Privacy, Security, Confidentiality, and Legal Issues

Learning Outcomes

At the end of this chapter, the student should be able to:

7.1 Identify the HIPAA privacy and security standards.
7.2 Evaluate an EHR system for HIPAA compliance.
7.3 Describe the role of certification in EHR implementation.
7.4 Apply procedures to set up security measures in PrimeSUITE.
7.5 Apply procedures to ensure data integrity.
7.6 Apply procedures to release health information using PrimeSUITE.
7.7 Account for data disclosures using PrimeSUITE.
7.8 Exchange information with outside healthcare providers for continuity of care using PrimeSUITE.
7.9 Outline the content of compliance plans.
7.10 Appraise the importance of contingency planning.

Key Terms

Access report
Accounting of disclosures
Audit trail
Blog
Breach of confidentiality
Compliance plan
Confidentiality
Contingency plan
Covered entity
Data Integrity
Disaster recovery plan
Directory information
Encryption
Firewall
Hardware
Health Information Exchange (HIE)
HIPAA
HITECH
Malware
Minimum necessary information
Notice of Privacy Practices
Password
Protected health information (PHI)
Privacy
Social media
User rights
Virus
You were introduced to HIPAA in Chapter 2, but to recap, HIPAA was passed in 1996. It contains several rules, though for our purposes, 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.

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 gives covered entities (a healthcare provider, a clearinghouse, or a health insurance plan) the leeway to access 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, e-mail address, and telephone number; his employer; any relatives’ names; social security number; medical record number; account numbers tied to the patient’s account; 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.
Covered entities include any healthcare entity that captures or utilizes health information. These include healthcare plans (insurance companies), clearinghouses that process healthcare claims, individual physicians and physicians’ practices, any type of therapist (mental health, physical, speech, occupational) and dentists; the staffs of hospitals, ambulatory facilities, nursing homes, home health agencies, and pharmacies; and employers.

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 only entitled 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 they can prove otherwise, the minimum necessary information they need 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 they do 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. 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 only upon written authorization of the patient/legal representative. Release to inside sources (access) is only on a need-to-know basis. The policy should also address any exceptions, for instance to an insurance company, to public health officials in cases of mandatory reporting (infectious diseases, for example), and to licensing and accrediting agencies.
- Release of directory information without a written authorization. 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.
- Written guidelines and examples of what is considered minimum necessary information.
- Faxing of documentation—information that can and cannot be faxed and also 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 desk 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.
• Signing by patients of a Notice of Privacy Practices so that they are aware of how their personal health information will be used. The Notice of Privacy Practices must be in writing, signed by the patient, and informs the patient how his or her health information will be used, reasons it may be released, notice that he or she may view or have copies of the health record and may request amendments to it, and 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.

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 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 something that can be easily discerned; for instance, the user’s birthdate, spouse’s name, child’s name, phone number, etc., would not be secure passwords. Instead, the password should be a combination of numbers and letters, at least six digits 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.
• 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.

• 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.”

• Security audits—a policy should be set and carried out that requires random security audits to monitor access to patients’ records. Often, this may be done on a rotating basis by staff members, 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.

• 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 is printed from the EHR or PM software, the more chance there is of unauthorized disclosure. Print only when absolutely necessary.

• 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.

• E-mail—it is a part of everyday life, not just in our personal lives but in our work lives as well. Anything written in an e-mail 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 e-mail messages, including what, if any, patient-related information can be sent via e-mail. E-mails, like faxes, can go to the wrong individual, constituting a privacy breach. There must be a policy regarding patient-related e-mails or e-mails to or from patients—are they a part of the patient’s health record, and if so, how will the e-mail become part of the record? E-mails should be encrypted, which means the words are scrambled and can only be read 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."²

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 the device and require a password to log on
- Never store the passwords to any of your hardware devices or sites on the computer
- Back up your files onto a CD, external hard drive, or flash drive
- Encrypt PHI if policy allows health records to be stored on it
- 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 drive of any computers that are taken out of use before recycling them or placing them in the trash

Privacy and security need to be kept in mind at all times in a healthcare facility. Not doing so, even if unintentionally, may result in fines ranging from $100 for each violation up to $250,000 for multiple violations. Or, if the breach was intentional, the fines start at $50,000 per violation and extend to $1,500,000 for multiple violations.

Healthcare organizations using an EHR must meet the HIPAA standards of privacy and confidentiality. In addition, states may have even more stringent rules. The American Recovery and Reinvestment Act of 2009 (ARRA), through HITECH, made the rules regarding privacy and security of electronic systems more stringent yet. Accounting of disclosures is one area that will affect hospitals and practices alike. Facilities must be able to provide a patient with a listing of disclosures, if requested; this is known as accounting of disclosures. Also, facilities with an EHR must be able to provide a patient with a listing of people who had access to their protected health information. This is known as an access report. The access report must contain the name of the individuals who accessed that person’s record, and also the names of persons who do not work at the facility who had access to the record. For instance, a hospital may grant a local nursing home admissions department the right to view the health record of a patient who is being considered for nursing home placement. This is required to assess whether or not the nursing home has the facilities needed to care for that patient, and is part of the continuum of care; thus, it is a necessary release. The hospital would note, in the access report, that the patient’s PHI was released to a certain nursing home, but would not be able to supply the names of the individual(s) who accessed it at the nursing home.

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 7.1.

Regarding passwords, though longer passwords are more secure than shorter ones, the most secure passwords include a combination of letters (upper and lower case), symbols, and numbers.

### Table 7.1: Functionality of an EHR as required by HIPAA regulations

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Protection</td>
<td>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 lock-out.</td>
</tr>
<tr>
<td>User Identification</td>
<td>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.</td>
</tr>
<tr>
<td>Access Rights</td>
<td>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.</td>
</tr>
<tr>
<td>Accounting of Disclosures</td>
<td>Upon authorized request, an accounting of all disclosures from a patient’s health record, going back a minimum of 6 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.</td>
</tr>
<tr>
<td>Security/Back-up/Storage</td>
<td>A back-up of the EHR database must be kept in a secure location, and restoration of the back-up 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, anti-virus programs, etc.</td>
</tr>
<tr>
<td>Auditing</td>
<td>The ability to run reports by user or by patient, 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.</td>
</tr>
<tr>
<td>Code Sets</td>
<td>The EHR must use ICD-9 codes, CPT codes, and HCPCS codes to store and transmit information.</td>
</tr>
</tbody>
</table>
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.

