HIPAA Security Risk Analysis Toolkit

MGMA
Medical Group Management Association

Medical Group Management Association

HIPAA Security Risk Analysis Toolkit

In January of 2013, the Department of Health and Human Services Office for Civil Rights (OCR) released a final rule implementing a wide range of HIPAA privacy and security changes. The long awaited "omnibus" regulation finalizes three rules mandated by the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, including breach notification for unsecured protected health information (PHI), enhanced enforcement authority, and a variety of other privacy and security changes.

This omnibus regulation expands the current requirements set out in the 2005 HIPAA Security Rule. That rule requires you to evaluate the risks and vulnerabilities in your practice and to implement security measures to protect against any threats to the security or integrity of electronic PHI. Conducting a comprehensive risk analysis is the first step in that process. Not only is this risk analysis a HIPAA Security rule requirement, it is also a requirement Stage 1 and Stage 2 of the Medicare and Medicaid EHR Incentive Program (Meaningful Use).

INTRODUCTION

Medical group practices are increasingly relying on health information technology to conduct the business of providing and recording patient medical services. Practices are now utilizing laptops, tablets, smart phones and more that both collect and utilize patient clinical data. With Medicare's Meaningful Use program, many organizations have transitioned to EHR systems to capture clinical data. The patient's data held in your EHR, and other electronic tools, is called electronic protected health information or ePHI. All ePHI created, received, maintained and/or transmitted by your practice is covered by the HIPAA Security Rule.

It's critical that practices take the appropriate steps to ensure that ePHI is kept secure and confidential. One important step to ensure that your practice's ePHI is adequately protected is to conduct a risk analysis of all your electronic tools and systems that hold and/or have access to patients' medical records.

A risk analysis is a technique used to identify potential problem areas and assess security protocols to protect your practice against any potential threats. The basic questions practices must ask themselves are: where are all ePHI within our organization located, where is it stored and used, how is it currently protected, is our current method of protection adequate, and, if not, what must we do to protect it?

We have provided this risk analysis toolkit to guide you in developing the appropriate policies and procedures that meet the specific needs of your practice, and help ensure that your organization is in compliance with the HIPAA Security Rule. As well, this toolkit will also help you in meeting the security risk analysis portion of the Meaningful Use program requirements.

MGMA is pleased to have partnered with Susan A. Miller, JD, one of the nation's foremost HIPAA Security experts, in the creation of this member resource. We hope that you find this toolkit helpful as you take on the challenging task of reviewing your current security environment.

TABLE OF CONTENTS

OVERVIEW

Health care lags significantly behind other industries in security; practices face unique challenges with limited resources. It's important to be aware of the potential risks, such as:

- Loss of patient financial data (identity theft)
- Permanent loss of confidential information
- Temporary loss of medical records
- Unauthorized access to confidential information
- Loss of physical assets (i.e., computers, tablets, smart phones)
- Damage to practice reputation, patient confidence
- Business continuity

When conducting a risk analysis the first critical question you need to ask is "*What are the potential areas of threat to my practices ePHI?"* Identifying all devices, tools and technologies that hold, or have the potential to hold, your practices ePHI is the starting point to conducting a risk analysis.

This toolkit will examine a number of potentials areas of threat to your ePHI. While not exhaustive, the issues included in this toolkit represent high priority concerns that practice professionals will commonly encounter. Some of these issues may be new to your practice while others may have been implemented many years ago. Regardless of when your practice adopted these technologies and/or protocols, conducting a thorough assessment is critical.

Each area of risk discussed in this toolkit will provide:

1. A brief background
2. Six essential steps to assess the potential risk(s)
3. A sample policies & procedures template practices may use to update their current protocols

CHAPTER 1 – MOBILE DEVICES

Mobile devices include:

- Laptops
- Tablets
- Smart phones
- Clinical tools

Mobile tools have largely taken the place of large, unmovable, computing workstations. Today, many practices are utilizing only laptops and tablets to access ePHI. In addition, many clinicians and other practice professionals are using smart phones to directly access the office scheduling system and other patient ePHI. Further, some organizations permit remote access to the EHR from the clinician's home.

As part of the risk analysis, practices will need to review and catalogue its current and expected use of mobile devices. This list of devices will change as the technology within your practice changes. Each device and protocol must be reviewed for potential threats to the security of ePHI.

MGMA
Medical Group Management Association

MOBILE DEVICES

1 IDENTIFY THE POTENTIAL RISKS:

- Loss or theft of a mobile device
  - Leaving it in a public area, outside of the practice (i.e., conference room of the hospital, backseat of a car)
  - Leaving a device on and open within the office so that unauthorized individuals can see patient data
- Lack of password protection and automatic log-off capabilities
- Unencrypted data

2 ANALYZE "HOW LIKELY COULD THIS OCCUR?"

- How many clinicians have access to a mobile device?
- Do non-provider employees have access? If so, what do they have access to?
- Does the practice permit clinicians or other staff to take a mobile device outside of the practice?

3 IDENTIFY WHAT YOUR PRACTICE CURRENTLY DOES TO PROTECT ePHI:

Data encrypted on all mobile devices?
What are our existing policies and procedures?

4 ASSESS THE IMPACT TO YOUR PRACTICE IF A DATA LOSS DOES OCCUR:

What steps will practice staff have to take in the event of a data loss?
What is the potential cost to the practice of a data loss?
What could a data loss mean in terms of lost patient confidence?
If the ePHI on the lost device is not encrypted it will be a breach, and you will need to report this to the HHS Office for Civil Rights (OCR)

5 DETERMINE WHAT METHOD(S) YOUR PRACTICE SHOULD USE TO ADDRESS THREATS:

- Inventory your mobile devices
- Number your mobile devices
- Assign you mobile devices to one individual, even if more than one person may use it in the office
- Password protection
- Automatic log-off
- Encrypt the data in all mobile devices while at rest
- Train your staff in the use of mobile devices inside and outside of the practice

6 EVALUATE HOW YOUR EHR SYSTEM COULD HELP:

Generally not in this case, although you should talk to your EHR vendor regarding the potential of using mobile devices to provide remote access to the EHR's data, but not have that data stored on the mobile device.

