

***Mercy Hospital***

***HIPAA Confidentiality and  
Privacy Training***

**For Healthcare Staff**

***Participant Self-Study  
Guide***

**Introductory Module**

**Department of Organization Development  
Human Resource Management**

# *HIPAA Confidentiality and Privacy*

## **Table of Contents**

<b>Course Outline and Objectives</b>	<b>3</b>
<b>Introduction and Overview: What is HIPAA</b>	<b>4</b>
<b>HIPAA: Confidentiality and Privacy Summary Sheet</b>	<b>6</b>
The HIPAA Privacy Rule	
Who is covered by the Privacy Rule	
What is Required of Providers?	
Rule Compliance Date	
Fines	
Protected Health Information	
Authorization for Use and Disclosure of PHI	
Safe Guarding PHI	
Rights and Responsibilities	
Provider (Hospital) Responsibilities	
Provider Rights	
<b>HIPAA Terminology</b>	<b>11</b>
HIPAA	
Administrative Simplification	
Protected Health Information	
HIPAA Rights for Patients	
Covered Entities	
HIPAA Obligations	
Workforce Education	
Business Associates	
State Preemption	
Notice of Privacy Practices	
Acknowledgement of Notice	
Treatment, Payment, Healthcare Operations (TPO)	
Authorization	
Agree or Object	
No Opportunity to agree or object	
Minimum Necessary	
Reasonable appropriate security	
Complaints of Violations	
Sanctions	
HIPAA Penalties and Sanctions	
<b>HIPAA: Privacy, Confidentiality, Data Security Dilemmas</b>	<b>14</b>
Post Test	16
Answer Keys	19-20

# *HIPAA Confidentiality and Privacy*

## **Course Outline**

The program is designed to introduce staff, volunteers, and students to the requirements for privacy and confidentiality under the ***Health Insurance Portability and Accountability Act (HIPAA)***. Training materials will cover an overview and background of HIPAA, Purpose of the HIPAA rule, Major provisions of the HIPAA privacy standard, and applications to staff at Mercy Hospital.

The course will discuss workplace practices that may affect privacy and confidentiality, and the risks of breaching confidentiality. Definitions of key terms and examples of breaches in confidentiality, privacy, and security will be presented.

### **Intended Audience:**

**This session is intended for general workforce training.** The intensity of education and training varies by the level of access the staff has to protected health information. Staff with high access to PHI (protected health information) will need **further training specific to employees' job function**. These departments include: Risk management, quality management, human resources, nursing, registration, physicians, pharmacy, lab, dietary, radiology, rehab, emergency department, other patient care staff, finance, information services, public relations, and marketing.

### **Course Objectives:**

#### **Upon completion of this training the learner will be able to:**

1. State what is HIPAA and what does it govern.
2. Explain who (entities) is covered by HIPAA privacy rule.
3. List examples of (confidential) ***protected health information*** (PHI).
4. Identify who is authorized to see PHI.
5. State what is compliance date for the HIPAA privacy rule.
6. State who is the Privacy Officer.
7. List four responsibilities of the hospital to ensure patient privacy.
8. State four rights guaranteed to patients by the HIPAA Privacy rule and regulations.
9. What are the penalties that can be imposed for violating HIPAA.
10. Discuss disclosure purposes that require authorization from the patient.
11. Discuss disclosure purposes that do not require authorization from the patient.
12. Describe patient health information that can be disclosed.
13. Given a scenario discuss the healthcare provider's role in protecting patient's privacy under HIPAA.
14. State four examples of things you can do to ensure security of patient data.

# ***Introduction***

## ***HIPAA Confidentiality and Privacy***

As employees of Mercy Hospital we promise to give patients the highest quality health care, and patients expect that we keep information about their health confidential, sharing it only with people who need the information to do their jobs. Confidentiality and patient privacy has been part of our **Code of Conduct, Standards of Behavior, State laws, and JCAHO standards for patient care.** Under a new national law it will be illegal to violate this code. The ***Health Insurance Portability and Accountability Act*** or **HIPAA** for short, includes punishments for anyone caught violating patient privacy. Under HIPAA, the hope is that educated patients will be able to trust their providers and the organization in which they work. To build trust, HIPAA calls on health care workers and others with access to patient information (***covered entities***) to learn the rules for privacy and confidentiality and then live by them.