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 EHR
- 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?

### 7.3 The Role of Certification in EHR Implementation

There are many agencies that certify EHR software. Both the information technology (IT) and the health information technology (HIT) aspects of an EHR system must be taken into consideration, and during the process of assessing various systems and vendors, looking at certified EHR systems is a good place to start.

Through HITECH, the ONC was given authority to establish a certification program for EHRs. The ONC, through consultation with the Director of the National Institute of Standards and Technology, recognizes programs for this voluntary certification if they are in compliance with certification criteria.¹

The Healthcare Information and Management Systems Society (HIMSS) is an independent, non-profit organization with the mission “To lead healthcare transformation through the effective use of health information technology.”⁴ HIMSS and the American Health Information Management Association (AHIMA) are

professional associations that are highly respected in the fields of Information Technology (IT) and Health Information Management (HIM). Each has myriad sources, references, guides, best practices, and practice briefs for use in the selection and implementation of an EHR, and both organizations highly value certification.

In 2004, The American Health Information Management Association (AHIMA), the Healthcare Information and Management Systems Society (HIMSS), and the National Alliance for Health Information Technology (NAHIT) organized the Certification Commission for Health Information Technology (CCHIT). Its mission is to create a non-government, non-profit organization that would certify EHR software, and it was called the Certification Commission.

The mission of CCHIT, as found on its website, is to “…accelerate the adoption of robust, interoperable health information technology.” CCHIT is an independent, non-profit organization that certifies EHR systems.

Other certifying agencies include InfoGard, Drummond Group, Inc., and ICSA Labs, to name just a few. The ONC-certified Health IT Product List can be found at http://onc-chpl.force.com/ehrcert/.

Selecting a product that is certified is good business practice and will save the office administration much of the leg work necessary to ensure selection of a product that not only meets the needs of the organization, but has already been tested and proven to meet regulatory requirements.

It is worth a student’s time to view this listing, select one or more products, and view the ONC criteria that has been met by each.

## 7.4 Applying Security Measures

Assigning passwords, allowing access to only the functions that are necessary to perform a job, and following the other policies outlined in Section 7.1 all play a role in assuring the privacy, confidentiality, and security of the health information stored in your facility’s PM and EHR systems.

The next two exercises apply basic security measures in PrimeSUITE. These functions will usually be set up by the office administrator or manager.

### Adding Users to PrimeSUITE

#### EXERCISE 7.1

**Add a New Clinical User and Assign a Password**

In this scenario, the office manager has just hired a new MA, Kevin Goodell, and he is going to set Kevin up as a user in PrimeSUITE. Certain information is needed from Kevin before the office manager begins the

---

set-up process. You will notice that the password “greenway” is used in the initial set-up of Kevin Goodell. In the examples used throughout the worktext, the default password is “greenway.” In an actual work setting, this default password would be changed to a password of the user’s choice that meets the practice’s password requirements.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full name</td>
<td>Goodell, Kevin</td>
</tr>
<tr>
<td>Username</td>
<td>kgoodell</td>
</tr>
<tr>
<td>E-mail</td>
<td><a href="mailto:kgoodell@greenwaymedical.com">kgoodell@greenwaymedical.com</a></td>
</tr>
<tr>
<td>Sex</td>
<td>Male</td>
</tr>
<tr>
<td>Telephone number</td>
<td>(770) 555-1234</td>
</tr>
<tr>
<td>DOB</td>
<td>07/08/1958</td>
</tr>
<tr>
<td>Soc. Security No.</td>
<td>123-45-6789</td>
</tr>
</tbody>
</table>

Follow these steps to complete the exercise on your own once you have watched the demonstration and tried the steps with helpful prompts in practice mode. Use the information provided in the scenario above to complete the information.

1. Click **User Administration**.
2. Click **Add New**.
3. The *Username* field is filled out. Press the tab key to confirm your entry.
4. The *Email* field is filled out. Press the tab key to confirm your entry.
5. The *SSN* field is filled out. Press the tab key to confirm your entry.
6. The *First Name* field is filled out. Press the tab key to confirm your entry.
7. **Tab** is now pressed to bypass the middle name field.
8. The *Last Name* field is filled out. Press the tab key to confirm your entry.
9. **Tab** is now pressed again to advance past several fields.
10. The *Contact Number* field is filled out. Press the tab key to confirm your entry.
11. The *Date of Birth* field is filled out. Press the tab key to confirm your entry.
12. Click *Sex*.
13. Clicking the entry *male* selects it.
14. Click **Must Change Password At Next Login**.
15. Click **Save**.
16. The *New Password* field is filled out. Press the tab key to confirm your entry.
17. The *Confirm Password* field is filled out. Press the tab key to confirm your entry.
18. Click **OK**.
19. Click **OK**.

✓ You have completed Exercise 7.1
Setting Up Care Providers

In our next scenario, there is also a new care provider starting this week, Daisy Logan, M.D. The office manager will set her up in the system, assigning a user ID and user rights.

The information necessary before beginning the set-up process is:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full name</td>
<td>Logan, Daisy</td>
</tr>
<tr>
<td>Sex</td>
<td>Female</td>
</tr>
<tr>
<td>Credentials</td>
<td>MD</td>
</tr>
<tr>
<td>NPI number</td>
<td>1234567890</td>
</tr>
<tr>
<td>State Medical License number</td>
<td>234567</td>
</tr>
<tr>
<td>DEA Number</td>
<td>GA123456</td>
</tr>
<tr>
<td>On staff at Greensburg Medical Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Provides billable services from Greensburg Medical Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Assigned User ID</td>
<td>dlogan</td>
</tr>
</tbody>
</table>

Follow these steps to complete the exercise on your own once you have watched the demonstration and tried the steps with helpful prompts in practice mode. Use the information provided in the scenario above to complete the information.

