JOY DARK
JEAN ANDREWS

AUTHORIZED

Authorized Cert Guide

Learn, prepare, and practice for exam success

- Master every topic on the HIT-001 exam.
- Assess your knowledge and focus your learning.
- Get the practical workplace knowledge you need!

CompTIA

HEALTHCARE IT TECHNICIAN

HIT-001

PEARSON
IT CERTIFICATION

CompTIA® Healthcare IT Technician HIT-001 Authorized Cert Guide

Joy Dark
Jean Andrews, Ph.D.

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

A covered entity might access e-PHI to distribute to the individual or its own personnel for treatment of the patient or to retrieve payment from the patient's insurance provider without acquiring a release form. Access permission is restricted based on the role of the personnel, called role-based access control. Personnel should have access to e-PHI only as required to fulfill their job descriptions, no more, no less. Ultimately the CFO has the final say in what access to the information systems used in the hospital is granted to hospital personnel. The CFO makes these determinations by approving access to each job role when each IS is initially configured. Therefore, the CFO does not need to be involved with assignments for each employee. When a professional starts a job at a healthcare facility, he is given access to e-PHI as defined by his job. For example, all lab technicians should have access as defined for a lab technician. All nurses should have access as defined for a nurse. A lab technician and a nurse might not have the same access. While performing duties of their job, these personnel do not require signed release forms from patients. The personnel is required to sign an acknowledgment of understanding HIPAA rules. These access policies are controlled by the covered entity and are expected to comply with HIPAA and state regulations.

The HHS offers case studies of HIPAA violations on its website. An example of one case study was a hospital employee who left a voicemail for a patient on the patient's home answering machine. The message included the medical condition and treatment plan of the patient. However the patient did not live alone and others in the household listened to the message. The patient had specifically asked to be contacted at her work phone number. The hospital employee did not follow confidential communication requirements as set by the hospital. To resolve this violation, the hospital implemented new policies for communication. For example, the policy set rules for the minimum information required to leave in a voicemail so as to not reveal PHI. The hospital also trained employees how to review registration information from patients to verify special instructions from the patient on how to contact them. Finally, the hospital integrated training for these new policies into the annual refresher series for employees.

With the background surrounding agencies, laws, and regulations covered, now turn your focus to a topic a little more practical: the rules of record retention and disposal.

Learning Rules of Record Retention and Disposal

HI001 Objectives:

1.3 Summarize regulatory rules of record retention, disposal, and archiving.

Documentation requirements, Time of storage, Types of records, Public records, Private records, Legal health record, Methods of record disposal

Documentation requirements are defined by HIPAA, but some requirements vary from state to state. The state defines how long records must be kept, called record retention. HIPAA defines how records are disposed of and how they are kept in storage (archived). The three types of records are public, private, and legal. All these follow the same rules for retention and disposal.

Types of Health Records

Health information comes in three different types. A patient's **public health record** is used for research and to create reports for public health data. For example, if a state requires a hospital to report how many patients are at risk for getting the flu, the public health records are accessible to calculate this information. Figure 3-10 shows the reporting function of an example EHR IS. Public health records are not intended to connect individuals to their health records.

public health record—Researchers need access to health records to analyze data. For this reason a public health record is made available for the collection of public health data in an anonymous manner.

A **private health record** is the health record created and maintained by an individual. The benefit of a private health record is the individual is completely aware of all healthcare received and is available to the individual no matter where she may be a patient. A private health record is great for chronically ill patients or for an individual who is a guardian of another individual.

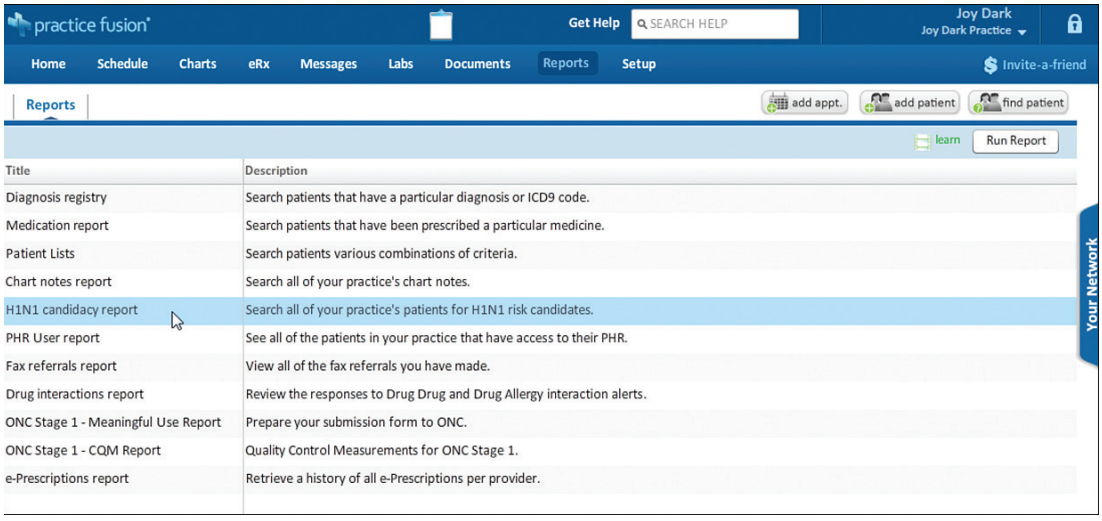

Figure 3-10 The reporting feature of an EHR IS provides a list of patients at risk for the H1N1 virus.

