PRIVACY & SECURITY SURVIVAL TRAINING: PROTECTING PATIENT PRIVACY
ASSESSMENT QUESTIONS

1. As a workforce member of this facility, you may access a patient's protected health information:

   a. whenever you want to do so
   b. if your co-worker or supervisor asks you to do so
   c. only if your job duties require you to do so
   d. in an emergency even if you're not authorized

2. It is your responsibility to immediately report any suspected privacy or security breach, such as any theft of computer equipment or unauthorized or inappropriate access, use, disclosure, or destruction of patient or confidential information:

   a. True
   b. False

3. Patient or confidential information should not be viewed, accessed, or disclosed without a need to know. Which of the following forms of confidential information would be protected under HIPAA?

   a. A paper-to-paper fax
   b. Verbal conversations
   c. Information written solely on paper
   d. All of the above

4. You only need to contact your facility Information Technology Help Desk to obtain authorization to e-mail PHI.

   a. True
   b. False

5. If you are only going to be away from your desk for a few minutes you do not need to lock or log off your workstation.

   a. True
   b. False

6. Jason's supervisor wants access to his computer when he is away from the office. The supervisor has a right to know his username and password.

   a. True
   b. False

7. DHS may log, review, or monitor any data you have created, stored, sent, or received using County Information Systems (e.g., computer, laptop, etc.).

   a. True
   b. False

8. What is the Notice of Privacy Practices (NPP)?

   a. It is a tool to enable patients to express their concerns about misuse of PHI
   b. It informs the patient of services the facility does not provide
   c. It is a tool that allows patients to select the type of information that they would like to have sent back to their provider
   d. It describes patient rights and the provider's responsibilities regarding PHI

9. Which of the following are authorized to release patient information when requested by a patient, law enforcement, etc.?

   a. Physicians
   b. Nursing staff
   c. Health Information Management staff
   d. Employee Health Services staff

10. A password on a portable storage device is sufficient to protect PHI in case of loss or theft of the device.

    a. True
    b. False

11. Which of the following disclosures of PHI is *not* a privacy breach and/or security breach?

    a. Mary has access to the patient information system and decides to check her health records to see what is in it
    b. Walter works in HIM and provided a patient's medical information to the United States Department of Health and Human Services
    c. Janice, a law enforcement officer, is friends with the hospital receptionist and asks her to look up her ex-husband's records to check which medicines were prescribed at his last visit
    d. All are allowable under HIPAA

12. Mary has been out sick. Her supervisor finds out from their Human Resources Return-to-Work Unit that Mary has cancer, and tells Mary's coworkers about it. It is okay for Mary's supervisor to let her coworkers know about Mary's cancer since the coworkers all care about her well-being.

    a. True
    b. False

13. You may be subject to fines and penalties under State and federal laws and/or disciplinary action if you fail to comply with patient privacy laws or County, DHS, or facility policies and procedures.

    a. True
    b. False

14. If the State determines you have violated the State privacy laws, they may report you to the appropriate licensing, registration, certification, or permit board/agency for possible disciplinary action.

    a. True
    b. False

15. A patient or individual can report a suspected privacy or security breach to the following entities:

    a. Supervisor
    b. Facility Privacy Coordinator or Information Security Coordinator
    c. County Fraud Hotline
    d. DHS Compliance Hotline
    e. Any of the above

16. There will be no retaliation against a workforce member who, in good faith, reports any actual or suspected privacy breaches or HIPAA violation

    a. True
    b. False

17. In addition to medical records, PHI may be found in written communications, electronic forms, verbal conversations, e-mails and memos, IV and medication labels, X-rays, monitors, EKGs, etc. and must be protected.

    a. True
    b. False

18. While working the 9pm – 6am shift at the hospital, you see some patient information in a trash can. What should you do?

    a. Remove it from the trash can, if safe to do so, and take it to the shredder bin.
    b. Remove it from the trash can, if safe to do so, or secure the trash can and immediately notify your supervisor.
    c. Immediately report it to the facility Chief Financial Officer
    d. Call the toll-free hotline and report it

19. An employee mistakenly receives a fax containing PHI from an outside healthcare agency. What should the employee do?

    a. Contact the person on the cover sheet
    b. Throw the FAX in the shredder bin
    c. Contact the facility Privacy Officer
    d. All of the above

20. When you have a patient's prior written permission to videotape them, it is permissible to use your own video camera.

    a. True
    b. False