1. Click **Care Providers**.
2. The **Last Name** field is filled out. Press the tab key to confirm your entry.
3. The **First Name** field is filled out. Press the tab key to confirm your entry.
4. Click **Sex**.
5. Clicking the entry **Female** selects it.
6. Click **Credentials**.
7. **M** is now pressed.
8. **MD** is selected from the drop-down list.
9. The **National Provider Identifier** field is filled out. Press the tab key to confirm your entry.
10. The **State License Number** field is filled out. Press the tab key to confirm your entry.
11. **Tab** is pressed to advance past the State Controlled Substance Number.
12. The **DEA Number** field is filled out. Press the tab key to confirm your entry.
13. Click **On Staff?**
14. Click **Billable?**

Go to http://connect.mcgraw-hill.com to complete this exercise.
Setting User Rights for Staff

We will take security functions a step further by adding user rights. Log-on rights simply mean that one is assigned a log-in and password to allow access to the computer software, in our case, PrimeSUITE. The user is then assigned user rights, which are privileges that limit access to only the functionality of the software needed by that individual. The position held and job description of each staff member (including care providers) dictate what privileges each person has.

Assign User Rights to an MA

In the scenario that follows, John Greenway is an office manager. He will be setting up the user rights for Kevin Goodell, an MA who is new to the office. We will start by setting up Chart rights from the action bar on the left side of the screen. Chart rights have to do with viewing, adding, editing, or changing documentation within patients’ charts. For instance, Kevin will be able to access the Patient Chart page of every patient. He will have access to a very extensive allergy module, which will include setting up a patient’s allergy shot schedule, dosage calculations, and similar applications. Of course, he will do this based only on the physician’s orders. John will be able to delete vital signs from a Facesheet; reasons for this may be that the vitals were incorrectly typed into the Facesheet, or were put on the wrong patient’s chart, or that the healthcare professional who entered the blood pressure, for example, did not get an accurate reading. These privileges are very sensitive and are only given to appropriate staff members with the expertise and position within the practice to warrant such rights. But even deleted, the original documentation is not lost forever—hidden is actually a better description for it—there is an audit trail that shows the original documentation, and then the corrected version. The topic of data integrity and versions of documentation will be covered in more detail later in this chapter.

Custom views of the Facesheet can be set up in many EHR software packages, PrimeSUITE included. The information displayed is consistent, but the way it looks on the screen is different. Some MAs or nurses are granted the right to sign off on lab results; that right is determined by office policy (and may vary by care provider) as well as level of knowledge of the individual. An example would be a standard blood test, such as a CBC, that is completely within normal limits on an established patient; the care provider may feel that an experienced MA or nurse is qualified to sign off on those results without

(continued)
sending them through for review by the care provider. The same applies to some prescriptions. The care provider may give a verbal order to an MA or nurse for a prescription renewal to be called in to the patient’s pharmacy or refilled by ePrescription. For example, Robyn Berkeley is a long-time patient of Dr. Rodriquez. She has a long-standing prescription for metronidazole for treatment of her rosacea, and she has run out; the MA gives Dr. Rodriquez the request, and he then authorizes her to send through a refill via ePrescribe. The MA is able to access and print (or electronically transmit) the prescription renewal with Dr. Rodriquez’s digital signature.

User rights for all registration functions are also set up; if the healthcare professional works in the reception and registration areas, she would have user rights to any routine daily functions including registering a patient for the first time, editing demographic information, scheduling an appointment, checking a patient in or out, viewing alert flags, and so on.

System rights affect just that—the overall system. The rights you will see in this exercise include importing documents that do not originate within PrimeSUITE and accessing patient tracking.

Follow these steps to complete the exercise on your own once you’ve watched the demonstration and tried the steps with helpful prompts in practice mode. Use the information provided in the scenario above to complete the information.

1. Click User Rights.
2. Click Current User.
3. Clicking the entry Kevin Goodell selects it.
4. Click Chart.
5. Clicking the entry Chart selects it.
6. Click Access the Patient Charts Page.
7. Click Allergy Module-Can modify serum sheet status.
8. Click Allergy Module-Override EP rules.
9. Click Facesheet-Delete vitals.
10. Click Facesheet-Manage problem list custom views.
11. Click Lab Flowsheet-Initial a lab or revoke initials.
12. Click Orders-Add to orders favorite list.
13. Click Orders-Edit/delete from orders favorite list.
15. Click OK.
16. Click Prescriptions-Can edit medication alert override.
17. Click OK.
18. Click Prescriptions-If a digital signature other than this user’s is saved with a prescription, allow printing of the signature.
19. Click OK.
20. Click Save.
21. Click Registration.
22. Click View Patient or Person Registration Information.
23. Click Modify Patient or Person Registration Information.
24. Click View Patient List.
25. Click Check-In patients
26. Click Undo Check-Out.
27. Click View and Modify Chart Patient Flags.
28. Click View Clinical Alerts Flags.
29. Click Save.
30. Click System.
31. Click Document Import.
32. Click Access Document Import.
33. Click Save
34. Click Patient Tracking.
35. Click Access Patient Tracking.
36. Click Save.
37. Click Close.

✓ You have completed Exercise 7.3

Setting User Rights for a Manager

Assign User Rights to an Office Manager

Office managers or administrators have increased functionality such as setting up files in accounts receivable management, chart configuration and administration, registration screens, research (clinical trial) functionality, reporting, scheduling, and overall system configuration. As you go through the exercise that follows, in which you will assign rights to Jennifer Pierce, take a look at the entire list of rights that are assigned. The research category pertains to participation in clinical trials that are run by the Food and Drug Administration.

Follow these steps to complete the exercise on your own once you have watched the demonstration and tried the steps with helpful prompts in practice mode.

