The HIPAA Privacy and Security Standards

HIPAA was passed in 1996 and contains several rules, though for our purposes in this chapter, we will be concentrating on the privacy and security rules. In addition, in 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) went a step further, making the original privacy and security rules under HIPAA more stringent. HITECH also gives more power to federal and state government authorities to enforce the privacy and security rules.

On March 26, 2013, the Omnibus Final Rule to the HITECH Act went into effect, with compliance required in September 2013. Changes included more enhancements to protecting patient privacy, additions to individual patient rights, and strengthening of the government's ability to enforce the law. HIPAA was expanded to give more control over any covered entity's business associates—for example, external coding consultants and software service providers. The Notice of Privacy Practices has been expanded, and the maximum penalty for violation of the law was increased to $1.5 million per violation. Related to HITECH, the breach notification standards have been enhanced. Examples of the enhancement in patient rights include the requirement that providers who utilize electronic health records must provide patients with their records in electronic form, when requested. In addition, patients who are paying for their services in cash may instruct the provider not to bill their insurance and not to divulge any information about the services to the patient's health insurance carrier.

The intent of both is to ensure that protected health information (PHI) is kept private and secure. They give patients the right to determine who sees their health information, but still give **covered entities** (healthcare providers, clearinghouses, or health insurance plans) the leeway to access the PHI needed to care for patients, collect payment for services rendered, and operate a business. Protected health information is any piece of information that identifies a patient—it includes a patient's name, DOB, address, email address, and telephone number; the patient's employer; any relatives' names; the patient's Social Security number and medical record number; account numbers tied to the patient's account; the patient's fingerprints; any photographs of the patient; and any characteristics about the patient that would automatically disclose his or her identity (for instance, "the governor of the largest state in the United States").

In addition, PHI includes the medical information that is tied to the person, including diagnosis, test results, treatments, and prognosis; documentation by the care provider and other healthcare professionals; and billing information. HIPAA states (and HITECH enhances) that only persons who have a need to know may have access to a patient's PHI. And, to take it a step further, they are entitled only to access to the **minimum necessary information** required to do their jobs. An example would be a covered entity such as a health insurance company that is working on a claim for a patient who underwent coronary artery bypass three months ago. Unless the insurance company can prove otherwise, the minimum necessary information it needs is the supporting documentation related to the bypass surgery. The fact that the patient delivered a child

in 1980 has nothing to do with the bypass surgery, and therefore the company does not need access to those records.

There are many ways that facilities protect the **privacy** and **confidentiality** of their patients. Privacy is the right to be left alone. In other words, no one should infringe upon a patient's time or personal space while being treated; that is why admissions departments and registration areas have partitions or cubicles, so that the patient has some privacy. Confidentiality is keeping a secret; in healthcare, it means keeping information about a patient to oneself. Patients have the right to expect that their medical information is going to be kept confidential. Written policies and ongoing education of staff are two very important aspects of complying with the HIPAA and HITECH rules.

Privacy and confidentiality policies should address, at a minimum:

- Release (disclosure) of information to outside sources. PHI is released to outside entities only upon written authorization of the patient/legal representative (or as required by law) and release to inside sources (access) is only on a need-to-know basis. The policy should also address exceptions.
  Let's first look at internal access as an example.
  Cathy Hess was a patient on unit 3E of Memorial Hospital from May 3 to May 5. Suzanne Hess is a nurse who works at Memorial Hospital and is Cathy Hess' sister-in-law. She does not work on 3E and did not take care of Suzanne. She did not have, does not have, and will not have a need to access Cathy's health record. But, let's say two months after Suzanne's hospitalization, Cathy is on a committee that is auditing records for a study and Suzanne's record happens to be one of the records in the sample. Cathy could ask one of the other reviewers to audit that particular record, but if Cathy does review Suzanne's record, she is accessing the record within the scope of her job, and she does have a need know in that case. Internal access does not require an authorization from the patient, if there is a need to know.
- Outside access without the need for authorization of the patient/ personal representative. This includes access by an insurance company (for payment of the bill), by public health officials in cases of mandatory reporting (infectious diseases, for example), and by licensing and accrediting agencies.
- Release of **directory information**. Directory information includes the fact that the patient is in the hospital (or is being treated at an ambulatory facility) and his or her room number. However, if a patient does not want certain individuals (or anyone) to know that he or she is in the hospital or the location within the hospital, then the patient/legal representative would sign an authorization stipulating who can and cannot have access to that information.
- Written guidelines and examples of what is considered minimum necessary information by reason for the request
- Faxing of documentation—information that can and cannot be faxed and the protocol to be followed, should information be faxed to the wrong location
- Computer access and lockdown. Policy requires staff to lock their computers down (sign out) if they are going to be away from their desks for any length of time.