**Confidentiality and privacy means** that patients have the right to control who will see their protected, identifiable health information. This means that communication with or about patients involving patient health information will be private and limited to those who need the information to provide treatment, payment, or healthcare operations. Such communications may involve verbal discussion, written communication, or electronic communications. Only those people and computer processors with an authorized need to know will have access to protected information.

Hospitals and healthcare organizations have always upheld strict privacy and confidentiality policies. Now with the passing of HIPAA a patient's right to have his or her health information kept private and secure/confidential became more than just an ethical obligation of physician's and hospital, it is now a law.

The U.S. government has begun to strengthen the laws protecting privacy and confidentiality in response to situations in which private medical information has ended up in the wrong hands. For example, in various states employers have fired good employees shortly after the company learned the employee tested positive for genetic illnesses that could lead to lost work time and increased insurance costs. Individual's health information has been used against them in divorce and custody proceedings, political elections, loan applications, and various other ways. Cases of misuse of health information have caused lawsuits. As the number of cases of health information being misused rises, Congress has taken action to ensure hospitals and healthcare providers protect health information privacy and confidentiality.

### **Overview: What is HIPAA?**

The Health Insurance Portability and Accountability Act of 1996 is a multifaceted piece of legislation that covered these three areas: 1) Insurance portability, 2) Fraud enforcement (accountability) and 3) Administrative Simplification (reduction in health care costs).

HIPAA was enacted to improve the efficiency and efficacy of the healthcare system. The first two components of HIPAA are already in effect, ***portability*** and ***accountability***.

**Portability** ensures that individuals moving from one health plan to another will have the continuity of coverage and will not be denied coverage under pre-existing clauses.

**Accountability** significantly increases the federal government's fraud enforcement authority in many different areas.

**Title I of HIPAA** protects health insurance coverage for workers and their families when they change or lose their jobs.

**Title II of HIPAA, the Administrative Simplification Provisions** of the act require the Department of Health and Human Services to establish:

- National standards for electronic health care transactions
- National identifiers for providers, health plans and employers and
- The security and privacy of “individually identifiable health information” past present or future.

The third component **Administrative Simplification**, is arguably the most significant part of the legislation and will be the focus of this course. Since the implementation date was later than the previous two components, Administrative Simplification requirements received little attention. But today, two of the rules, privacy (which is finalized) and security (which was recently finalized), are generating much discussion and debate in the healthcare community. Concern centers around the administrative, technical, and policy changes that the rules required healthcare organization to make in order to protect their patient’s privacy and confidentiality of patient health information (PHI).

The **Administrative Simplification** portion, specifically privacy and confidentiality will be the focus of this course. This portion of HIPAA deals in areas of: **Privacy, Security, Transaction standards**. This rule set national standards for the protection of health information, as applied to **three types of entities: health plans, health care clearing houses, and health care providers** who conduct certain health care transactions electronically.

**The three major purposes for the privacy rules are:**

- Protect patients’ right by giving them access to their health information and control over making sure the records were used appropriately.
- Improve the quality of care by restoring trust in the health care system.
- Improve the efficiency and effectiveness of the way health care is delivered by creating a framework for privacy that build on efforts by states and health systems.

The new changes to **HIPAA will become effective Monday, April 14, 2003**. Once the law is in effect it will be illegal to violate this code. Under the **privacy rule**, finalized during August 2002, healthcare organizations across the country must train all employees in the basics of patient privacy and confidentiality by April 14, 2003. There are significant criminal and civil penalties and liability risks for noncompliance. This applies to all staff members, nurses, physicians, volunteers, and some contract workers at health care facilities. All must become aware of their role in protecting privacy of all patients. The Office for Civil Rights, in the Department of Health and Human Service (HHS), has been charged with enforcing the HIPAA privacy rule.