1. Click User Rights.
2. Click Current User.
3. Clicking the entry Jennifer Pierce selects it.
4. Click A/R Management.
5. Click Select All.
6. Click Save.
7. Click Chart.
8. Clicking the entry Chart Admin selects it.
9. Click Select All.
10. Click Save.
11. Clicking the entry Research selects it.
12. Click Select All.
13. Click Save.
14. Click Registration.
15. Click Select All.
16. Click Save.
17. Click Reporting.
18. Click Select All.
19. Click Save.

(continued)
20. Click **Scheduling**.
21. Click **Select All**.
22. Click **Save**.
23. Click **System**.
24. Click **Select All**.
25. Click **Save**.
26. Click **Close**.

✔️ You have completed Exercise 7.4

### Setting Up a Group

Create a Group

In the previous exercises, we have been working with just one staff member. In this exercise we will set up an entire group within PrimeSUITE. Setting up groups, such as all medical assistants, all receptionists, all care providers, etc., allows the office administrator to give rights by group rather than having to set up each person individually. Of course, if some of the users within the group have higher-level rights, then their profile can be modified by adding rights individually.

In Exercise 7.5 we will be working within the Group Administration module of the Systems Menu. Essentially, a group is formed and the individual staff members are moved into it, and finally the group is named. Or, a group may already exist and staff members are moved into it. The other advantage of groups is that if an e-mail needs to be sent to an entire group, for instance, the health records staff, then just one e-mail needs to be sent rather than to each staff member. An example would be that the health records staff is required to attend an in-service meeting on HITECH regulations at 2:00 p.m. on August 5th. Just one message can be sent to the entire group notifying them of this in-service meeting.

Follow these steps to complete the exercise on your own once you’ve watched the demonstration and tried the steps with helpful prompts in practice mode.

1. Click **Group Administration**.
2. Click **Allison Tubiak (atubiak)**.
3. Click the arrow: **Move highlighted item to selected list**.
4. Click the **scroll button**.
5. Click **Jennifer Brady (jbrady)**.
6. Click **Move highlighted item to selected list**.
7. Click **Jared Howerton (jared)**.
8. Click **Move highlighted item to selected list**.
9. Click **Kevin Goodell (kgoodell)**.
10. Click **Move highlighted item to selected list**.
11. Click **Save Group**.
12. Enter **MAs** in the **Group Name Field**. Press the tab key to confirm your entry.
13. Click **Save**.
14. Click **Enable Messaging**.
15. Click **Save Group**.

✔️ You have completed Exercise 7.4
Set General Security

General security settings involve password maintenance. To complete the exercise, you will need the following information regarding Greensburg Medical Center’s security policies:

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password length</td>
<td>7 characters</td>
</tr>
<tr>
<td>Password change occurs</td>
<td>Every 90 days</td>
</tr>
<tr>
<td>Maximum inactivity before system</td>
<td>30 minutes</td>
</tr>
<tr>
<td>automatically logs off</td>
<td></td>
</tr>
<tr>
<td>No. of days before password can be</td>
<td>364 days</td>
</tr>
<tr>
<td>re-used</td>
<td></td>
</tr>
<tr>
<td>Log-in banner</td>
<td>Good Morning Greensburg!</td>
</tr>
</tbody>
</table>

Follow these steps to complete the exercise on your own once you have watched the demonstration and tried the steps with helpful prompts in practice mode. Use the information provided in the scenario above to complete the information. There are already some values that appear in the exercise, so we will not be covering every setting.

1. Click System Configuration.
2. The Min Password Chars field is filled out. Press the tab key to confirm your entry.
3. The Days Password Valid field is filled out. Press the tab key to confirm your entry.
4. Tab is now pressed to advance past the Visit Search Max Row Count field.
5. The Inactivity Limit field is filled out. Press the tab key to confirm your entry.
6. The Days Prevent Password Reuse field is filled out. Press the tab key to confirm your entry.
7. Click Save.
8. Click OK.

You have completed Exercise 7.6

Audit Trails

Run an Audit Trail Report

In this exercise, an audit trail report will be run. This functionality helps to fulfill the HITECH requirement to provide an accounting of disclosures (or, in this case, accesses to a record), or it may be used to monitor activity of a certain staff member or activity in general in a particular area of the EHR software. (continued)
Data integrity refers to the accuracy, timeliness of collection, the consistency of definitions used to collect the data, and, in addition, there is an expectation that there has been no manipulation or tampering with the data once it has been collected and reported. To maintain data integrity, the healthcare facility must have strict policies regarding who may access data, the definition of a complete record, accuracy of data, consistent applications of data dictionary definitions, and the timeliness of data entry. Think of it this way: if a patient is seen on Wednesday, but the documentation in the health record is not entered until Friday, how accurate do you think it will be? Or, if one of the staff members instructs a patient to document his past surgical history, but to only include surgeries done under general anesthesia in the past five years, yet the office policy shows a data dictionary definition of surgery as any procedure the patient has had while under local, regional, or general anesthetic at any time in the past, then how consistent is the data? What about a healthcare professional who finds a blood pressure reading of 152/80 in a patient, yet enters it as 140/80 and knowingly leaves it as is, figuring it is “close enough.” If you were a care provider using the information found in your EHR database, and you knew poor documentation practices were occurring, you wouldn’t have much faith in using that data would you? Or, if you were conducting a research study and knew that the data was flawed, how valid would the study be? In other words, any data found within the health record must be accurate, complete, and documented at the time of or as close to the time of occurrence as possible.
Amending a Chart Entry

Integrity also applies to the addition, amendment, or omission of documentation that has already been recorded. Any alteration in the original documentation must be recoverable. With the use of paper records, if an entry in a health record was amended or corrected, it was obvious. See Figure 7.1 for an example of a proper chart correction. You can see readily that the entry was corrected; originally, it read that the patient had sustained a laceration to her right hand, when in fact, it was the left hand. A single line was drawn through the incorrect word, the correct word was inserted, and the correction was initialed and dated by the person who made the correction.

