Chapter 4

Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity

To support patient care, providers store electronic Protected Health Information (ePHI) in a variety of electronic systems, not just Electronic Health Records (EHRs). Knowing this, providers must remember that all electronic systems are vulnerable to cyber-attacks and must consider in their security efforts all of their systems and technologies that maintain ePHI.[46] (See Chapter 6 for more information about security risk analysis.)

While a discussion of ePHI security goes far beyond EHRs, this chapter focuses on EHR security in particular.

The HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule[47] establishes a national set of minimum security standards for protecting all ePHI that a Covered Entity (CE) and Business Associate (BA) create, receive, maintain, or transmit. The Security Rule contains the administrative, physical, and technical safeguards that CEs and BAs must put in place to secure ePHI.

Resources

- HIPAA Requirements,[48] in detail
- HIPAA Privacy Rule,[49] in detail
- HIPAA Security Rule,[50] in detail
- Privacy and Security Resources[51]

[46] Refer to the booklet "Partners in Integrity" at http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Provider-Education-Toolkits/Downloads/understand-prevent-provider-idtheft.pdf for more information about medical identity theft and fraud prevention.

[47] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

[48] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

[49] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

[50] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

[51] http://healthit.gov/providers-professionals/ehr-privacy-security/resources

These Security Rule safeguards can help health care providers avoid some of the common security gaps that could lead to cyber-attack intrusions and data loss. Safeguards can protect the people, information, technology, and facilities that health care providers depend on to carry out their primary mission: caring for their patients.

The Security Rule has several types of safeguards and requirements which you must apply:

1. **Administrative Safeguards**[52] – Administrative safeguards are administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations. Administrative safeguards involve the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of workforce members in relation to the protection of that information. A central requirement is that you perform a security risk analysis that identifies and analyzes risks to ePHI and then implement security measures to reduce the identified risks.
2. **Physical Safeguards**[53] – These safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.[54] These safeguards are the technology and the policies and procedures for its use that protect ePHI and control access to it.
3. **Organizational Standards**[55] – These standards require a CE to have contracts or other arrangements with BAs that will have access to the CE's ePHI. The standards provide the specific criteria required for written contracts or other arrangements.
4. **Policies and Procedures**[56] – These standards require a CE to adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A CE must maintain, until six years after the date of their creation or last effective date (whichever is later), written security policies and procedures and written records of required actions, activities, or assessments. A CE must periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI.

Visit the Office for Civil Rights (OCR) website[57] for a full overview of security standards and required protections for ePHI under the Security Rule.

[52] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
[53] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf
[54] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
[55] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf
[56] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf
[57] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

How to Keep Your Patients' Health Information Secure with an EHR

Your practice is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of ePHI maintained in your EHR.

Having an EHR affects the types and combinations of safeguards you will need to keep your patients' health information confidential. EHRs also bring new responsibilities for safeguarding your patients' health information in an electronic form.

To uphold patient trust as your practice continues to adopt and use an EHR or other electronic technology for collection and use of ePHI, and to comply with HIPAA Security Rule and Meaningful Use requirements, your practice must conduct a security risk analysis (sometimes called "security risk assessment"). (See Chapter 6 for more discussion on security risk analysis.) The risk analysis process will guide you through a systematic examination of many aspects of your health care practice to identify potential security weaknesses and flaws.

Many health care providers will need to make changes to reduce risks and to comply with the HIPAA Rules and Meaningful Use requirements. Fortunately, properly configured and certified EHRs[58] can provide more protection to ePHI than paper files provided. (See Step 5A in Chapter 6 for more information about using electronic capabilities to help safeguard patients' information.)

Your EHR Software and Hardware

Most EHRs and related equipment have security features built in or provided as part of a service, but they are not always configured or enabled properly.

As the guardian of ePHI, it is up to you — along with your designated staff members — to learn about these basic features and ensure they are functioning and are updated when necessary. **You and your staff must keep up-to-date with software upgrades and available patches.**

Remember, security risk analysis and mitigation is an ongoing responsibility for your practice. Vigilance should be part of your practice's ongoing activities.