There are several provisions under HIPAA such as electronic signature, security, transaction, and standard code set, unique identifiers, and information shared between health plans. The **transaction standards and standard code sets** were the first ones to become final. The privacy rules was the second, and most recently, the **security** standard, finalized February 2003, will become effective in 2005. The **electronic signature standards** will also have a great impact on healthcare workers.

## **Who is covered by the privacy rule?**

All healthcare organizations and providers including: hospitals, physician offices, health plans, employers, public health authorities, life insurers, clearing houses, billing agencies, information systems vendors, service organizations, universities. These are known as **covered entities** for HIPAA’s privacy and security regulations and covered entities must comply with its regulations.

Covered entities, such as the hospital must implement standards to protect and guard against the misuse of individually identifiable health information. Failure to timely implement these standards may, under certain circumstances, trigger the imposition of civil or criminal penalties.

## Summary

The information provided will review the main points of the new regulation, identify **who must comply, what is covered, and discuss the legalities and their everyday applications in health care.** Strategies for compliance will also be discussed. HIPAA requires organization to have detailed policies and procedures in place that dictates how patient information is to be used, when it can be disclosed, and how it should be disposed of. Some of these policies are new and/or are being revised.

Mercy Hospital is committed to protecting patient privacy and confidentiality and expects all employees to adhere to the privacy and confidentiality policies. When you fail to protect patient information and patient records by not following the hospital's privacy policy, it can have an impact on your ability to do your job, your status with the organization, and your license to practice. Be sure to read and become familiar with these policies as they become available. **If you are unsure or have any questions, see your supervisor or consult with the hospital's privacy officer.**

Employees are encouraged to **report violations or suspected abuse** to the hospital's **privacy officer** (Marie Auguste ext. 2999). You may report violations anonymously, if you wish, and should not fear retaliation for reporting a privacy violation. It is considered part of your job to report instances where you suspect the privacy or confidentiality policies are being broken.

# *HIPAA: Confidentiality and Privacy Summary Sheet*

The **HIPAA privacy rule guarantees patients access to their medical records, gives them more control** over how their **protected health information** is used and **disclosed**, and **provides recourse** if their medical privacy is compromised. The rule also protects the confidentiality of medical records. Health care providers need to understand their responsibilities and rights under the federal privacy regulation to implement new policies and procedures without interfering with access to quality care.

This guide summarizes the HIPAA privacy rule, its implication, and steps to take to ensure compliance.

## .. **The HIPAA Privacy Rule**

The privacy rule creates national standards to protect individuals' medical records and other personal health information. The rule:

- Gives patients more control over their health information.
- Sets boundaries on the use and release of health records.
- Establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- Holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- Takes into account public responsibility to disclose some forms of data to protect public health

## .. **Who Is Covered By the Privacy Rule?**

Providers who conduct electronic transactions, health plans and clearinghouses are covered. If business associates receive or create **protected health information** to perform some function for a hospital, contracts must declare that those business associates will use the information only for the purposes that they were hired to perform, will safeguard the information from misuse and will help the covered entity comply with its HIPAA obligations. They are prohibited from using information in any way that would violate HIPAA.

## .. **Protected Health Information (PHI)**

- HIPAA protections extend to any identifiable information related to the "past, present or future physical or mental health condition" of a person
- In any form or medium
- Only adequately "de-identified information" is exempt:
- Information that contains no direct identifiers
- It would be virtually impossible to identify from the indirect one that remain

**Examples of protected health information** include: zip codes, telephone numbers, fax numbers, e-mail addresses, pictures, dates of service, patient history, discharge summary, phone notes, inpatient progress notes, outpatients progress notes, census and allergies. The **Minimum Necessary Standard** states that when using or disclosing protected health information or when requesting protected health information from another covered

entity, the provider must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. **“Incidental disclosures”** are not a violation of the privacy rule.

