data is lost or stolen there is no need to notify patients or report the breach. The official description of encryption is that it is a Safe Harbor under the HIPAA Security Rule but we like to call it the "get out of jail free card". If you lose a laptop with patient information and it is encrypted you can act, for HIPAA compliance purposes as though it was never lost. It costs less than $100@year to encrypt a laptop. Encryption usually has no noticeable effect on using the laptop and only requires a password to be entered when you first startup the laptop.

We have heard arguments from clients that "our laptops don't have any patient data on them so why should we encrypt them?" While it may be true that you did not intend the laptop to contain patient information, the fact is it COULD contain patient information.

There could be emails with patient information; spreadsheets, documents or PDFs with patient information could be stored on the laptop; reports downloaded from an EMR could be on the laptop. If a laptop is lost or stolen the process of trying to figure out what data was stored on the laptop would likely cost you much more than the cost to encrypt the laptop in the first place. Bottom-line, if your laptops are encrypted you no longer have to worry about a HIPAA breach if they are lost or stolen

Tip # 2 – Minimize the use of portable devices and the amount of data on portable devices

In order to reduce the risk of losing patient information stored on a portable device, make it a practice to not use portable devices. Raise your employee awareness of the risks of portable devices. Write a memo or send an email to all employees stating that the use of portable devices to store patient information is frowned upon. If employees must use portable devices then the amount of patient information stored on the devices should be only the minimum needed.

If USB drives must be used then only use encrypted USB drives. While it is true that encrypted USB drives are more expensive than non-encrypted USB drives, the cost is not prohibitive.

Tip #3 – Encrypt all backup tapes

If you are still using tapes to backup your data then ensure that they are encrypted. Backup tapes hold all your data. If a backup tape is lost or stolen you could have a very large data breach. Don't assume your IT people are using encryption on your backup tapes. Have a conversation with your IT people and confirm that they are encrypting your tapes. Most backup software supports data encryption but it must be enabled first.

Tip #4 – Ensure you have a startup password and inactivity timeout on your smartphone

Smartphones such as iPhone, Android, Windows Phone and BlackBerry may contain patient information. More and more smartphones are used to access EMRs, imaging systems, etc. In addition, more and more patient information is contained in emails between physicians, physician assistants, billing departments, etc. Smartphones are easily lost or stolen and represent a risk to the patient information that they may contain. So what can be done to protect the information in the event that a smartphone is lost or stolen?

Smartphone Safeguards

There are many safeguards you can put in place to reduce the risk of data breaches caused by smartphones. Here are 3 safeguards that will go a long way to minimize the impact if your phone is lost or stolen.

1. Minimize the amount of patient data that is sent via email
2. Protect your smartphone by ensuring that a start-up password and inactivity timeout has been implemented
3. Implement data encryption on your smartphone

You can reduce the impact of a lost smartphone by minimizing the amount of patient data that is on the phone. By implementing a start-up password, inactivity timeout and utilizing data encryption, you can reduce the likelihood that patient information is compromised if the phone is lost or stolen.

Tip #5 – Implement good password controls

Passwords are the key to protecting systems that contain patient information. The stronger the passwords that your employees use the more secure your systems are. Here are a few inexpensive ways to ensure you implement good password controls.

Complex Passwords

Encourage employees to use complex passwords that have upper and lower case letters, special symbols such as "@ ! $ % &" and numbers. The more complex the password the harder it is to guess or crack. Keep in mind that your employees probably have so many different passwords that they will not be too happy to have another password especially if it is hard to remember. You will have to ensure they understand the importance of protecting patient information and the importance of using complex passwords in order to respond to any employees' resistance.

Don't write passwords down

Passwords should not be written down. They should not be stuck to monitors on yellow sticky notes. They should not be on a piece of paper under the keyboard. Passwords, like credit card and social security numbers should be protected and not shared.

Lock accounts after failed password attempts

Accounts should be locked after a number of failed passwords attempts. For example if an employee enters their passwords incorrectly 5 times the account should be locked and require the network administrator to unlock the account. Account lock outs prevent passwords from being guessed or hackers from using special tools to break into accounts. Needing to reset passwords may be a little inconvenient, but account lockouts are a very effective way to protect patient information from unauthorized access.

Conclusion

We mentioned a few simple and inexpensive tips that you can easily implement to protect patient information and help you toward HIPAA security compliance. Following these tips will go a long way toward providing increased protection of your patient information. If you would like to discuss implementing these safeguards, or learn more about our comprehensive SmartHIPAA, feel free to contact us at office@smartpathtech.com