Next are a few suggestions you might need in Workstation Policies and Procedures that includes your practice's mobile devices. Note that the information below may not be complete or sufficient to meet your individual practice requirements.

Workstation Policy and Procedures
(Mobile Tools Policy and Procedure should be part of)

Purpose

[Practice name] is obligated to establish safeguards to protect ePHI and other PHI, confidential information and business information. This policy establishes [Practice name]'s procedures with respect to security measures to protect [Practice name]'s electronic information systems.

Scope

This policy applies to all [Practice name] staff members. All staff must be on the lookout for any potential problems that could jeopardize the security of electronically stored information, especially ePHI.

Procedure

Workstation Security and Use

A "workstation" is defined as any electronic computing device, such as a desktop computer, laptop computer, PDA, a tablet, smart phone or any other device that performs similar functions, and electronic media stored in its immediate environment.

General principles of [Practice name]'s workstation security program include the following:

1. All workstations are set with password protection so that the computer may not be accessed without the proper password;

2. All workstations are set up to go "inactive" after a set time period so that if the staff member leaves the workstation and forgets to logout or shut down, access will not be permitted without the proper password; at this time this is set at 10 minutes;

3. All screens will be pointed away from hallways and open areas. The screens will be pointed away from chairs or other locations in the office where unauthorized persons, such as patients, may sit within that office;

4. Workstations will be set so that staff members may not inadvertently change or disable security settings, or access areas of the information system they are not authorized to access;

5. Only those authorized to access and use the workstation will be permitted to use the workstation;

6. No software may be downloaded or installed on the workstation in any manner without prior authorization. This prohibition includes computer games, screen savers and anti-virus or anti-spam programs;

7. All staff members will "log off" the workstation whenever it is left unattended; and

8. Use of mobile devices is granted by the [Practice name]'s _____;

9. All mobile devices will have necessary security and privacy controls prior to use.

CHAPTER 2 – THE INTERNET AND PROTECTING EMAIL

The Internet is a useful tool in many practice offices but is also an open environment-meaning that the Internet has no centralized governance in either technological implementation or policies for access and usage. Making control even more challenging, Internet usage in your office is often through the mobile tools discussed in Chapter 1, laptops, tablets, and now through smart phones.

OCR has addressed the issue of email in an FAQ:

Question: ***Does the HIPAA Security and Privacy Rules permit health care providers to use e-mail to discuss health issues and treatment with their patients?***

Answer:

Yes. The HIPAA Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. See 45 C.F.R. § 164.530(c). For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail. In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 C.F.R. Part 164, Subpart C.

Note that an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. See 45 C.F.R. § 164.522(b). For example, a health care provider should accommodate an individual's request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that provider to communicate with the patient. By the same token, however, if the use of unencrypted e-mail is unacceptable to a patient who requests confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated.

Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

Found at: http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570.html

Thus, while you cannot stop your patients from communicating with your practice through email and putting PHI into the email, what you can do in these circumstances is educate your patients that this is unsafe and that your office will not reply by email.

It is important to remember that in many instances your patient's employer owns the rights to the employee's work email address and h[illegible]ese emails. There could be a negative

outcome for the patient (and potentially for the practice) should sensitive information be sent by the practice to a patient's work email address, and read by the employer.

Example:

There is a doctor who has been using email in his practice for over ten years now. He has printed on the back of his business card his office email and website address, how to use these, what is ePHI, what the risks are, and what might happen to ePHI communicated this way. While his email address is provided to patients, he suggests that no patient sends him ePHI and instructs his office not to send PHI in emails to patients, or post anything to an Internet site about patients or their medical information.

Standard Operations

The Internet is a very useful tool, but it must have reasonable "rules of the road" associated with its use, and only for your practice's standard operations. Examples of Internet use as part of your practice's standard operations include:

- Staff going online to determine patient eligibility
- Check on claims payment status
- Ordering business supplies over the web
- Ordering clinical supplies over the web

There are many uses of the Internet, however, that are not part of your practice's standard operations. These include sending a threatening or harassing email or visiting inappropriate websites. While these uses of the Internet should be strictly prohibited, each practice will need to develop their policy regarding personal use of the Internet for non-work related tasks. Some may decide to restrict this type of use complexly, others may allow it when staff is on break, or the practice may choose to simply encourage employees to limit personal use of the Internet during working hours.

MGMA
Medical Group Management Association

THE INTERNET

1 IDENTIFY THE POTENTIAL THREATS:

- Accidently sending ePHI to the wrong person
- Putting ePHI in open emails
- Giving a hacker the opportunity to pick off the email
- Misusing access to the Internet
    - Access to “adult sites”
    - Personal purchase

2 ANALYZE HOW LIKELY A THREAT COULD OCCUR

The Internet is ubiquitous and is used by almost everyone; so many think is fine to use the Internet for any purpose while at work

3 IDENTIFY WHAT YOUR PRACTICE CURRENTLY DOES TO PROTECT ePHI:

Passwords?
Access controls?
Encryption?

4 ASSESS THE IMPACT TO YOUR PRACTICE IF A THREAT DOES OCCUR:

If the ePHI on the lost tool is not encrypted it will be a breach, and you will need to report this to the Office for Civil Rights (OCR)

5 DETERMINE WHAT METHOD(S) YOUR PRACTICE SHOULD USE TO ADDRESS THREATS:

- Encrypt any ePHI that you send over the Internet
- Internet policy and procedures that state do not put ePHI in emails
- Train your office staff on the do’s and don’ts’ of office Internet use

6 EVALUATE HOW YOUR EHR SYSTEM COULD HELP:

Your office EHR system may assist in sharing ePHI with hospitals and other physician practices, plus laboratories; much of this sharing may be on the Internet, but through portals

Next are a few suggested Internet and Email Policies and Procedures. Note that the information below may not be complete or sufficient to meet your individual practice requirements.