.. **Who is authorized to see protected health information?**

**Healthcare providers** who are directly involved in providing **treatment, payment, or involved with health operations** (TPO) are authorized to see access patient information.

.. **Compliance Date for HIPAA Privacy Rule**

The compliance date is **April 14, 2003**. An additional year is allowed for completion of existing contracts that have not expired by the compliance date. New or renewed contracts with business associates must incorporate the requirements into the contracts. HHS expects to issue an enforcement rule soon. The Office for Civil Rights is the enforcement authority.

.. **What is Required of Providers (the hospital) to ensure privacy of patients?**

- **Provide information to patients** about their **privacy rights** and how their information may be used.
- Adopt **clear, enforceable privacy procedures**.
- **Train employees** to understand the privacy procedures.
- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed.
  - This individual is known as the **Privacy Officer: Marie Auguste, RN, MBA**. She is also the Corporate Compliance Officer at Mercy Hospital and can be reached at ext. 2999.
- **Secure patient records** containing individually identifiable health information so that they are not readily available to those who do not need them.
- Comply with the **minimum necessary** information requirements.

.. **Provider (Hospital’s) Responsibilities**

- Ensure that patient information is not disclosed improperly.
- Allow patients access to examine their records.
- Allow patients to suggest changes to those records.
- Educate patients on privacy policies (how their data will be used).
- Give patients the right to revoke permission to use data.
- Notify patients of anyone who has seen their records.
- Provide a formal complaint process for patients.
- Allow patients to determine where communications are sent.
- Mitigate damage from inappropriate uses or disclosure.
- Respond within reasonable time and costs to patient requests.
- Maintain a permanent copy of the record (required by law) and appropriately manage it.

## ◆ HIPAA Rights Guaranteed to Patients

HIPAA provides rights to patients for their protected health information:

- **"access"** - to see, get copy of one's records
- **"amendment"** - to request corrections, statement of disagreement when errors are found
- **"accounting"** - of uses and disclosures of protected health information (patient may request a list of (some of) the entities to which/whom one's records has been disclosed)
- for especially sensitive information, can request extra protections and/or confidential communications
- to complain about, get resolution of, privacy problems

## •• Provider Rights

- Use patient information for treatment, payment, and health care operations.
- Disclose information for treatment, payment and operations by other covered entities.
- Withhold part of the record if disclosure would result in patient harm.
- Disclose information to family members or other patient representatives, if patients cannot speak for themselves.

## •• Fines and Penalties for Violating HIPAA Standards

Civil and criminal penalties for noncompliance include fines up to \$250,000 and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.

### HIPAA Sanctions

- **Civil**  
\$100 each violation, up to \$25,000/person/year  
liability of knew, or reasonably should have known, and attempted cur
- **Criminal**
  - "knowing" - up to \$50,000, 1 year in prison
  - "under false pretenses" - \$100,00, 5 years in prison
  - with "malice" or intent for "personal or commercial gain" - \$250,000, 10 years in prison

### Other Sanctions

- Institutional reputation – loss of business, profits
- Employee suspension or termination
- Loss of license to practice
- Civil fines
- Criminal fines and imprisonment

## Authorization for Use or Disclosure of Protected Health Information (PHI)

Authorization is not required for use or disclosure of PHI for treatment, payment and health care operations (TPO).

### .. Individual authorization required from patient for:

- Marketing and fund-raising.
- Research-related treatment (unless waived by an institutional review board).
- Psychotherapy notes.
- Employment determinations.
- State laws impact that may provide authorization for an individual.