In an electronic record, original documentation that is found to be incorrect or incomplete may be hidden from view, and the amended information becomes part of the health record and is all that is viewable to the healthcare professional or care provider; however, that original hidden documentation can be recovered at any time. Our next exercise illustrates amendment of an entry in PrimeSUITE.

Amend a Chart Entry

William Jackson’s record contains an error in the progress note. The care provider documented the HPI of William Jackson, but after she completed documenting and saved the note, she noticed a word was misspelled. She accesses the progress note of the chart and makes the correction. Notice, while going through the exercise, that in order to make the correction, the care provider must enter her password in order to change an entry. This additional step allows the care provider to think twice about amending the entry to be certain it is necessary and that the information she is about to add is correct. The original progress note with the error is known as version 1 and the corrected progress note as version 2.

Follow these steps to complete the exercise on your own once you’ve watched the demonstration and tried the steps with helpful prompts in practice mode.

1. Click Documents.
2. Click Progress Note.
3. Click Amend Document.
4. Click HPI.
5. A letter “s” is added to the end of the word “present.” Press the tab key to confirm your entry.
6. Click Save & Sign.
7. The Password: field is filled out with greenway. Press the tab key to confirm your entry.
8. Click the green check mark.
9. Note the lower left corner of the action bar.

You have completed Exercise 7.8
Hiding a Chart Entry

There are times when documentation is added to the wrong chart, or when misinformation is given or documented. In these cases, we would need to hide an entry. As noted above, though the entry is hidden, it is still retrievable at a later time. Our next exercise steps us through hiding an entry on William Jackson’s chart. In this case, it is a progress note that was intended for another patient’s chart. Typically, only certain staff members such as those who are in lead or administrative positions have this user right. This is not a procedure that is done often, nor is it done without a valid reason. Reasons might be that the note was put on the wrong patient’s chart, or that the note pertains to that patient but not to that particular visit. Some software vendors use the term deleting rather than hiding, but regardless, the deleted/hidden entry will always be retrievable should the record be needed in a lawsuit, to verify some sort of inconsistency, or for insurance purposes.

Follow these steps to complete the exercise on your own once you have watched the demonstration and tried the steps with helpful prompts in practice mode.

1. Click Documents.
2. Click Manage Chart Documents.
4. Click Delete.
5. Click Yes.
6. Click Other.
7. The Other field is filled out with wrong patient. Press the tab key to confirm your entry.
8. Click OK.

✓ You have completed Exercise 7.9

Recovery of a Hidden Entry

Recover a Hidden Chart Entry

Hiding a document does not mean that it is truly deleted forever. The original documentation can be retrieved by accessing the Documents Menu and then accessing Manage Chart Documents from the action bar.

Follow these steps to complete the exercise on your own once you have watched the demonstration and tried the steps with helpful prompts in practice mode.

1. Click Documents.
2. Click Manage Chart Documents.
3. Click View Deleted Docs.
5. Click Undo Delete.
6. Click Yes.
7. Click Accidental Delete.
8. Click OK.

✓ You have completed Exercise 7.10
Another requirement of Meaningful Use initiatives is to share health information with other healthcare professionals when necessary. For instance, Virginia Hill is a patient of Dr. Ingram’s, and he is referring her to a specialist. It is important for the specialist to know her medical history and the reasoning for the referral; therefore, information is released electronically. This reason is known as continuity of care.

Many releases require a written authorization from the patient or legal representative. The specifics of release of information regulations will be covered in another course. For our purposes, we will be accounting for the disclosure. Release of information in the case of this referral would not require an authorization, nor would release of information to an insurance company for purposes of payment of the claim, nor release of information to public health agencies, as required by law. Written authorization is required for all releases of information to physicians’ offices or hospitals that are not a result of a direct referral, attorneys, employers (if not a Workers’ Compensation claim), spouse, children, and law enforcement agencies. Also, certain records such as those related to drug and alcohol abuse, mental health, and HIV/AIDS have more stringent release of information regulations; those will be discussed in great detail in another course.

Releasing information without a required authorization is known as a breach of confidentiality. Offices and healthcare facilities are required to report breaches, as was discussed earlier in this chapter, as part of the HITECH regulations. Not only is the office or facility held liable for any breaches, but individual staff members may be as well.

---

**Composed a Correspondence Letter to Accompany the Release of a Patient's Immunization Record**

Now, let’s look at an exercise where a correspondence letter is accompanying the release of immunization records of a patient, Ian Mikeals, to a day care center as requested by the child’s mother.

Ian Mikeals has had the following vaccines: Hepatitis B, Pentacel (DTaP – IPV/Hib), PCV13, and ProQuad (MMRV).

Follow these steps to complete the exercise on your own once you’ve watched the demonstration and tried the steps with helpful prompts in practice mode. Use the information provided in the scenario above to complete the information.

1. Click **Search for Patient**.
2. The **Last Name** field is filled out. Press the tab key to confirm your entry.
3. Click **Search**.
4. Click **Select**.
5. Click **Patient Charts**.

(continued)
An accounting of the releases is also necessary in order to comply with regulations. As noted above, most releases require a written authorization, but to comply with HITECH, all releases must be accounted for, whether the disclosure is to internal staff members or external requestors.

### 7.7 Accounting of Information Disclosures

An accounting of the releases is also necessary in order to comply with regulations. As noted above, most releases require a written authorization, but to comply with HITECH, all releases must be accounted for, whether the disclosure is to internal staff members or external requestors.

**EXERCISE 7.12**

**Run a Report of Information Disclosures for a Particular Patient**

In this scenario, the office manager needs to run a report of information disclosures (or, in this case, access) of the chart of a patient, Megan Hallertau, whose chart ID is 19927. She is particularly looking for disclosures (accesses) to one of the staff members, Bob Denney, who has a user ID of bdenney, that were made today.

Follow these steps to complete the exercise on your own once you have watched the demonstration and tried the steps with helpful prompts in practice mode. Use the information provided in the scenario above to complete the information.