Internet Access and Use
(Including email Use)

Purpose

Internet access to global electronic information resources on the World Wide Web (www) and through [Practice name] e-mail system is provided by [Practice name] to assist staff members in obtaining work-related information ONLY.

All ePHI transmitted over the Internet will be encrypted.

There will be no ePHI sent in emails.

Scope

This policy applies to all [Practice name] staff who have access to the Internet. This policy also applies to all Internet access using [Practice name] equipment, as well as Internet access when personal equipment is used, such as laptops, tablets, PDAs and smart phones.

Procedure

All Internet data transmission, website use and review, or e-mail that is composed, transmitted or received via [Practice name] computer communications systems is considered to be part of the official records of [Practice name] and, as such, is subject to disclosure to law enforcement or other third parties. Consequently, staff members will always ensure that the information contained in Internet e-mail messages and other transmissions is accurate, appropriate, ethical and lawful.

The equipment, services and technology provided to access the Internet and electronic mail system remain at all times the property of [Practice name]. As such, [Practice name] may monitor Internet traffic without your knowledge, and retrieve and read any data composed, sent or received through [Practice name] online connections and stored in [Practice name] computer systems.

Data that is composed, transmitted, accessed or received via the Internet or e-mail must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation or any other characteristic protected by law..

Abuse of Internet access and the e-mail system in violation of the law or [Practice name] policies will result in disciplinary action, up to and including termination of employment. Staff members may also be held personally liable for any violations of this policy.

The following behaviors are examples of actions and activities that are prohibited and can result in disciplinary action:

1. Sending or posting discriminatory, harassing or threatening messages or images;

2. Accessing any web sites that are pornographic in nature, including any “adult sites”;

3. Using the organization’s time and resources for personal use or pleasure without prior authorization;

4. Stealing, using or disclosing someone else's code or password without authorization;

5. Copying, pirating or downloading software and electronic files without permission;

6. Sending or posting confidential material, trade secrets or proprietary information outside of the organization;

7. Sending or posting messages or material that could damage the organization's image or reputation;

8. Sending or posting messages that defame or slander other individuals;

9. Attempting to break into the computer system of another organization or person;

10. Refusing to cooperate with a security investigation;

11. Sending or posting chain letter, solicitations or advertisements not related to business purposes or activities;

12. Using the Internet for political causes or activities, religious activities or any sort of gambling;

13. Sending or posting messages that disparage another organization's products or services;

14. Sending anonymous e-mail or text messages;

15. All software used to access the Internet shall be configured to use a firewall;

16. Non-business related purchases made over the Internet are prohibited. Business related purchases are subject to [Practice name] procurement rules; and

17. All sensitive [Practice name] material, especially PHI and ePHI, transmitted over external networks must be encrypted.

Note: A federal secure email messaging service is being developed called DIRECT that is gaining in popularity and is more and more usable. It is free for anyone who wants to use it. You may find out more about direct at http://www.healthit.gov/policy-researchers-implementers/direct-project.

CHAPTER 3 – ENCRYPTION, INCLUDING CLINICIAN-TO-CLINICIAN DATA SHARING

Under the HIPAA Rules ePHI is considered unsecured if it is not encrypted. Under the HIPAA Rules encryption is not required. Under Stage 2 of the Meaningful Use requirements, encryption is specifically mentioned as an issue that must be addressed by eligible professionals.

Encryption is the electronic scrambling of ePHI so that no one can read it or decrypt it, or open it unless they have the proper "key." Today, encryption technology is available for Internet communications as well as email.

Encryption is an inexpensive way to secure and protect your patients' medical information, especially if it is compared to the expense the practice would incur if it experienced a breach of ePHI.

OCR has increased its enforcement activity in recent years, and small providers are not exempt. As an example, OCR fined a hospice in Idaho $50,000 in 2012 for the loss of a laptop. In comparison, the cost to secure your mobile tools is from $50 - $200 per tool. If your practice has four laptops and four tablets the encryption costs would most likely be $1,600. In addition, some estimates are that the cost to identify the cause of a breach, correct the problem, train appropriate staff and complete the patient notification process can be more than $200 per individual record.

There are many ways to send patients' medical information from one clinician to another clinician. You can call your colleague, fax data, have a face-to-face conversation, or use the U. S. Mail.

Joining two areas together – how might you send patients' medical information clinician-to-clinician electronically using encryption? For clinician-to-clinician, or office-to-hospital communication, your EHR system may have the capability of performing that now or it may be coming very soon. Discuss this with your EHR vendor.

In Meaningful Use Stage 2, there is a requirement that you offer your patients an online portal that permits them to view, download and transmit their health information and provide them a method to send the practice a secure electronic message. A minimum of five percent of your patients must use this portal and engage in secure messaging. Plus, your office EHR system may be connected to a Health Information Exchange (HIE) for the sharing of the patients' medical information in a secure and protected way to other physicians, hospitals, and laboratories.

MGMA
Medical Group Management Association

ENCRYPTION

1 IDENTIFY THE POTENTIAL THREATS:

Misuse or improper disclosure of your patients' medical information, their PHI

2 ANALYZE HOW LIKELY A THREAT COULD OCCUR

3 IDENTIFY WHAT YOUR PRACTICE CURRENTLY DOES TO PROTECT ePHI:

- PHI in emails?
- PHI from your office EHR system to another EHR system
  - Directly
  - Through an Health Information Exchange (HIE)

4 ASSESS THE IMPACT TO YOUR PRACTICE IF A THREAT DOES OCCUR:

The costs can be rather substantial. Using the hospice example from above:

- Fine = $50,000
- Cost of notification, and loss of reputation is approximately $200 per patient
  - 441 hospice patients x $200 = $88,200
- Cost of a consultant to do the risk analysis and other work, at least $150 per hour
  - 100 hours x $150 = $15,000
- TOTAL COST = $153,200.