### .. Disclosures Not Requiring Authorization from Patient

These disclosures can occur without patient permission:

- Required by law: **public health** (reporting of diseases and conditions, suspicious deaths)
- Health oversight
- Medical devices reporting for injuries, breakdown or malfunction
- To report child abuse, neglect, domestic violence
- For law enforcement investigations
- For judicial or administrative proceedings
- To avert a serious, immediate threat to public safety
- For national security purposes
- Research (IRB approved)
- Decedents
- Worker's compensation
- Specialized governmental functions

### .. Ways to Safeguard Protected Health Information (PHI)

Reasonable efforts for implementation of administrative, technical and physical safeguards are required:

- Verbal conversations precautions: Close doors when discussing treatments and administering procedures.
- Close curtains and speak softly in semi-private rooms when discussing treatments and administering procedures.
- Avoid discussion about patients in public areas such as elevators and cafeteria lines.
- Do not leave messaged on answering machine regarding patient conditions or test results.
- Avoid paging patients using information that could reveal their health problems.
- Secure storage and transportation of patient information.
- Display precautions (e.g., computer screens displayed away from public access)
- Posted or written patient information i.e., whiteboards kept away from public access areas).
- Log off computers when away from workstation.
- Telephone and facsimile precautions: When given patient information regarding condition on the phone limit responses to basic responses *stable* or *critical*.

- Verify the doctor is working on the patient's case; send to a registered fax number on record with the hospital. Send fax only when someone is there to receive it- do not leave in the fax machine for long periods of time.
- Shredding and disposal of PHI. PHI should be placed in closed receptacles, burned, or shredded- never leave in open garbage bins.
- Records are kept locked, only people with a need to see information about patients have access to them.

## ***HIPAA Terminology***

### **HIPAA**

Health Insurance and Portability Act of 1996.

- HIPAA has two main goals:
  - making health insurance more portable when persons change employers
  - making the health system more accountable - especially reducing waste and fraud

### **Administrative Simplification**

- Provision promoting efficiency in the health care system particularly by more use of computers
- Four “rules” that set standards for collection, use and disclosure of health information:
  - Transactions and Code Sets Rule
  - Identifier Rule (unique Ids for providers, plans, employers and maybe, patients)
  - Security Rule (for electronic health information)
  - Privacy Rule (for all health information)

### **Covered Entities**

**HIPAA protections for pm put obligations on almost every organization that provides or pay for health care in the US:**

- health plans (health insurers, HMOs, etc.)
- health care providers (that use electronic transactions)
- health information clearinghouses (businesses that specialize in health data processing)

### **HIPAA Obligations**

Covered entities must have appropriate privacy and security policies, which include:

- role-based rules on information use
- training and sanctions to ensure that workforce practices follow policies

### **Workforce Education**

- obligations for a covered entity actually fall on its “workforce” - includes every employee, and every volunteer
- Every member of covered entity's workforce must be educated – “as necessary and appropriate” to do his/her job

## **Business Associates**

Companies that handle health information on a covered entity's behalf are also reached by HIPAA:

- covered entities must enter into contracts with all business associates
- limited obligation for covered entities to monitor business associates' practices

## **State Preemption**

**State laws that provide "more stringent" privacy protections remain in force:**

- HIPAA provides a floor of protections for everyone
- State laws that are "more stringent" are not preempted by HIPAA
- State laws relating to public health and health system oversight also remain in force

## **Notice of Privacy Practices**

Every patient will receive a Notice from his or her "direct treatment providers" informing him or her of

- Access, correction, accounting, special protections and communications, and complaint processes
- The covered entity's obligations for
  - Appropriate privacy and security policies
  - Workforce training in those policies
  - Business associate monitoring

## **Acknowledgement of Notice**

"direct treatment providers" must make an effort to get written acknowledgment of receipt of the notice from each patient:

- The notice must also be posted in a facility, and copies must be available
- Acknowledgement process provides an opportunity for patients to discuss privacy issues with providers
- **Health plans must also issue such notices periodically**

## **Treatment, Payment, Healthcare Operations (TPO)**

Acknowledgement constitutes permission for a broad range of "routine" transactions:

- for any and all treatment needs
- to secure payment for that treatment
- for a very long list of other "health care operations"

**"Consent" is not required from patient for TPO**

## **Authorization**

- Patients must sign a written authorizations for non-routine uses beyond TPO
  - Certain kinds of fundraising, research, marketing
- Authorizations specify who is receiving protected information, for what purpose, and for how long
- Stricter state laws may impose additional authorization (or consent) requirements

