

HIPAA Privacy Self-Study, Test, and Answer Sheet

This self-study packet serves as a review of important Health Insurance Portability and Accountability Act (HIPAA) requirements.

Please read these materials and take the post test that follows. You will need to return the quiz, as instructed on the answer sheet, after you have completed it. If you have read these materials, you should have no trouble completing the quiz.

The objective of the HIPAA training is as follows:

- To heighten your awareness of and commitment to HIPAA regulations
- To reinforce the role you play in creating and maintaining organizational integrity, ethics, and compliance
- To renew your working understanding of HIPAA requirements

Reporting Concerns

There will be no retribution for asking questions, raising concerns about the Code of Conduct, or for reporting possible improper conduct that is done in good faith. Any colleague who deliberately makes a false accusation with the purpose of harming or retaliating against another colleague will be subject to reprimand and/or termination.

We encourage the resolution of issues at the local level whenever possible. To obtain guidance on an ethics or compliance issue or to report a potential violation, you may choose from several options:

- Consult your Staffing Manager
- Consult your Office Manager
- Consult your company's Ethics Coordinator

Any one of these options is an easy and anonymous way to report possible violations or obtain guidance on an ethics or compliance issue. You are encouraged to use these options anytime. In order to properly investigate reports, it is important to provide enough information about your concern.

Information Security

ID's and Passwords

Patient Financial Information, Clinical Information, and User Passwords are all examples of confidential information. A User ID without a password is not confidential and is frequently included in directories and other tools widely available. The person granting access to a system or application typically assigns a User ID to the end user, and the User ID is sometimes used for identification, tracking, and other maintenance procedures.

If you have access to information systems, please keep in mind that your password acts as an individual key to the facilities network, critical patient care and business applications, and it must be kept confidential.

It is Worldwide Travel Staffing, Ltd.'s policy and procedure for each employee to learn about and practice the many ways that one can help protect the confidentiality, integrity, and availability of electronic information assets.

Confidential Information

A patient's diagnosis, the facility's marketing strategy, and computer network configurations are all considered confidential information. Individuals with access to confidential information will not discuss or disclose any confidential information even after assignment, shift, or contract is completed and/or employee termination.

No Worldwide Travel Staffing, Limited colleague or healthcare partner has a right to any patient information other than that necessary to perform his or her job.

Although you may use confidential information to perform your function, it must not be shared with others unless the individuals have the need to know this information and have agreed to maintain the confidentiality of the information.

Patient or Confidential information should not be sent via email. If it is necessary to send Patient information to a business associate outside of the assigned facility, arrangements other than email must be made.

HIPAA Privacy Self-Study, Test, and Answer Sheet

Privacy

HIPAA and its implementing regulations set forth a number of requirements regarding ensuring the privacy of protected health information (PHI).

HIPAA requires healthcare entities to appoint a facility privacy official (FPO). The FPO in a facility oversees and implements the Privacy Program and works to ensure the facility's compliance with the requirements of the HIPAA Standards for Privacy of Individually Identifiable Health Information. The FPO is also responsible for receiving complaints about matters of patient privacy. Worldwide Travel Staffing, Ltd. recommends each employee assigned to any/all facilities become familiar with the facility's designated FPO.

HIPAA regulations contain a number of restrictions on the transmission of PHI; however, they do not prevent faxing or mailing health information as long as certain precautions are taken. The regulations mandate that health information not be sold by a facility.

The Notice of Privacy Practices must be made available to all patients, posted on the facility's Internet site (unless the facility does not have a site, and the consent form language must refer to the notice. Patients do need to sign an acknowledgement form confirming receipt of the notice.

Patients have the right to access any health information that has been used to make decisions about their healthcare at any facility. They can also access billing information. They may review the paper chart (supervised) or be provided a hard copy.

A patient may have access to all the records in the designated record set. This record set includes any information that is maintained, collected, used, or disseminated by a facility to make decisions about individuals. The paper record is the legal medical record, and a copy should be provided upon request (electronic access is not appropriate). A patient may be denied access under certain circumstances (e.g., when a person may cause harm to him or herself or others, or when protected by peer review). The designated facility FPO has more information on the right to access.

A patient may add an amendment to any accessible record for as long as the record is maintained by a facility. The request for amendment should be made in writing to the facility. The designated facility FPO should have any/all necessary information regarding the right to amend.

While patients have a right to amend their record, that does not mean that health information can be deleted from the record. The patient may submit an addendum correcting or offering commentary on the record, but no information may be deleted from the record.

Everyone is responsible for protecting patients' individually identifiable health information. Any piece of paper that has individually identifiable health information on it must be disposed of in appropriate receptacles. The paper must be handled and destroyed securely. The elements that make information individually identifiable include: name, zip or other geographic codes, birth date, admission date, discharge date, date of death, email address, social security number, medical record/account number, health plan ID, license number, vehicle identification number, and any other unique number or image.

HIPAA privacy regulations do not prevent facilities from storing the medical record at the patient's bedside. However, the facilities must implement reasonable safeguards to protect an individual's privacy. For example, possible safeguards may include limiting access to the area by non-employees or placing patient charts in holders with the identifying information facing the wall.