5 DETERMINE WHAT METHOD(S) YOUR PRACTICE SHOULD USE TO ADDRESS THREATS:

- Mandating in your policies and procedures the use of encryption in all mobile tools
- Mandating in your policies and procedures the use of encryption for emails, or no ePHI in emails
- Mandating in your policies and procedures the use of encryption in Internet transmission

6 EVALUATE HOW YOUR EHR SYSTEM COULD HELP:

- Your EHR system may have both a portal and a connection to one or more HIEs
- You should to talk to your EHR vendor about encryption options
- Explore the potential of using an online portal to communicate securely with other provider offices

Next are a few suggestions you might need in Encryption and Decryption Policies and Procedures. Note that the information below may not be complete or sufficient to meet your individual practice requirements.

Encryption and Decryption of ePHI

Purpose

[Practice name] is responsible for ensuring the security of all PHI that [Practice name] creates, receives, maintains or transmits under both the Privacy Rule and the Security Rule of HIPAA and the HITECH Act privacy and security requirements.

Security involves protection of ePHI, PHI and other important [Practice name] information during its transmission and receipt via electronic means such as electronic mail and file, information or software transfers. Encrypting and decrypting electronic information and files during their "transit" is a technical means of ensuring that if the information or files are intercepted or end up in the wrong hands, they cannot be deciphered or interpreted.

While [Practice name] is not legally required to "encrypt" electronic information or files in most cases, [Practice name] is obligated to ensure that ePHI, PHI, and other important patient or [Practice name] information does not fall into the wrong hands or is viewed or used by those who will not have access to it. Thus, it is the policy of [Practice name] to use encryption or decryption techniques wherever possible for both ePHI at rest and ePHI in transmission.

Scope

This policy applies to all [Practice name] staff members who are responsible for the manner in which ePHI and other important [Practice name] information is transmitted or received by the [Practice name].

Procedure

1. The Privacy or Security Officer has, as part of a risk assessment, identified all transmission and reception points for electronic information to determine:

    a. Where the information is sent;

    b. The type of information that is sent; and

    c. The general content of the information to determine if it contains ePHI or other important or confidential information.

2. The Privacy or Security Officer has determined that:

    a. Encryption and decryption of the information will be implemented based on the type of information, its destination (internal or external) and the risk of improper interception;

    b. Encryption and decryption of the information has been implemented when the data is at rest and when it is in transmission outside the corporate firewall;

3. Encryption/decryption is implemented; a careful review of all available technology, its features, and the ability to maintain and upgrade the software in the future.

    At all times [Practice name] encryption standards shall meet or exceed the standards outlined in the Breach Notification Final Rule published on January 25, 2013 including the encryption processes of the National Institute of Standards and Technology (NIST) and judged to meet this standard outlined in the final rule.

CHAPTER 4 – SHREDDING

Shredding is a practical way for any practice to implement the HIPAA Security Rule requirements of disposal of devices and electronic media, as well as paper PHI. This area is part of the physical protections' within the HIPAA Security Rule that will be discussed further in Chapter 7.

Shredding is the complete destruction of either paper that holds patients' medical information or the electronic media and tools, such as a USM "thumb" drive, CD-ROM, laptop or tablet, or any other device that electronically holds patients' demographic, clinical, and/or payment information.

Patients' electronic information is held on what are called "hard drives" in your office devices. You will typically find hard drives in:

- Laptops
- Tablets
- Fax machines
- Copier + Printer machines
- Clinical tools

Paper PHI includes the patients' medical records, images and test reports that are not scanned into electronic tools.

Example:

CVS Drugstores were fined $2.5 million by OCR for throwing un-shredded paper documents that contained PHI in dumpsters in several states. (Remember that CVS, as a provider of pharmacy services, is a covered entity under HIPAA.)

Often your office copier, printer and fax are a 3-in-1 machine; meaning that the machine does all three (3) types of work. These devices could also store patient information.

It is important to remember that simple deletion of electronic files or folders is not sufficient to ensure complete removal of the file or data from the device. This only removes the directional "pointers" that allow a user to find the file or folder more readily. Deleted files are usually completely findable with special software and computer system expertise.

Example:

When the HIPAA regulations were new over 10 years ago many doctors' offices gave their old computers to public libraries and public schools. This was and continues to be a very good community idea. But in the beginning the patients' ePHI was not removed from the computers and this could be accessible by the new users..

However, most practices have a shredding company that collects and destroys their paper that contains PHI. Now shredding companies can physically destroy hard dives after they are removed from the laptop, tablet, fax machine, copier, printer or clinical tool. This is by far the best way, and the best practice, to permanently remove ePHI from any electronic tool.

SHREDDING/DESTRUCTION

1 IDENTIFY THE POTENTIAL THREATS:

Misuse or improper disclosure of PHI or ePHI

2 ANALYZE HOW LIKELY A THREAT COULD OCCUR

VERY! If you do not shred paper and destroy hard drives!
All breaches are either a paper or electronic misuse or improper disclosure of PHI!

3 IDENTIFY WHAT YOUR PRACTICE CURRENTLY DOES TO PROTECT ePHI:

- Laptops, how many do you have?
- Tablets, how many do you have?
- Fax machine (or do you use computer-to-computer fax)
- Copier(s), how many to you have?
- Printer(s), how many do you have?
- Clinical tools; name the ones you enter patient demographics into

4 ASSESS THE IMPACT TO YOUR PRACTICE IF A THREAT DOES OCCUR:

If the ePHI or PHI is not shredded or destroyed and is lost or stolen, it could be a breach, and thus would need to be reported to OCR. This will result in practice expense to notify patients and could result in government fines.

5 DETERMINE WHAT METHOD(S) YOUR PRACTICE SHOULD USE TO ADDRESS THREATS:

- Good policies and procedures
- Staff training
- Making it easy for your staff to report problems
- Once you know of a problem, fix it immediately

6 EVALUATE HOW YOUR EHR SYSTEM COULD HELP:

No, not with shredding or destruction; but it does and will provide many other security protections.