### **Agree or Object**

- For a few kinds of routine practices, only an opportunity for oral agreement (or objection) is required:
  - including patient's name and condition in a facility's "directory information"
  - discussions of patient's condition with immediate family members

### **No opportunity to agree or object**

- A large number of disclosures can occur without patient permission, just as now:
  - For public health (reporting of diseases and conditions)
  - To report child abuse, neglect, domestic violence
  - For law enforcement investigations
  - For judicial or administrative proceedings
  - To avert a serious, immediate threat to public safety
  - For national security purposes

### **Minimum Necessary**

- Use and disclosure of patient's protected health information should be no more than necessary to get the job done:
  - The regulations acknowledge that "incidental; uses and disclosures" inevitably happen
  - All that is required is "reasonable" effort by health care workforce to achieve minimum necessary

### **Reasonable, appropriate security**

- Attention to technical, physical and administrative measures:
  - Computer and communications protections, door locks and alarms, policies about information use
  - Protections need only be "reasonable" for the circumstances, given costs and current technology
  - Protections must also be appropriate to the kind and amount of information being protected

### **Complaints of Violations**

- Any patient may complain to the institution's "privacy officer" or to the US Department of Health and Human Services (DHHS) Office of Civil Rights
  - Institutions must respond promptly and take appropriate action as needed
- Workforce members may complain to privacy officer or DHHS:
  - With reasonable good faith belief, and disclosing no more than necessary
  - No intimidating, retaliatory acts by covered entity

# Privacy, Confidentiality, Data Security, and HIPAA Dilemmas

## How would you handle these situations?

1. A family member calls and inquires about the condition of a relative. What do you do?
2. You are a healthcare provider caring for Mrs. Jones, a patient at Mercy Hospital. Dr. Max, a physician at Mercy Hospital asks you to see Mrs. Jones' chart. He is not her physician but her next-door neighbor and is concerned about her health. What do you do?
3. Big Daddy is a well-known entertainer and is a patient in the hospital for a few days before he dies of injuries sustained in an auto accident. All of your friends are begging you to find out more information about what happened to Big Daddy. Your position gives you access to patient's records in the hospital and it would be easy to find out everything everyone is curious about. Your friends tell you Big Daddy won't know or care, plus information will come out in the press in a few days any way. What should you do?
4. You attended a meeting to evaluate certain patients and their medical progress. A list of each patient's name, patient number, and diagnosis is given to everyone at the table for purposes of discussion. At the end of the hour everyone leaves but you notice that several copies of the patient list are still on the table. What do you do?
5. A nurse enters an order and refers to patient information in the computerized patient record and then leaves the computer terminal without logging off properly. You are working in the area and notice that the computer is on, but you assume the nurse is coming back in a minute. Meanwhile a patient wandering the hallway goes to the computer to review his friends' patient records. Who is responsible for the patient's lost privacy?
6. A student nurse arrive on your unit to review a patient's chart prior to his/her clinical rotation begins the next day. Would it be appropriate to allow access to the patient's medical record?
7. Dr. Anderson is discussing a patient's care with the nurse outside the patient's door. Another patient wondering the hall overhears the conversation. Dr. Anderson later discussed the case in the elevator with dr. Smith. Everyone in the elevator hears the conversation. Has Dr. Anderson violated the privacy regulation?
8. You work in the hospital and notice some papers in a box that is to go in the shredding machine. Since Mercy has an Environmental Stewardship program, you decide to take it home to use for coloring paper for the kids and printer paper for the family computer. Is this the proper thing to do?
9. You work in a clinical lab. Dr. Brian's office calls to check lab results for a patient and is told the results would be ready late evening. Dr. Brian's office representative tells you to fax the information to them whenever it is ready and gives you the fax number. You have never dealt with Dr. Brian's office before. Should you send the fax?