1. Click **Report Selection. . . F7.**
2. Click **System.**
3. Click **Audit Log Report.**
4. Click **User.**
5. The letter b is pressed.
6. The **Patient ID** field is filled out. Press the tab key to confirm your entry.
7. Click **Component.**
Communicating with other healthcare providers is another Meaningful Use requirement. It is known as **Health Information Exchange (HIE)**. An advantage of utilizing an EHR is that patient care improves through the sharing of patient information at the point of care. With this functionality, care providers can access the findings of other physicians or test results immediately. Of course, this sharing is done through a secure environment, and there are regulations that address telecommunications and networking security as well. Secure e-mail is one way that information can be shared between providers, the National Health Information Network (NHIN) Exchange is another, and there are state and private HIE programs as well. The State HIE Cooperative Agreement Program operates through use of ONC funding, and its purpose is to coordinate local HIEs or serve as the HIE for a given area.

**7.8 Information Exchange**

Using a search engine, take the time to find your state’s HIE on the Internet; each HIE has its own site and includes valuable information for care providers and staff.

**Exchange of Information for Continuity of Care**

In this scenario, Ian Mikeals is a pediatric asthma patient of Dr. Ingram. Dr. Ingram is referring Ian to a pediatric asthma specialist. Follow these steps to complete the exercise on your own once you’ve watched the demonstration and tried the steps with helpful prompts in practice mode.

1. Click **Document Import**.
2. Click **Data Submission**.
3. Click **Referral Summary (XDS-MS)**.
4. The **Reason for Referral** field is filled out with **asthma**. Press the tab key to confirm your entry.
5. Click **Preview**.
6. Click **Print**.
7. Click **Close**.

**Exchange of Information Outside the Organization**

There is another type of information exchange that has nothing to do with continuity of care, business purposes, or insurance purposes. It involves communicating about care via **social media**. Social media includes Facebook, YouTube, Twitter, **blogs** (ongoing
conversations about a topic that take place on-line), and the like). These outlets are used by patients to share their experience with a healthcare organization or to recount their journey through an illness; they can also be used by the organizations themselves as a means of marketing or public relations. Take a look at the Facebook page of Children’s Hospital, Boston, for example, found at http://www.facebook.com/#!/ChildrensHospitalBoston?sk=info. Here you will find videos, testimonials, facts and figures about its patient population, and links to other related sites, as well as support groups and blogs, awards the organization has won, and a link to its social media policy, which is short, to the point and, in summary, states that while all comments are welcome, they should not be offensive, should be on-topic, and should not violate the privacy of patients or their family.

There is some risk in allowing patients to provide comments since not all of them will be positive, but by the same token, they are a vehicle to promote the institution, its accomplishments, and its services. They are also a service to the community by including needed information about the organization as well as links to related sites such as public health, educational sites, and support groups.

Employees of an organization also use social media (Facebook, Twitter, and LinkedIn, for example) and may contribute to blogs about their organization. Since what they say and how they say it can sometimes be misconstrued, it is imperative that healthcare organizations develop a policy to address the use of social media; and it should include this information:

- Circumstances under which an employee may access any social media site during work hours.
- Employees should maintain a positive tone in their posts, and be respectful of the organization and its staff when posting on an organization-sponsored site.
- The PHI of patients should never be posted (directly or implied).
- The identity of any patients (directly or implied) should never be posted.
- No copyrighted materials should be posted.
- No information about the organization may be posted, as this is the responsibility of the marketing or public relations department.
- Penalties or potential disciplinary action for failure to comply with the organization’s social media policy.

The use of social media to share information about a particular person, which is set up and maintained by someone authorized by the patient with the objective of keeping family and friends updated on the patient’s condition, is gaining popularity. One such site is Caring Bridge (www.caringbridge.org). What the patient or family cares to share on this site is under their control, but healthcare professionals who are or were involved in the patient’s care need to be careful. A posting that you intend to be caring and helpful may be misinterpreted and perceived as intrusive by the family, so before posting, you should think twice about what you want to say and how you say it!
7.9 Compliance Plans

Think of all the regulations that affect healthcare—HIPAA, ARRA, HITECH, not to mention Medicare, Medicaid, and managed care plan requirements; it is a daunting task to ensure compliance with all of them. Having a formal compliance plan is key to surviving the regulatory maze. Think of a compliance plan as your office or facility’s policies that assure regulations are followed, and use it as a check-sheet to assure that staff and care providers in your office or facility are following your own policies, which in turn ensure the following of rules and regulations. A compliance plan should include:

- A named compliance officer—a staff member who keeps up with new regulations, monitors existing ones, and is the “go-to” person, should an incident occur that is not in compliance.
- Written policies that cover, at a minimum:
  - Routine daily operations (registration, scheduling, human resources, etc.)
  - File back-up
  - Computer access (both physical access as well as access to software and databases)
  - Release of patient information
  - Breach of confidentiality, including unauthorized disclosure
  - Security breaches, internal and external
  - Coding and billing (including anti-fraud and -abuse practices)

Policies should be kept in a location accessible to all office staff. All policies should also include the disciplinary process, should policies not be followed, intentionally or unintentionally.

An example of a Policy Statement regarding computer access and use of passwords may read:

Access to computer software, databases, and equipment shall be restricted to employees (including care providers) of Greensburg Medical Center. The extent to which access and rights are given is based on position description in order to carry out their job duties. Employees (including care providers) are required to keep their log-in user ID and password confidential; sharing with others is grounds for immediate disciplinary action, up to and including dismissal.

Reporting of compliance with Meaningful Use is also required; specific compliance strategies to conform with Meaningful Use will be covered in Chapter 9.

The use of formal internal audits, which should be performed on every staff member (including care providers) on a periodic basis, not only allows the administrative staff to be proactive in finding and correcting problems, it also serves as a reminder and an educational tool for staff.