Next are a few suggestions you might need for your Device and Media Controls Policies and Procedures. Note that the information below may not be complete or sufficient to meet your individual practice requirements.

Device and Media Controls

[Practice name] carefully monitors and regulates the receipt and removal of hardware and electronic media that contain ePHI, PHI and other patient and business information into and out of the facility. These controls pertain to the movement, re-use or disposal of hardware and media within [Practice name] facility.

Disposal. [Practice name] has in place procedures governing the disposal of hardware and electronic media:

1. Sanitizing Hard Disk Drives: All hard disk drives that have been approved by the Privacy or Security Officer for removal and disposal or taken out of active use shall be sanitized so that all programs and data have been removed from the drive. [Practice name] will follow industry best practices when cleaning off hard drives;

    a. [Practice name] will destroy hard drives when they will no longer be used.

    b. No hard drive will be reissued, sold or otherwise discarded. It will be destroyed.

2. Media Re-Use: All ePHI and other patient and business information shall be removed from any media devices before they are made available for reuse;

3. All Media on which the PHI is stored or recorded will be destroyed in one of the following ways:

    a. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed; and

Electronic media and tools hard drives have been shredded or destroyed such that the ePHI cannot be read or otherwise cannot be reconstructed.

CHAPTER 5 - ACCESS TO ePHI

The HIPAA Security Rule includes a Health Access Management Standard that outlines how individuals, staff, are authorized to gain access to and use the ePHI in their work.

There are a number of steps necessary to gain access to ePHI for employees at a medical practice.

They must first be trained on the practice's HIPAA policies and procedures before they are permitted to have access. *Employees need to know how to secure the PHI and ePHI, plus how s/he may use or disclosure the patients' medical information.*

Second, employees must have a user ID and password to get onto the system and into specific functions specific to their job and its tasks. *Think of what could happen when employees, for example, share a user ID and/or passwords.*

Example:

Soon after HIPAA went into effect, a hospital medical records director took her teenager to work on a weekend, and set the child up on an unused computer to play games. The child went into the medical records finding the HIIV/AIDs list of patients and emailed the list to the local newspaper.

Next, if employees change jobs within the practice they may need to have access to a different part of the office EHR system and electronic tools than they were using previously.

- *Consider, for example, what could happen if a nurse who works with the pediatric practice in a multi-specialty practice, and then assists with claims management for the practice evenings and weekends, s/he has a need for different populations and differing parts of the medical record to do these two distinct jobs.*

Plus, you need to understand the special needs if you permit a staff member to work remotely, and s/he is permitted through a portal into your EHR system and electronic data held on other tools. The security for the remote work should be no different than if the staff member were working in the office.

- *Consider what might happen if your employee is working from home and children also use the computer. It is critical that sessions be closed down and that adequate password protections are in place.*
    - *This might be a breach as someone who was not supposed to see the ePHI did see the ePHI*
    - *Remember a computer is often a family communication too.*

Finally, at the end of the employment for an employee there needs to be a termination checklist to make sure the practice gets back all its keys to the physical environment, and to disable the sign-on ID and password for the staff member who is no longer employed in your office.

- *Consider what might happen if you do not get the key to the door back.*
- *Consider what might happen if you do not revoke a user ID and password and you permit remote access to your EHR system.*

ACCESS TO ePHI

1 IDENTIFY THE POTENTIAL THREATS:

- Individuals sharing passwords
- Passwords written on a sticky and placed in an easily seen location
- Forgetting passwords
- Leaving your computer on when you walk away (both in the practice and outside if remote access is permitted)
- Terminating work, but not user IDs and passwords

2 ANALYZE HOW LIKELY A THREAT COULD OCCUR

In a fast paced medical practice one of these mistakes will happen unless one individual has the responsibility for this area of granting and revoking access to ePHI

3 IDENTIFY WHAT YOUR PRACTICE CURRENTLY DOES TO PROTECT ePHI:

- Current policies and procedures?
- Who is assigned to be responsible for granting and revoking access to ePHI?

4 ASSESS THE IMPACT TO YOUR PRACTICE IF A THREAT DOES OCCUR:

- Unauthorized individuals may gain access to ePHI, triggering a costly breach notification process
- A former worker may steal patients' contact information, including social security numbers and credit card numbers for fraud and abuse, plus identity theft
- A former worker may steal a doctors Medicare, or Medicaid, or DEA number; submit false claims, write false prescriptions

5 DETERMINE WHAT METHOD(S) YOUR PRACTICE SHOULD USE TO ADDRESS THREATS:

- Policy and procedures for access management
- Training your office staff in access management (including remote access)
- Policy and procedures to sanction an staff member who misbehaves
- Policy and procedures to terminate
- Password authorization form
- Staff termination checklist

6 EVALUATE HOW YOUR EHR SYSTEM COULD HELP:

Yes, if your EHR system permits role base access

Next are a few suggestions you might need in your Access Policies and Procedures. Note that the information below may not be complete or sufficient to meet your individual practice requirements.

Access to the Information System and ePHI

Purpose

[Practice name] has established this policy to ensure that all staff members have appropriate access to ePHI and PHI, and that his or her identity is properly verified before such access can be attempted. This policy also addresses procedures to prevent staff members and former staff members who will not have access to ePHI and PHI from obtaining it, and for emergency access to the information system.

Scope

This policy applies to all [Practice name] staff members who utilize the electronic information system. It covers key provisions concerning who has access to ePHI and PHI, the level of access they have, protections to ensure proper user identification for access, and emergency access to ePHI and PHI. This policy also addresses the steps to be followed to terminate access to ePHI and PHI when a staff member's authorization to access has ended, such as when employment or membership is terminated.

Procedures

Users shall be provided with:

1. Initial access to authorized PHI amd ePHI upon hire
2. Training that emphasizes employee's access limits to PHI and ePHI, with clear expectations discussed and explanation of sanction/termination should employee violate access policy
3. Increased access as job responsibilities change, and
4. Access to different systems and applications as job responsibilities change and new systems and applications are added to the network.