10. You work in the hospital and decide to download some patient information so you can do some catch up work at home on your p.c. Is this O.K.?
11. A patient calls medical records and requests for a note in his medical record to be corrected. Who makes the decision on this issue?
12. A patient requests a copy of his health information access log, stating it is his right to have an accounting of all disclosures. Is he/she correct?
13. Mr. Smith writes Mercy Hospital requesting a copy of his wife's medical record. Mr. Smith does not include a written authorization from his wife. Are we obligated to supply the information?
14. A local sheriff or police department calls Mercy Hospital requesting information on a specific patient (e.g. address information). Can you give them this information?
15. A reviewer from XYZ Home Health Agency with proper ID comes to your floor and picks up a patient's medical record to review. Is this the appropriate process?
16. The infection control nurse wants to report all tuberculosis cases diagnosed in the hospital to the State Public Health Department. Is this permissible?
17. A man comes to your department and tells you he is here to work on the computer. He wants your password to log onto the computer. What should you do?

## Post Test

1. The issue of portability deals with protecting healthcare coverage or employees who change jobs and allowing them to carry their existing plan with them to new jobs.
  - a) True
  - b) False
2. The privacy and data security portions of the HIPAA go into effect:  
**Monday, April 14, 2003**
3. The proliferation of computers in medicine has
  - a. Slowed down procedures
  - b. Created new dangers for breaches of confidentiality
  - c. Made it harder to access records
  - d. Automatically made breaches of confidentiality less likely
4. The set of rules that provide administrative simplification by standardizing the codes and format used for exchange of medical data is referred to
  - a) CPT
  - b) Written notice
  - c) ICDM-10
  - d) Electronic transaction standard
5. In general, information about a patient can be shared
  - a) When it is directly related to treatment
  - b) Only when it is not related to treatment
  - c) Only when the patient authorizes it specifically
  - d) Only with other medical personnel
6. Data security issues that must be addressed by HIPAA implementation teams include:
  - a) Data backup
  - b) Access control
  - c) Internal audits
  - d) All of the above
7. The single most important key to administrative simplification is standardizing throughout the healthcare system a set of transactions standards and code sets.
  - a) True
  - b) False
8. One good rule to prevent unauthorized access to computer data is to:
  - a) Never access medical data with a computer
  - b) Always leave the computer on when you go away
  - c) Make sure screens are visible to passers-by
  - d) Black the screen or turn off the computer when you leave it
9. You can reveal information needed for medical research if :
  - a) A physician requests it
  - b) Your supervisor request it
  - c) The patient authorizes it
  - d) You feel it is in the best interest of science
10. The general privacy rule now is that patients must be notified of the institution's privacy policies, and healthcare workers must always obtain a written acknowledgement of this.
  - a) True
  - b) False

11. In a hospital, the obligation to maintain confidentiality applies to:
  - a) Medical information only
  - b) Personal information only
  - c) All medical and personal information
  - d) Patients with HIV only
  
12. If you are sending patient information via e-mail, security is best maintained with:
  - a) Password protection at both ends
  - b) Encryption if it goes over the Internet
  - c) Destroying any printouts or placing them in the patient's medical chart
  - d) All of the above
  
13. One exception to confidentiality is \_\_\_\_\_.
  - a) A gunshot wound
  - b) When any doctor asks you for information, for any purpose
  - c) A minor who is pregnant
  - d) A celebrity who is already well known to the public
  
14. HIPAA overrides all state laws that define and regulate patient privacy.
  - a) True
  - b) False
  
15. Anyone caught selling private health care information can be fined up to \_\_\_\_\_ and sentenced to up to \_\_\_\_\_ in prison.
  - a) \$500,000; 15 years
  - b) \$25,000; 5 years
  - c) \$100,000; 10 years
  - d) \$250,000; 10 years
  
16. Facilities will no longer be able to post \_\_\_\_\_ anywhere where visitors might see them. This includes door tags and whiteboards at the nurses' station that are in public view.
  - a) Patient's full names
  - b) Shift start and end times
  - c) Patient's room numbers
  - d) Patient's ID numbers
  