Photo credit: http://www.practicefusion.com

> **private health record**—A health record created and maintained by an individual. Sometimes called a personal health record (PHR).

An individual may keep a private health record in any format she prefers. She may simply place her health records in a file folder on her computer or move it to a jump drive for added security and mobility. She might decide to keep her health records with a web-based service designed for private health records. The benefit of using a web-based service is that many healthcare providers can access and easily format the data from these services for the HIS used at the facility with the permission from the individual.

A **legal health record** is the health record created by healthcare providers. The regulations for legal health records are set by the state and healthcare organization with a few basic standards set by the federal government. The legal health record can be requested by the patient or legal services. For example, if a patient brings up a lawsuit due to received healthcare, the court might need the legal health record to know what was charted in the patient's health record.

legal health record—Health organizations must retain a health record of patients for use by the patient or legal services.

Record Retention

HIPAA sets a minimum timeframe for record retention of six years and for two years after a patient's death, and Medicare requires Medicare beneficiaries' records be retained for five years. HIPAA enables the states to create laws to dictate their own policy for record retention so long as the state law meets minimum HIPAA requirements. If a state requires more time for record retention, covered entities in that state must comply with the state law.

States have the freedom to determine how long documents need to be stored before disposal. States retain records anywhere from 6 to 20 years. Some states choose to vary the length of record retention based on resources, type of patient, events during the course of care, or any other stipulation.

When you start a new job, check with your state's legislature website or ask someone in the medical records department at your facility. For example, if your new job is to implement a new EMR/EHR IS in a hospital, you would need to know how long to program the EMR/EHR IS to retain the health records.

Record Disposal

HIPAA states that record disposal is the responsibility of covered entities. Physical documentation can be shredded, burned, or pulverized. PHI on electronic media is sometimes disposed of by cleaning, purging, or destroying the device. The covered entity is at fault if any physical or electronic PHI is recovered at any point after the disposal of records.

The basic rule when disposing of an electronic device that contained e-PHI is to make sure the data on the device is unreadable, is indecipherable, and cannot be reconstructed. Following are three ways records on electronic media can be disposed of :

- Cleaning the device is when irrelevant data (1s and 0s) is written on the memory several times. This method is considered unacceptable in the healthcare environment by many technicians. The only reason cleaning a device is okay is when the device has never had PHI on it; for example, the gift shop computer or the server used to control HVAC in the facility.
- Purging or degaussing is when exposure to a strong magnetic field is used to purge data from the device.

- Destroying a device is when physical destruction is used to render a device useless. For example, you can drive a nail through a hard drive to make sure no one can recover the data that was once on that hard drive.

Learning Legal Best Practices and Documentation

HI001 Objectives:

1.4 Explain and interpret legal best practices, requirements, and documentation.

Waivers of liability, Business Associate Agreements (BAA), and Third-party vendor review agreements (SLA, MOU)

Whether or not it is convenient, HIT technicians must deal with legal issues. You need to make sure you are covered for all possible legal issues, so if any issues come up you will be prepared. Best practices and documentation need to be established for HIT technicians because of the necessity to be prepared for a legal issue. For example, HIT technicians are responsible for having the ability to audit all PHI accessed. With the ability to audit activity in information systems, if someone in the hospital violates HIPAA by viewing a patient's record they should not, the IS can track who accessed the e-PHI that was violated. As another example, when you depend on a vendor to support the equipment in the lab, a contract with the vendor is needed to know the time frame the vendor has to reply to repair needs. If the vendor is slow to respond to your repair requests, you have the contract to remind the vendor of its agreements with consequences to not meeting the commitments outlined.

Hospitals and healthcare providers must use legal best practices to protect themselves from unwarranted lawsuits. **Waivers of liability** are forms used by healthcare entities to be protected from being inappropriately responsible or sued for harm or debt. An example of a waiver of liability relates to Medicare. Medicare has a law that states healthcare providers are only responsible for providing services that are reasonable and necessary for a patient's health. However if a patient wants further healthcare, the patient can sign a waiver of liability to receive services not covered by Medicare if he agrees to pay out-of-pocket for the expense of the extra services.

waiver of liability—A contract used to protect healthcare entities from being inappropriately responsible or sued for harm or debt.

HIPAA requires that when a covered entity requires the services of a person, company, or organization outside the organization, the covered entity must enter into contracts with these third parties. The purpose of this **business associate agreement (BAA)** is to establish rules for safeguarding e-PHI. Third parties need access to e-PHI to fulfill obligations to a covered entity. For example, a vendor needs access to data that might contain e-PHI to research a bug that needs to be fixed with the next update to an IS.

business associate agreement (BAA)—A contract used between healthcare entities and third parties to establish a mutual understanding of safeguards of e-PHI.

Access allowed to business associates must be limited to the minimum amount of access required to perform necessary functions and activities of the job. This access is controlled by role-based access. This access must have the ability to be audited for activity of the business associates, the same as how auditing abilities are required for internal e-PHI activity.

For example, third parties need a BAA to access e-PHI data to perform the following functions:

- Insurance claims processing
- Data analysis
- Quality assurance
- Private practice office management

Covered entities often require third-party assistance with operations; for example, a software vendor might be contracted to support software and provide regular updates and bug fixes. It is recommended to have a **service-level agreement (SLA)**. An SLA, much like a BAA, establishes how information is to be shared and used. It also sets expectations for service provided so everyone is on the same page and understanding.

service-level agreement (SLA)—Contracts used between healthcare entities and third parties to establish how e-PHI is shared and used. An SLA also establishes expectations of service provided.