Security Password Management

To ensure that passwords created and used by [Practice name] to access any network, system or application used to access, transmit, receive or store ePHI is properly safeguarded the following procedures are established:

1. All staff members who access networks, systems or applications used to access, transmit, receive or store ePHI will be supplied with, or self-select a unique user identification and password to access ePHI.

2. All staff members must supply a password in conjunction with their unique user identification to gain access to any application or database system used to create, transmit, receive or store ePHI.

3. All passwords used to gain access to any network, system or application used to access, transmit, receive or store ePHI must be of sufficient complexity to ensure that it is not easily guessable.

4. Staff members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:

    a. Passwords are only to be used for legitimate access to networks, systems or applications;

    b. Passwords must not be inappropriately disclosed to other staff members or individuals;

    c. Staff members must not allow other staff members or individuals to use their password;

d. Passwords must not be written down, posted or exposed in an insecure manner such as on a notepad or posted on the workstation; and

e. Log-in attempts shall be monitored by the system administrator.

Security Password Structure

To ensure that all passwords used to control access to any network, system, application, media or file containing ePHI are secure and not easily guessed, the following procedures are established:

1. Passwords must be a minimum of eight characters in length;

2. Passwords must incorporate three of the following characteristics:

   a. Any lower case letters (a-z);

   b. Any upper case letters (A-Z);

   c. Any numbers (0-9); and

   d. Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ `).

3. Passwords should not include easily guessed information such as personal information, names, pets, birth dates, etc.; and

4. Passwords should not be words found in a dictionary.

[Practice name] Password Authorization Form

Name: _____ Date: _____

Address: _____

City: _____State: _____ Zip Code: _____

Employee ID: _____

New Password ☐ Replacement Password ☐

Organizational Software _____

Employee Sign-on _____

Password _____

I agree that I will comply with all privacy, security and confidentiality policies and procedures set in place by during my entire employment or association with [Practice name]. If I, at any time, knowingly or inadvertently breach privacy, security and/or patient confidentiality policies and procedures, or become aware of any breach of patient information, I agree to notify the Privacy Officer and/or Security Officer of [Practice name] immediately. In addition, I understand that a breach of privacy, security or patient confidentiality policies may result in suspension or termination of my employment or position at [Practice name]. Upon termination of my employment or association for any reason, or at any time upon request, I agree to return any and all patient confidential information in my possession. This agreement is not a contract for continued employment.

Employee Signature: _____ *Date:* _____

Privacy/Security Officer Signature: _____*Date:* _____

[Practice name] Staff Member Termination Checklist

This checklist shall be completed by the Information Security Officer upon the termination of a staff member for any reason–whether voluntary or involuntary.

Name of Staff Member:

Date of Termination: Position:

Item	Date Completed	Initials
Network password terminated		
Handheld device password(s) terminated		
User accounts deactivated		
Keys returned		
Key Cards, etc. returned		
All company property returned		
All PHI and ePHI returned		
Remote access rights deactivated		

CHAPTER 6 – DATA BACKUP

Data Backup is part of the same area of Device and Media Controls in the HIPAA Security Rule outlined in Chapter 5. Its full name is Data Backup and Storage. Data backup refers to the copying and archiving of computer data typically found in EHRs, practice management system software, and other clinical and administrative tools, so it may be used to *restore* the original after a data loss event such as a computer failure, fire or theft.

Backups have two distinct purposes. The primary purpose is to recover data, the patients' medical information, after its loss. Practices are strongly encouraged to explore offsite or remote data backup options. This protects the practice should there be a fire or theft and the data backup system itself is destroyed or lost.

The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy. In HIPAA, it is a six (6) year retention requirement. Note that, depending on your business purposes and state and local laws, you may wish to retain the ePHI for longer than six (6) years.

Example:

After hurricane Sandy in 2012 along the coast of New Jersey, remote data backups were used to recover patient data allowing physicians to provide care when the offices, ambulatory centers and hospitals were destroyed or damaged in the storm.

It is important to remember that every practice, regardless of its configuration or location, is vulnerable to natural disasters, fire, and theft that might impact EHR systems and other electronic tools.

DATA BACKUP

1 IDENTIFY THE POTENTIAL THREATS:

PHI or ePHI could be destroyed or lost in a storm,
fire, flood, theft, is intentionally destroyed, or the original data source is corrupted.

2 ANALYZE HOW LIKELY A THREAT COULD OCCUR

In terms of physical disasters, this may depend on where your offices are geographically located; if you are in tornado alley in the middle of the United States or along either coast it may be more likely that you must prepare for something weather-related to happen. However, all practices can be impacted by fire, flooding, power or Internet outage, theft or loss of data due to other reasons.

3 IDENTIFY WHAT YOUR PRACTICE CURRENTLY DOES TO PROTECT ePHI:

- Electronic back up by EHR system vendor?
- Electronic back up by a different vendor?
- Office backup on to DVDs or other media?
- Don't know?

Where is your data (back up device) stored:

- In the practice itself on a physical device (this approach leaves data extremely vulnerable)
- Collected on a regular basis and then physically stored offsite (better but still vulnerable)
- Data stored offsite in a central server
- Data stored in the "cloud"
- We do not back up our data
- Don't know

4 ASSESS THE IMPACT TO YOUR PRACTICE IF A THREAT DOES OCCUR:

- Loss of data will impact your ability to bill, coordinate care and effectively treat your patients
- Loss of data will impact your practice's reputation with your patients, those providers that yiou have referring relationship with, and others
- With no data back up your basic office functions will be impacted and potentially even your entire business continuity could be compromised

5 DETERMINE WHAT METHOD(S) YOUR PRACTICE SHOULD USE TO ADDRESS THREATS:

- Having a tested data backup policy and procedures
- Train you staff members in data backup
- Review your contracts for terms relating to the speed of which the vendor will be on site to assist with data loss-related issues
- If this type of contractual language is not sufficient or available, the practice should consider contracting with an outside support vendor to provide "on call" technical assistance
- In terms of power, review the terms of your lease or contract with your power company and consider the installation of a power back-up unit

6 EVALUATE HOW YOUR EHR SYSTEM COULD HELP:

Yes, if your EHR system vendor is doing backup for you, or is storing your ePHI in the Cloud

Next are a few suggestions you might consider for your Data Backup and Storage Procedures, which are part of a larger set of Policies and Procedures. Note that the information below may not be complete or sufficient to meet your individual practice requirements.