Encryption 101

Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (a type of formula). If information is encrypted, there is a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text. For more information about encryption, review the National Institute of Standards and Technology (NIST) *Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices*.[59]

[58] http://oncchpl.force.com/ehrcert
[59] http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

Working with Your EHR and Health IT Developers

When working with your EHR and health information technology (health IT) developers, you may want to ask the following questions to help understand the privacy and security practices they put in place.[60]

- When my health IT developer installs its software for my practice, does its implementation process address the security features listed below for my practice environment?
    - ePHI encryption
    - Auditing functions
    - Backup and recovery routines
    - Unique user IDs and strong passwords
    - Role- or user-based access controls
    - Auto time-out
    - Emergency access
    - Amendments and accounting of disclosures
- Will the health IT developer train my staff on the above features so my team can update and configure these features as needed?
- How much of my health IT developer's training covers privacy and security awareness, requirements, and functions?
- How does my backup and recovery system work?
    - Where is the documentation?
    - Where are the backups stored?
    - How often do I test this recovery system?
- When my staff is trying to communicate with the health IT developer's staff, how will each party authenticate its identity? For example, how will my staff know that an individual who contacts them is the health IT developer representative and not a hacker trying to pose as such?
- How much remote access will the health IT developer have to my system to provide support and other services? How will this remote access be secured?
- If I want to securely email with my patients, will this system enable me to do that as required by the Security Rule?

[60] For additional information about questions to ask health IT developers, see the Questions for EHR Developers document at http://bit.ly/EHRdevqs.

Cybersecurity

An Internet connection is a necessity to conduct the many online activities that can be part of EHR and ePHI use. Exchanging patient information electronically, submitting claims electronically, generating electronic records for patients' requests, and e-prescribing are all examples of online activities that rely on cybersecurity practices to safeguard systems and information.

The Threat of Cyber-Attacks

Most everyone has seen news reports of cyber-attacks against, for example, national retail chains or the information networks of the federal government. Health care providers may believe that if they are small and low profile, they will escape the attention of the "hackers" who are running these attacks. Yet every day there are new attacks aimed specifically at small to mid-size organizations because they are less likely to be fully protecting themselves. Criminals have been highly successful at penetrating these smaller organizations and carrying out their activities, while their unfortunate victims are unaware until it is too late.

Cybersecurity refers to ways to prevent, detect, and respond to attacks against or unauthorized access against a computer system and its information. Cybersecurity protects your information or any form of digital asset stored in your computer or in any digital memory device.

It is important to have strong cybersecurity practices in place to protect patient information, organizational assets, your practice operations, and your personnel, and of course to comply with the HIPAA Security Rule.[61] Cybersecurity is needed whether you have your EHR locally installed in your office or access it over the Internet from a cloud service provider.

The Office of the National Coordinator for Health Information Technology (ONC) offers online Cybersecurity information,[62] including the Top 10 Tips for Cybersecurity in Health Care, to help you reduce your risk. For a full overview of security standards and required protections for ePHI under the HIPAA Security Rule, visit OCR's HIPAA Security Rule web page.[63]

Mobile Devices

The U.S. Department of Health and Human Services (HHS) has put together a collection of tips and information[64] to help you protect and secure health information that you may access, receive, and store on mobile devices such as smartphones, laptops, and tablets.

[61] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/
[62] http://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility
[63] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[64] http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Email and Texting

Consumers increasingly want to communicate electronically with their providers through email or texting. The Security Rule requires that when you send ePHI to your patient, you send it through a secure method and that you have a reasonable belief that it will be delivered to the intended recipient. The Security Rule, however, does not apply to the patient. A patient may send health information to you using email or texting that is not secure. That health information becomes protected by the HIPAA Rules when you receive it.

In this environment of more online access and great demand by consumers for near real-time communications, you should be careful to use a communications mechanism that allows you to implement the appropriate Security Rule safeguards, such as an email system that encrypts messages or requires patient login, as with a patient portal. If you use an EHR system that is certified under ONC’s 2014 Certification Rule, your EHR should have the capability of allowing your patients to communicate with your office through the office’s secure patient portal.[65]

If you attest to Meaningful Use and use a certified EHR system, you should be able to communicate online with your patients. The EHR system should have the appropriate mechanisms in place to support compliance with the Security Rule. You might want to avoid other types of online or electronic communication (e.g., texting) unless you first confirm that the communication method meets, or is exempt from, the Security Rule.[66]

[65] 45 CFR 170.315(e)(3).

[66] 45 CFR 164.312(e)(1).