- Password sharing—makes it a disciplinary offense to share one's password with another
- Computer screens—should be kept out of view of the public or anyone else who might have access to areas with computers
- Shredding any hard-copy documents (where applicable) rather than just discarding them in a waste paper basket.
- Signing by patients of a **Notice of Privacy Practices** so that patients are aware of how their personal health information will be used. The Notice of Privacy Practices must be in writing and be signed by the patient/legal representative. It informs the patient how his or her health information will be used and the reasons it may be released, notifies the patient that he or she may view or have copies of the health record and may request amendments to it, and states the procedure for filing a complaint with the Department of Health and Human Services.
- Requirement that all staff (including care providers) sign a document committing themselves to keeping private and confidential the information that is written, spoken, or overheard about any and all patients

Once a paper record is converted to an electronic one, the paper copy is no longer needed. It is best practice to destroy the paper copy, if the electronic version is considered the legal document, and the one upon which healthcare decisions are made. The paper record should be destroyed either by incineration or by shredding. An example of a shredding policy statement in an office that no longer keeps hard-copy records (a "paperless environment") is

> *The electronic health record is the legal health record at Greensburg Medical Center. Printed copies should only be made when there is a need to refer to the printed document rather than the computerized image. Once the printed document is no longer needed, it is to be placed in one of the marked shred bins immediately. Shred bins are located in the business office and in the secure area of the front office. The only exception to this policy is the printed copies made for patients' requests, or that are to be mailed by the Release of Information Specialist.*

In addition to the policies noted above, security-specific policies should address:

- Password protection. Every computer user must have a unique code, or **password**, that is known (and used) only by the user. Passwords should not be easily discerned; for instance, the user's birthdate, spouse's name, child's name, phone number, and the like would not be secure passwords. Instead, the password should be a combination of numbers, letters, and special characters (symbols), no less than six and no longer than eight characters in length, and the system should be set up to prompt users to change their password at least every 90 days. Individual offices and facilities will set policies regarding their password configuration requirements. The software system in use will dictate some of the password constraints as well.
- Appointment of a security and/or privacy officer. Someone in the facility must be named as privacy and security officer, though these may be two different individuals. The privacy/security officer is ultimately responsible for setting,

monitoring, updating, investigating, and enforcing all privacy and security policies.

- Log-in attempts. The system set-up should include automatic lock-out when a user attempts to log in a certain number of times (usually three) with the wrong password. The policy and procedure should also address how to regain access. No doubt you have already experienced this with online banking, a credit card company, or the learning management system at your college.
- Protection from **computer viruses** and **malware**. This should include the facility's policy on downloading music or other attachments that may carry viruses and malware. A virus is a "deviant program, stored on a computer floppy disk, hard drive, or CD, that can cause unexpected and often undesirable effects, such as destroying or corrupting data. Malware comes in the form of worms, viruses, and Trojan horses, all of which attack computer programs" (Williams and Sawyer). In early 2016 several hospitals were plagued by computer malware. Though patient records were not accessed, MedStar Health near Washington, DC, was affected and the system's users were not able to log in. This attack affected 250 outpatient locations and 10 hospitals. As a precaution, the health system sent patients to other facilities until the problem was resolved and the FBI was involved in the investigation (Cox, Turner, and Zapotsky).
- Security audits. A policy should be in place and carried out that requires random security audits to monitor access to patients' records. Often, this may be done on a rotating basis so that all staff members (including providers) are audited periodically, or it may be done based on a random selection of patients in the database. Of course, the investigation of any rumored or known breaches should include a security audit. It is important that internal security audits be carried out, since the Officer of Inspector General (OIG) also carries out random audits of EHR system security vulnerabilities.
- Off-site access. With the use of current technology, many PMs and EHRs can be accessed via the Internet. Policies must dictate who can access remotely as well as what information can be viewed and/or edited remotely.
- Printing policies. The more information that is printed from the HER or PM software, the greater chance there is of unauthorized disclosure.
- Destruction policies. If paper copies of the electronic record are going to be made, then the destruction of those copies also needs to be addressed. The usual method of destruction is shredding, either externally by a destruction company or internally through use of portable shredders. Regardless of which is used, a policy must be addressed that states when paper copies are destroyed, how, by whom, and when.
- Detailed policies and procedures that address privacy or security incidents. Disciplinary action should be addressed in this policy as well.
- Staff education—requirement that all staff (including care providers) participate in continuing education opportunities to reinforce the laws governing privacy and security.
- Email. It is a part of everyday life, not just in our personal lives but in our work lives as well. Anything written in an email is protected information. However, it is not a secure means of communication, and the facility should adopt policies