Data backup and Storage procedures

Data Backup and Storage: [Practice name] will create an exact copy of all ePHI when necessary immediately prior to any movement or disposal. This procedure is in addition to the standard routine backup protocol to ensure that all ePHI is preserved before potential compromise.

[Practice name] will explore offsite or “cloud” based data backup options to ensure business continuity.

As backup systems are useless if the recovery fails, [Practice name] will test data backup recovery on a periodic basis. (When appropriate, this will be conducted with the assistance of the software vendor.) This complies with the HIPAA Security Rule’s requirement to "Implement procedures for periodic testing and revision of contingency plans."

CHAPTER 7 – PHYSICAL PROTECTIONS

The HIPAA Security Rule outlines a number of required physical safeguards, including:

- Facility access controls
- Workstation use
- Workstation security, and
- Device and media controls.

Workstation use and security were discussed in the chapter on mobile tools. Device and media controls were discussed in the chapter on shredding.

Facility access controls is an important component of a practice's risk analysis process. This is the area that considers the access to your offices through doors and windows, the closets and cabinets within your offices, to the electronic tools themselves.

This area considers any and all locks into and within your office to doors, windows, closets, file drawers, and cabinets.

The federal regulation permits a wide variety of approaches to physical security. It may include alarms on your external doors and windows if you are in a vulnerable place whether in a city or rural setting.

It may include motion lights or spot lights on the outside of your office building.

It may include a guard inside the front door with a paper sign-in log.

Part of your Physical Safeguards evaluation should be a comprehensive review of your work space and where the practice keeps paper records and how the practice physically protects the EHR system and other electronic tools.

Example:

One office review determined that there were sufficient locks on the front door and windows, plus a lock on the medical records room. Once inside the medical records room, however, the reviewer discovered the back door into the offices was through the medical records room and was propped open so that people could quickly enter and leave.

Example:

One office review determined that the fax machine and copier were located in a publically-accessible area of the practice. Thus, paper PHI was left on both the copier and the printer where visitors could potentially see it. Worse yet, the "shredding" process consisted simply a cardboard box, again located in an area of the practice accessible to visitors that held paper that contained PHI waiting to be shredded.

PHYSICAL PROTECTIONS

1 IDENTIFY THE POTENTIAL THREATS:

- Breach by improper disclosure of PHI and ePHI
- Theft of PHI or ePHI
- Theft of mobile tools

2 ANALYZE HOW LIKELY A THREAT COULD OCCUR

It might depend on the type of specialty your office practices;
if you have drugs, such as controlled substances, in your office that someone might want to steal; or or
if you have valuable mobile devices

3 IDENTIFY WHAT YOUR PRACTICE CURRENTLY DOES TO PROTECT ePHI:

locks, swipe cards, smart cards and other devices on all doors?
What else?

4 ASSESS THE IMPACT TO YOUR PRACTICE IF A THREAT DOES OCCUR:

- With a breach you will need to notify the individuals impacted by the breach, the government, and in cases involving more than 500 individuals, local media. This breach notification process not only would be expensive, but it could impact the practice's reputation
- With a theft of mobile tools you might need to call the police

5 DETERMINE WHAT METHOD(S) YOUR PRACTICE SHOULD USE TO ADDRESS THREATS:

- Good strong facility access protections
- Facility access policy and procedures
- Training for your staff members

6 EVALUATE HOW YOUR EHR SYSTEM COULD HELP:

Many EHR vendors have security options, including self locking processes after a few minutes of non-use. Some of these features may be optional and require additional expense. Review the available security features with your vendor

Next are a few suggestions you might need for your Facility Access Control Procedures. Note that the information below may not be complete or sufficient to meet your individual practice requirements.

Facility Access Controls procedures (are part of a larger set of policies and procedures, so there are only demonstration procedures below)

Facility Access Controls

Access to areas of [Practice name]'s facility that contain [Practice name]'s information system components will be granted only to those with a verifiable and approved business need to have access.

Access control will be established with physical hardware that prevents improper or inadvertent entry into a secure area. This hardware may include combination locks, swipe cards, smart cards and other devices on all doors and [Practice name]'s information system equipment.

Disabling or circumventing any of the physical security protections is strictly prohibited. Any problems with physical security measures must be reported to the Security Officer.

APPENDIX A – HIPAA SECURITY SELF ASSESSMENT

Check Yes or No:	YES	NO
Security Official and Security Team	☐	☐
A Security Officer or Security Team has been appointed for your organization		
A job description has been developed for the Security Officer/Team	☐	☐
The Security Officer and Security Team have been trained on their duties as identified in the job description	☐	☐
The Security Officer and Security Team have been trained on the Security Policies and Procedures	☐	☐
Risk Management		
An Initial Risk Analysis has been conducted to assess potential risks and vulnerabilities	☐	☐
Risk Analyses are performed and documented on a regular basis, or when changes occur	☐	☐
Threat sources have been identified and classified	☐	☐
Risk determinations are documented	☐	☐
Impact analyses have been conducted and documented	☐	☐
Response and Reporting Procedures		
The Security Officer and Security Team have established a process for reporting and identifying security questions and violations	☐	☐
The organization has established criteria for what constitutes a security incident	☐	☐
Security incidents are analyzed and remedial actions are documented	☐	☐
Policies and Procedures		
Security Policies and Procedures have been developed	☐	☐
The Security Management Process has been documented	☐	☐
Security Policies and Procedures are made available to applicable users and employees	☐	☐
Security Policies and Procedures undergo annual or other periodic review	☐	☐