17. There must now be a system in place to record the name of every person who views a patient's record.
  - a) True
  - b) False
  
18. Which organization has been charged with enforcing HIPAA's Privacy Regulation?
  - a) JCAHO
  - b) The Office for Civil Rights
  - c) The Health Financing Administration
  - d) FBI
  
19. When is the patient's authorization to release information required?
  - a) In most cases, when patient information is going to be shared with anyone for reasons other than treatment, payment of healthcare operations
  - b) Upon admission to a hospital
  - c) When information is to be shared among two or more clinicians
  - d) When patient information is used for billing a private insurer
  
20. If you suspect someone is violating the organizations' privacy policy, you should
  - a) confront the individual involved and remind him or her of the rules
  - b) watch the individual involved until you have gathered evidence against him or her
  - c) report your suspicions to the organization's privacy or complaint officer, as outlined in the hospital's policy

21. Under HIPAA, what is an example of a “healthcare operation”?
- a) Some fundraising activities
  - b) Medical record reviews
  - c) Billing
  - d) Accreditation surveys
22. If you are working elsewhere in the hospital when you hear that a neighbor has just arrived in the ER for treatment after a car crash. You should
- a) contact the neighbor's spouse to alert him or her about the accident
  - b) do nothing and pretend you don't know about it
  - c) tell the charge nurse in the ER that you know how to reach the patient's spouse and offer the information if it's needed

## **Answers to *Privacy, Confidentiality, DataSecurity, and HIPAA Dilemmas***

1. Respond with basic acknowledgements by stating the patient is in stable or critical condition.
2. Politely tell him "I'm sorry that information is confidential and cannot be shared."
3. Tell them the information is confidential and we cannot share with individuals not involved in the patient's case. Disclosing that information could cost you your job, open the hospital to liability, sanction, and fines.
4. Destroy/dispose of the papers in the appropriate manner, and remind your co-workers who attended the meeting that they are dealing with protected confidential information and everyone has to be extremely careful so that patient information is not left unsecured or accessible to others.
5. The nurse and the employee observing the situation, and ultimately the Hospital. These situations should be reported to the department manager.
6. Yes, after verifying the student's identity from their student picture I.D. They may view the medical record, take notes for school assignments (care plan, etc.) as long as there is no individual identifiable patient information with these notes. They may not under any circumstances make a copy of any portion of the chart.
7. Yes. Discussing patients and disclosing protected health information in an open area where others can easily hear is a violation of patient's privacy rights.
8. Any documents that contain patient information should not be removed from the hospital- unless authorized to do so. All private and confidential information should be destroyed appropriately.
9. Verify that the doctor is working on the patient's case; see that his office has a registered fax number on record with the hospital. Both are needed to send a fax. Also faxes should be sent when someone is there to receive it- it should not be left to stay in the fax machine for long periods of time.
10. Any documents that contain patient information should not be removed from the hospital- unless authorized to do so.
11. The Privacy Officer is the only individual authorized to make this decision.
12. Mercy Hospital does not have to provide a complete listing of every employee who uses the information for performance of their official duties i.e., routine uses for treatment, payment, and health care operations. The patient must submit their request in writing. The request should be referred to Mercy's Privacy Officer.
13. The hospital cannot provide the spouse a copy of the medical record without written authorization from the patient (except in rare circumstances). All exceptions must be approved by Mercy's Privacy Officer.
14. The sheriff/police office should be referred to the Privacy Officer. The hospital may disclose limited individually identifiable information to a law enforcement agency for the purpose of locating criminals in response to a written request from the law enforcement agency.
15. No, the reviewer must present a "pass" obtained in Case Management identifying the name of the patient they are to review. The reviewer must ask the unit secretary for the patient's chart.
16. Yes, State law requires the reporting of communicable diseases- this is considered a beneficial disclosure.
17. Do not give or share your password with anyone. You should also know the identify of anyone coming into your area. Ask questions and follow up with appropriate department to determine if the person is authorized to be in your area.