related to the sending and receiving of email messages, including what, if any, patient-related information can be sent via email. Like faxes, emails can go to the wrong individual, constituting a privacy breach. There must be a policy regarding patient-related emails or emails to or from patients—are they a part of the patient's health record, and if so, how will the email become part of the record? Emails should be **encrypted**, which means the words are scrambled and can be read only if the receiver has a special code to decipher it, but encrypting still does not ensure total security. Encryption applies to any information that is electronically transmitted.

Firewalls should also be used to deter access to the system by unauthorized individuals. Williams and Sawyer define a firewall as "a system of hardware and/or software that protects a computer or a network from intruders."

Hardware also has to be protected, and policies must be written to govern the security of hardware devices. Hardware includes desktop computers, laptop computers, hand-held devices, and the like. These devices are always at risk for loss or theft. But to protect the information on a device, follow these simple rules:

- Always lock down (sign out of) the device when it is unattended, and require a password to log on.
- Never store the passwords to any of your hardware devices or sites on the computer.
- Back up files onto a CD, external hard drive, or flash drive.
- Encrypt PHI if policy allows health records to be stored on the device.
- Use the portable devices in a secure area—using one in the cafeteria and walking away to freshen your coffee is not secure.
- Wipe the hard drives of any computers that are taken out of use before recycling them or placing them in the trash. This is typically a responsibility of the IT department.

Evaluating an EHR System for HIPAA Compliance

According to the Office of the National Coordinator for Health Information Technology (ONC) website, “Health information technology (health IT) makes it possible for health care providers to better manage patient care through secure use and sharing of health information.” Health IT includes the use of electronic health records (EHRs) instead of paper medical records to maintain people’s health information.

To better manage patient care using electronic means, however, it is necessary to comply with certain regulations. The HIPAA rules that address electronic health information are listed in Table 1. Regarding passwords, though longer passwords are more secure than shorter ones, the most secure passwords include a combination of letters (upper- and lowercase), symbols, and numbers. The password “summerday” is more secure than “summer,” for example, yet “summer18$#” is even more secure. Healthcare organizations set their own policies regarding the length and configuration of passwords. In a medical practice, it may be the office administrator who starts the search for EHR software and keeps in mind the requirements of a compliant system. Other individuals who should also be involved in researching, selecting, and implementing the EHR include a representative of care providers, a member of the front office (reception) staff, a clinical staff representative, health information staff, coding/billing staff, and an information technology (IT) professional who is an expert in the technological aspects of the software and hardware, networking, and interoperability of systems. This group should always keep in mind · The required components of a compliant HER:

- The needs of the office or facility
- The intended budget for acquiring a system as well as yearly budget requirements
- Staff and training needs
- The intent of the EHR—is it to interface with the existing PM system, or will an entirely new system that accomplishes both be purchased?
- The timeline—what is the target date for implementation?

TABLE 1 **Functionality of an EHR as Required by HIPAA Regulations**

Functionality	**Meaning**
Password Protection	Passwords must be assigned to all users of an electronic health record system and the passwords must meet certain criteria: length, properties, expiration intervals, and number of log-in attempts before lockout.
User Identification	Each user must have a unique identifier to log in. Often consists of the person’s first initial and last name. Allows for tracking and reporting of activity within the system by the user.
Access Rights	Policies are written and adhered to regarding access to

	functionality within the EHR that is dependent on the person's (or position's) need to know.
Accounting of Disclosures	Upon authorized request, an accounting of all disclosures from a patient's health record, going back a minimum of six years from the date of request, must be provided. The patient's health record must also be made available to the patient, or to an outside entity at the patient's request.
Security/ Backup/ Storage	A backup of the EHR database must be kept in a secure location, and restoration of the backup database must be possible at any given time. Other security requirements include controlled access to the database, use of passwords to access the database, use of firewalls, and antivirus programs.
Auditing	This task provides the ability to run reports by users or by patients that specify the menu, module, or function accessed; the date and time of the access; whether the information was viewed, edited, or deleted; and the user ID of the individual staff member.
Code Sets	The EHR must use ICD-10 codes, CPT codes, and HCPCS codes to store and transmit information.