7.10 Safeguarding Your System and Contingency Planning

Protecting computer hardware and software is as important as protecting the information within the systems. Computer crime, unauthorized access to information, and natural disasters are all security concerns that must be addressed within any healthcare organization that processes or stores digital data.
Written policies as noted in Section 7.9 are deterrents at a very basic level, in particular, regarding controlling access. Restricting access in offices or areas where computers are present to employees only, turning computer screens away from public view, and shredding printed documents that include patient information are all examples. Encryption of data is necessary to deter unauthorized access to what is documented. Tracking the computer accesses of all employees on a periodic basis helps ensure that access is only on a need-to-know basis. Carefully screening job applicants and verifying previous employment are additional important screening mechanisms, since people are the greatest threat to computer security.

Backing up data on a daily basis is crucial. Back-up can be made to online secondary storage, hard disk, optical disk, magnetic tape, and/or flash memory. A key component of back-up is that the backed-up files should be stored at an off-site location. Should a fire or flood occur in your office, and the back-up files are also damaged by the flood, they do little good.

Recent worldwide disasters have shown the need for having a disaster recovery plan. The plan must be written and staff must know what to do in the event of a disaster that affects the computer systems within the facility. At a minimum, the plan should include:

- An accounting of all functions that are performed electronically within the office
- A listing of all computer hardware, software, and data related to each of those functions
- The specific location of the back-up files and the format used for the back-up
- Step by step procedures for restoring the backed-up data
- An alert system to notify personnel of the disaster
- Required security training for all personnel

Unfortunately, many facilities lack a disaster recovery plan and may not realize its importance until a data loss, security breach, or other disaster occurs. Not only should the facility have a plan, they should actually carry out the plan periodically as any other disaster plan would be practiced.

The importance of keeping all computerized functions safe, confidential, and secure cannot be overstated.

---

### LEARNING OUTCOME CONCEPTS FOR REVIEW

**7.1 Identify the HIPAA privacy and security standards.**

- HIPAA passed in 1996
- Contains privacy and security rules, among others
- HITECH made HIPAA rules more stringent and gave government authorities the power to enforce the privacy and security rules
- The intent is to ensure protected health information (PHI) is private and secure
- Covered entities include any healthcare facilities, health plans, clearinghouse, or other businesses that handle PHI
- Only minimum necessary information may be released
- Standards include:
  - Define directory information
  - Use of authorization to release PHI
  - Enforce minimum necessary information release
  - Password configuration and protection
  - Appointment of a privacy and/or security officer
  - System configured to minimize number of login attempts
  - Protection from viruses and malware
  - Use of security audits to monitor access
  - Policy to address remote access to the system
  - Policy on use and protection of hardware, particularly wireless devices
  - Written policy and procedures on breach notification
  - Staff education

**7.2 Evaluate an EHR system for HIPAA compliance.**

**HIPAA Regulations and the EHR**

- Password protection
- Use of unique identifier for each user
- Access to PHI only for those who have a need to know
- Accounting of all disclosures (internal and external)
- Security policy that addresses back-up of data, storage, and restoration of backed-up data
- Ability to audit by user or by patient who has accessed a record, and which area(s) of the record were viewed, edited, or deleted
- Use of code sets—ICD-9-CM, CPT, and HCPCS to store and transmit information

**7.3 Describe the role of certification in EHR implementation.**

- CCHIT organized by AHIMA, HIMSS, and NAHIT in 2004
- Mission is to accelerate the use of an interoperable health information technology
- Role is to certify EHR systems that meet all requirements of HIPAA and HITECH
<table>
<thead>
<tr>
<th>LEARNING OUTCOME</th>
<th>CONCEPTS FOR REVIEW</th>
</tr>
</thead>
</table>
| 7.4 Apply procedures to set up security measures in PrimeSUITE. pp. 136–144 | - Add new clinical users  
- Assign password to new clinical users  
- Set up a care provider’s user rights  
- Assign user rights to a healthcare professional (medical assistant)  
- Assign user rights to an office manager  
- Create a group  
- Set general system-wide security requirements  
- Run an audit trail report |
| 7.5 Apply procedures to ensure data integrity. pp. 144–146 | - The integrity of data can be ensured only if it is complete, accurate, consistent, timely, and has not been altered, destroyed or accessed by unauthorized individuals  
- Strict organization-wide policies that are adhered to must be in place  
- Amendments and deletions to entries must be obvious, and the original format must remain  
- Amend a chart entry  
- Hide a chart entry  
- Recover a hidden chart entry |
| 7.6 Apply procedures to release health information using PrimeSUITE. pp. 147–148 | - Release of information is necessary for a multitude of reasons, including continuation of care  
- Authorization to release information may be required, and must be addressed in written organization policies  
- Must account for all disclosures to comply with HITECH  
- Compose correspondence and release immunization record using PrimeSUITE |
| 7.7 Account for data disclosures using PrimeSUITE. pp. 148–149 | - Internal and external disclosures of PHI must be accounted for  
- Run a report of information disclosures from a patient’s chart |
| 7.8 Exchange information with outside healthcare providers for continuity of care using PrimeSUITE. pp. 149–150 | - Meaningful Use standards require exchange of information between providers for smooth continuation of care  
- Sharing of electronic information must be through secure means  
- Exchange information for continuity of care using PrimeSUITE |
| 7.9 Outline the content of compliance plans. p. 151 | - Healthcare organizations must have written compliance plans that address how the organization ensures compliance with all regulations governing operation of the organization as well as privacy, security, Meaningful Use, and general health information regulations  
- Written policies must be kept and available to all staff at all times |
| 7.10 Appraise the importance of contingency planning. pp. 151–152 | - Contingency plan is equivalent to a back-up plan, should the system fail or a natural or other disaster occur  
- All potential security concerns should be addressed with a detailed back-up plan  
- A written Disaster Recovery Plan should be in effect |
MULTIPLE-CHOICE QUESTIONS
Select the letter that best completes the statement or answers the question:

1. [LO 7.6] In the event of a breach, who may be held responsible?
   a. Providers
   b. Office staff
   c. The facility
   d. All of the above

2. [LO 7.1] Which of the following would be considered a covered entity?
   a. Healthcare provider
   b. Friend
   c. Significant other
   d. Teacher

MATCHING QUESTIONS
Match the terms on the left with the definitions on the right.

