

# HIPAA Assessment

1. When you comply with HIPAA standards, what are you ensuring?
  - a. Patients have unlimited access and control over their health information.
  - b. Patients have legal rights regarding who can access and use their PHI.
  - c. Our organization has implemented the proper security controls required by law.
  - d. Our organization has the final say on who can access our patients and/or customers' PHI.
  
2. You attempt to log in to an unattended computer but notice one of your coworkers is still logged in with their credentials. What should you do?
  - a. Log out of the computer and log back in with your credentials.
  - b. Stay logged in as your coworker—you will only be using the computer for a minute.
  - c. Ask around to see if anyone else has used the computer.
  - d. Log out and report the situation to the Privacy Officer.
  
3. You are eating lunch in a public place with a coworker who begins to tell you details about a patient's condition. Is this permitted?
  - a. Yes, if you have an authorized need to know.
  - b. Yes, as long as she doesn't disclose the patient's name.
  - c. No, only your coworker and her patient are legally allowed to discuss the patient's condition.
  - d. No, even if you have an authorized need to know, you should never discuss PHI in a public place where others may hear.
  
4. You receive a medical file containing a patient name, address, e-mail address, injury report, and automobile VIN number. Which of the information is PHI?
  - a. The patient name
  - b. The patient name, address, and e-mail address
  - c. All of the information is PHI
  - d. None of the information is PHI
  
5. What's your responsibility in protecting PHI?
  - a. To know and follow our organization's HIPAA security and privacy policies and procedures for safeguarding PHI.
  - b. Limited, the person who gave me the PHI is responsible for its protection.
  - c. To know what it is and report violations as needed.
  - d. None, I don't ever work with PHI.
  
6. True or False: You are only liable for securing physical or electronic forms of PHI.
  - a. True—having conversations about PHI is just part of our business and requires no security controls.
  - b. False—reasonable safeguards need to be taken to secure all PHI, regardless of its form.

7. To what extent can you access, use or disclose PHI?
  - a. To the minimum degree necessary required for treatment, payment, and health care operations.
  - b. To the minimum degree necessary to ensure a profit for the organization.
  - c. To the extent necessary to fulfill authorizations allowed by the patient.
  - d. Generally, if you can access PHI, you can use it.
  
8. As you scan your badge to enter a restricted area, a coworker approaches you and asks you to hold the door. Should you let him follow you in?
  - a. Yes, as long as you are sure he works at our organization.
  - b. Yes, as long as he says he is authorized to enter the area.
  - c. Yes, as long as he has an employee badge.
  - d. No, all employees need to scan their badges to enter a restricted area.
  
9. You receive a patient complaint that their privacy has been violated. What should you do?
  - a. Try to resolve the situation.
  - b. Direct the complaint to the appropriate person in the organization (the Privacy Officer).
  - c. Determine if it is a valid complaint and then report it as necessary.
  - d. Nothing—complaints are a natural part of business operations.
  
10. A coworker asks you to provide him with PHI for one of his employees. He isn't authorized to access the information himself, but assures you he has no malicious intent. Should you do this?
  - a. Yes, because he is a coworker, he has a business need.
  - b. Yes, if he has no malicious intent, there's no harm in doing a favor.
  - c. No, you can't be sure he won't use this information illegally.
  - d. No, providing this information—regardless of intent—is against the law and could result in massive legal repercussions.

**Note: 80% correct is required to pass this assessment.**

Name (Please Print): \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Score: \_\_\_\_\_