Technical Security Configuration Documents exist for all major applications, such as operating systems, routers and other technical areas	☐	☐
Security Requirements are included in all applicable vendor solicitation documents including RFPs	☐	☐
The decisions and reasons for **not** implementing addressable specifications are documented	☐	☐
Periodic technical and non-technical evaluations are scheduled to determine compliance with policies and procedures	☐	☐

Other Necessary Policies and Procedures

Email policy and procedures developed

☐ ☐

Internet policy and procedures developed

☐ ☐

Remote access policies and procedures developed

☐ ☐

Computer and Network Management

Network Security Mechanisms, such as firewalls, have been implemented	☐	☐
Virus Detection Systems have been installed	☐	☐
Virus Signature Files are routinely updated	☐	☐
Intrusion Detection Systems have are installed on appropriate systems	☐	☐
Prevention Testing is performed on the system	☐	☐
Integrity Controls have been implemented to prevent improper alteration or destruction of PHI	☐	☐
An Information System Activity Review is regularly performed	☐	☐
An inventory system for all hardware and software is implemented	☐	☐
Movement of all stationary and mobile electronic devices, including hardware, is tracked within the organization	☐	☐

Data Backup or Storage is conducted before moving equipment	☐	☐
Inventory Logs are periodically reviewed and updated	☐	☐
Workstation Procedures are established for each type of workstation, including procedures for both equipment and the physical surroundings or the workstation	☐	☐
Transmission Security Measures are in place to appropriately protect ePHI transmitted over communication networks	☐	☐
Audit Controls are in place to record and examine information systems containing ePHI	☐	☐

Updates and Maintenance

Security Requirements are identified for all new system designs	☐	☐
Risk Assessments on all new or updated systems are performed	☐	☐
System Documentation is modified as changes to systems occur	☐	☐
System Maintenance Plans are developed and implemented on a regular basis	☐	☐
Maintenance and Repairs are documented and maintained on a regular basis	☐	☐
Authorization for software modifications are obtained and documented	☐	☐
New and Revised hardware and software is authorized and tested before implementation	☐	☐
Distribution of new software is documented	☐	☐
Data backup and storage is performed before maintenance or updates	☐	☐
Risk Determinations are documented	☐	☐
Impact Analyses have been conducted and documented	☐	☐

Disposal

Disposal processes for ePHI are established	☐	☐
Disposal Procedures are established for specific types of media, such as hard drives, CD, and all others	☐	☐
Disposal Records are maintained and verification of proper disposal is documented	☐	☐
Paper records are destroyed when no longer needed	☐	☐
Procedures for the re-use or media and devices that previously contained ePHI have been established	☐	☐

Contingency Planning

A Contingency Plan for if the practice experiences a temporary loss of power, Internet and or data has been developed, tested and implemented	☐	☐
The Contingency Plan is reviewed periodically and updated as needed	☐	☐
A Disaster Recovery Plan has been tested and in place	☐	☐
Responsible parties have been provided detailed procedures and training for their assigned duties under the Contingency and Recovery Plans	☐	☐
A copy of both the Contingency Plan and the Disaster Recovery Plan are in a secure location	☐	☐
Data criticality analyses are performed where necessary to assess the relative criticality of application and data	☐	☐

Training and Education

Employees (including volunteers) have been trained on all applicable security requirements for their job functions	☐	☐
Security Requirements are communicated to staff on a regular basis	☐	☐

Access Controls

Access Controls are used for all sensitive systems, files and directories	☐	☐
Password Management procedures are used	☐	☐
Unique User Identification for identifying and tracking individuals is assigned to each user	☐	☐

Remote Connections into the organization's network are secured	☐	☐
User Privileges are based on job functions or employee classification	☐	☐
Access is granted based on valid business needs	☐	☐
User Privileges are evoked when an employee is terminated	☐	☐
User Privileges are modified when an employee's job description or classification changes	☐	☐
Emergency Access Procedures have been established for accessing ePHI information during an emergency	☐	☐
Automatic Logoff Procedures have been implemented	☐	☐
Authentication procedures to ensure that the person or entity seeking access is the one claimed are implemented	☐	☐
If encryption is used, proper procedures are followed for database, password and file encryption	☐	☐

Physical Security

Facility Access Control Procedures have been implemented to limit physical access to ePHI and facilities where it is housed	☐	☐
Facility Security Plans have been developed and documented	☐	☐
Periodic reviews of Facility Security Plan(s) have been scheduled	☐	☐
Access to facilities is controlled through identification or key cards	☐	☐
Visitor identification is required throughout the practice	☐	☐
Keys, keycards and other access devices are assigned and logged	☐	☐
Keys or other access devices are required for sensitive areas, such as server rooms, mobile device storage areas, and areas where drugs are kept	☐	☐
Unused keys and access devices are properly secured	☐	☐
Computer, faxes and printers are placed in areas that are not easily accessible to unauthorized persons	☐	☐
Portable systems, such as laptops, are properly secured when not in use	☐	☐

Workforce Security

Authorization procedures are followed for workforce members requiring access to ePHI [when feasible and necessary]	☐	☐
Clearance procedures are followed when determining access of employees [when feasible and necessary]	☐	☐
A Sanction Policy to apply appropriate sanctions has been developed and communicated to workforce members who do not comply with security policies and procedures	☐	☐

Business Associates

Business Associate contracts are in place with all business associates who create, receive, maintain or transmit ePHI	☐	☐
Satisfactory assurances are obtained from business associates that they will appropriately safeguard information	☐	☐
A definition as to what constitutes satisfactory assurances has been developed and documented	☐	☐
In cases where Business Associate contracts are not applicable, other arrangements are made between organizations and the business associate to keep data confidential	☐	☐

Date Assessment Completed: _____

Name of Person who Completed the Assessment: _____

Title of Person who Completed the Assessment: _____