1. [LO 7.4] breach
   a. person or group who has legal right to access protected health information by virtue of being a healthcare provider, clearinghouse, or health insurance plan

2. [LO 7.1] confidentiality
   b. private, secure code that allows a user access to computer systems and software

3. [LO 7.1] hardware
   c. security measure in which words are scrambled and can only be read if the receiving computer has the code to read the message

4. [LO 7.4] audit trail
   d. listing of patient information, such as hospital room number

5. [LO 7.1] virus
   e. plan for addressing critical issues in the event of a crisis

6. [LO 7.1] covered entity
   f. permanent record of the changes made to various documents; available even after files are deleted

7. [LO 7.1] password
   g. a break or failure of security measures that results in information being compromised

8. [LO 7.10] disaster recovery
   h. devices such as laptops, PDAs, and desktop computers that are at risk for theft

9. [LO 7.1] directory
   i. keeping information about a patient to oneself

10. [LO 7.1] encryption
    j. deviant program, stored on a computer floppy disk, hard drive, or CD, that can destroy or corrupt data.

Enhance your learning by completing these exercises and more at http://connect.mcgraw-hill.com!
3. **[LO 7.4]** Of the following, which factor contributes to the access rights allowed a user?
   a. Annual job performance
   b. Job description
   c. Level of education
   d. Number of patients seen

4. **[LO 7.10]** It is critical that back-up files be stored:
   a. in paper form.
   b. offsite.
   c. onsite.
   d. with the originals.

5. **[LO 7.7]** HITECH regulations require that _______ information releases are accounted for.
   a. all
   b. external
   c. internal
   d. no

6. **[LO 7.2]** According to HIPAA regulations, healthcare providers must use _______ as opposed to written diagnoses to store and transmit information to insurance carriers.
   a. CPT codes
   b. ICD-9 codes
   c. HCPCS codes
   d. all of the above

7. **[LO 7.3]** Meaningful Use standards require offices to select an EHR that is:
   a. certified.
   b. cheap.
   c. fast.
   d. simple.

8. **[LO 7.6]** Releasing information without proper authorization is called a/an:
   a. breach of confidentiality.
   b. breach of trust.
   c. information breach.
   d. security breach.

9. **[LO 7.5]** When a document is amended or changed in an EHR, the original documentation is:
   a. deleted.
   b. hidden.
   c. printed.
   d. visible.

10. **[LO 7.9]** An office’s compliance manual should be kept in a/an _______ location.
    a. accessible
    b. external
    c. electronic
    d. protected
11. [LO 7.8] The sharing of health information must be done in a ______ environment.
   a. healthcare
   b. private
   c. public
   d. secure

12. [LO 7.4] Under a care provider’s order, medical assistants and nurses ________ allowed to send an ePrescription or call in a refill prescription to a pharmacy.
   a. are
   b. are not
   c. might be
   d. should not be

13. [LO 7.1] To help guard against security breaches, e-mails containing protected health information should be:
   a. deleted.
   b. encrypted.
   c. forbidden.
   d. sent.

14. [LO 7.3] The mission of CCHIT is to:
   a. actively promote the use of smartphones.
   b. ensure information security.
   c. increase the implementation of EHR systems.
   d. train facilities on HIPAA regulations.

SHORT ANSWER QUESTIONS

1. [LO 7.2] According to the ONC website, how does health information technology help care providers manage patient care better?


3. [LO 7.1] List at least four ways to keep information stored on your computers and hardware safe.

4. [LO 7.5] Why must a user enter her password in order to change a chart entry in PrimeSUITE?

5. [LO 7.9] List at least six pieces of information that must be included in an office’s compliance plan.

6. [LO 7.10] List the six pieces of information that form the minimum requirements of a disaster recovery plan.

7. [LO 7.4] List three responsibilities that fall into the office manager’s or office administrator’s job description.

8. [LO 7.3] What does it mean if an EHR system has been certified by the Office of the National Coordinator?
9. **[LO 7.1]** Explain what a security audit is, and list one example of when a security audit might need to take place.

10. **[LO 7.8]** Explain one advantage of using an EHR for communicating with other healthcare providers as discussed in the text.

11. **[LO 7.9]** What is the best way to ensure that your office is following all the different regulatory bodies governing healthcare?

12. **[LO 7.7]** Why must an office manager account for all information released, including those released internally?

13. **[LO 7.4]** Would a care provider and a medical assistant be assigned the same rights in PrimeSUITE? Why or why not?

14. **[LO 7.2]** List six things that an office's EHR team should keep in mind when rolling out a new system.

15. **[LO 7.10]** List three methods to safeguard computer hardware and software systems.

**APPLYING YOUR KNOWLEDGE**

1. **[LOs 7.1, 7.8]** Discuss two advantages and two disadvantages of using e-mail to send information between providers.

2. **[LOs 7.1, 7.2, 7.4, 7.9, 7.10]** Discuss why many practices require users to change their passwords after a specified period, and why they do not allow users to reuse the same passwords over and over again.

3. **[LO 7.3]** Imagine that you are working in a small healthcare practice. Your supervisor has asked you to spearhead the adoption of an EHR program. Follow the link provided in the text to find the website listing certified EHRs. After browsing the site and looking at the sheer number of products listed, discuss some methods your healthcare office could use to choose the best EHR option.

4. **[LOs 7.5, 7.6]** Provide an example of both an internal and an external Breach of Confidentiality that might occur in a healthcare setting, and list a possible consequence of each breach. (For example, letting a temporary employee access a patient’s chart with your username would be an internal breach; a consequence could be that a patient’s health information is compromised when the temp accidentally sends the patient’s chart information out in an accidental “reply all” e-mail.)

5. **[LOs 7.1, 7.4, 7.5, 7.9, 7.10]** You are in the office cafeteria getting some water. One of your colleagues is at her desk, working on a laptop. She gets up to join you at the water cooler. As the two of you are talking, another staff member sits down in your colleague’s chair and begins using the laptop to check her e-mail. What is wrong with this scenario?