Any member of the workforce with a legitimate need to know to perform their job responsibilities may access a patient's health information. However, the amount of information accessed should be limited to the minimum amount necessary to perform their job responsibilities.

The hospital information desk or volunteers should have a directory or listing of patients containing only patient name, room/location and condition in general terms. Patient diagnosis or procedures should not be released. Also, this information may not be released about confidential patients or patients who ask not to be listed in the directory nor have their whereabouts known.

List of patients may be provided to clergy. The lists should consist of the patient name, room/location, and may include the condition in general terms. The list should be restricted by religion, and not include confidential patients; confidential information such as social security numbers should not be included. If any questions or concerns regarding release of list to clergy, please seek out facility FPO.

HIPAA Privacy Self-Study, Test, and Answer Sheet

1. What is an FPO?
 - a. Facility Privacy Official
 - b. Facility Police Officer
2. Confidential Information includes all of the following except:
 - a. Patient Financial Information
 - b. User ID
 - c. Passwords
 - d. Clinical Information
3. Individual identifiable health information may NOT be:
 - a. Faxed
 - b. Mailed
 - c. Sold
4. Which of the following can you disclose after your assignment, shift, or contract is completed and/or relationship with Worldwide Travel Staffing, Ltd. ends?
 - a. Your salary
 - b. A Patient's Diagnosis
 - c. The Company's Marketing Strategy
 - d. Computer Network Configurations
5. Who is responsible for protecting patients' individually identifiable health information?
 - a. CEO
 - b. ECO
 - c. Physician
 - d. All of the above
 - e. None of the above
6. It would be appropriate to release patient information to:
 - a. The patient's (non-attending) physician brother
 - b. The transferring hospital's personnel checking on the patient
 - c. The respiratory therapy personnel doing an ordered procedure
 - d. A retired physician who is a friend of the family
7. True or False: If a person has the ability to access facility or Company systems or applications, they have the right to view any information contained in that system or application?
8. True or False: Patient information may be attached within a company email sent via the Internet to a business associate to resolve questions related to a patient's account.
9. A patient listing given to a member of the clergy should be restricted by religion and may have the following information except:
 - a. Patient name
 - b. Patient social security number
 - c. Patient location
 - d. Patient condition in general terms
10. Which of the following is the appropriate person with whom to share patient information even if the patient has NOT specifically authorized the release of information to the individual?
 - a. A former physician of the patient who is concerned about the patient
 - b. A colleague who needs information about the patient to provide proper care
 - c. A friend of the patient
 - d. A pharmaceutical salesman who is offering a fee for a list of patients to whom he could send a free sample of his product

HIPAA Privacy Self-Study, Test, and Answer Sheet

11. The acronym for HIPAA stands for:
 - a. Health Information Protection and Accountability Act
 - b. Health Insurance Portability and Accountability Act
 - c. Health Information Publication and Accumulation Act
 - d. None of the above
12. Confidential information must not be shared with another unless the recipient has:
 - a. An OK from a doctor
 - b. The need to know
 - c. Permission from Human Resources
 - d. All of the above
13. True or False: HIPAA privacy regulations prevent facilities from storing the medical record at the patient's bedside.
14. True or False: It is part of our jobs to learn and practice the many ways we can help protect the confidentiality, integrity, and availability of electronic information assets.
15. True or False: Patients have a right to access their health information.
16. What is the standard for accessing patient information?
 - a. A need to know for the performance of your job
 - b. If a physician asks you the diagnosis of the patient
 - c. Just because you are curious
 - d. You are a relative of the patient
17. If an employee has medical testing in a facility, the appropriate way for him or her to access the test result is:
 - a. Complete release form and receive a copy of results
 - b. Check the computer system for his or her results
 - c. Get a fellow employee to access the results while looking over his or her shoulder
 - d. Call a friend in the department where the test was done to get the results for the employee
18. True or False: Patient or confidential information may be sent through the Internet with guaranteed security.
19. Patient information is considered individually identifiable if which of the following elements are included:
 - a. Social security number
 - b. Name
 - c. Fingerprint
 - d. All of the above
20. True or False: Patients do not need to sign a form acknowledging receipt of the facility's Notice of Privacy Practices.
21. True or False: Only clinicians may access patient's health information.
22. Each facility must designate a person to oversee and implement the Privacy Program. Which of the following is the appropriate person?
 - a. A facility privacy official (FPO)
 - b. A HIPAA officer
 - c. An Ethics and Compliance officer
 - d. A mediator
23. A visitor who asks for a patient by name may receive the following information except:
 - a. Patient name
 - b. Patient condition in general terms (e.g. stable, critical, etc.)
 - c. Patient location
 - d. Patient diagnosis
24. True or False: Copies of patient information may be disposed of in any garbage can in the facility.

HIPAA Privacy Self-Study, Test, and Answer Sheet

Name: _____ Date: _____

Signature: _____ Score: _____

1. _____

13. _____

2. _____

14. _____

3. _____

15. _____

4. _____

16. _____

5. _____

17. _____

6. _____

18. _____

7. _____

19. _____

8. _____

20. _____

9. _____

21. _____

10. _____

22. _____

11. _____

23. _____

12. _____

24. _____