Annual Privacy and Security CBL Test Questions 2016

1. An athlete of an OSU sports team has been hospitalized. You are not involved in providing care to the individual. You are permitted to access the patient's record because you are a Buckeye fan and you do not intend to share the information you obtain with anyone else.
   - A. True
   - B. False

2. Individual staff members can help prevent identity theft by:
   - A. Placing documents in collection bins for shredding.
   - B. Maintaining electronic security by encryption of computers and handheld devices.
   - C. Eliminating use of social security numbers wherever possible.
   - D. All of the above.

3. Angela has an unusual medical condition that requires costly medical intervention. Angela does not have health insurance, but her friend, Beth does. Angela "borrowed" Beth's identity. Each time Angela came in for services, she provided registration with Beth's name, date of birth, and social security number. Eventually, Beth called patient accounting to complain about paperwork she has received from her insurance company indicating she received services. Beth is complaining to OSUMC patient accounting that she did not receive these services. The representative from patient accounting should:
   - A. Ignore the call because Beth is probably lying.
   - B. Tell Beth there is nothing OSUMC can do to help.
   - C. Notify her manager who will notify the Privacy Officer who will engage the Identity Theft Red Flag Rule Response Team.
   - D. Tell Beth to wait and call us back if it happens again.

4. If an adult daughter accompanies her elderly father to his appointment and wishes to come into the treatment room with her father, the provider should:
   - A. Prohibit her from accompanying her father
   - B. Verify with the father that he is comfortable with having his daughter in the room, since the information discussed may be sensitive or embarrassing to him
   - C. Make the father sign a release form

5. In my job at Ohio State, I have a part in protecting the privacy and security of sensitive information.
   - A. True
   - B. False

6. In the course of doing your job, you learn that a coworker is currently hospitalized. Is it ok to talk about that worker with the others in your department?
   - A. Yes
   - B. No

7. It is OK to send email messages with sensitive information as an unencrypted attachment?
   - A. True
   - B. False

8. Janice works as a registrar in an outpatient clinic. She has received an email from an unknown individual who has offered her money if she provides the names, addresses, dates of birth, and social security numbers of some of her patients. She has been offered $10 for each data set she provides. Janice's husband has been recently laid off, and she would like the extra money. She decides to sell the patient information. Janice's coworker, Ken, notices that Janice is transcribing patient information on a work sheet each day, and placing the work sheet in her pocket book. Janice's co-worker Ken must:
   - A. Ignore the activity.
   - B. Notify his manager who will assess the situation and notify the Identity Theft Red Flag Rule Response Team via the Privacy Officer.
   - C. Ask Janice how he can help her get more information.
   - D. Write Janice a note asking her to stop what she is doing, but not notify the manager.

9. Misusing or failing to protect patient information, can result in corrective action up to and including termination.
   - A. True
   - B. False

10. My job does not involve direct patient contact at the Medical Center; but I still need to be attentive to the Identity Red Flag Rules.
   - A. True
   - B. False

11. Paper with sensitive information such as Protected Health Information should be discarded in the regular trash bin.
   - A. True
   - B. False

12. Protected Health Information includes the patient's Medical Record Number.
   - A. True
   - B. False

13. Saving a document containing PHI to "my documents" on my desktop computer is permitted.
   - A. True
   - B False

14. Terry is called away to another emergency while logged into the electronic medical record. Terry, in a hurry, does not log-off of the electronic medical record leaving it open for others to inappropriately access information under his username and password. What should Terry have done?
   - A. Terry did everything correctly because there was an emergency and he needed to respond fast. Logging-out would only slow him down.
   - B. It does not matter because Terry is not responsible for any activity that happens under his username and password when he is not performing the action.
   - C. Terry should have logged-off prior to leaving the electronic medical record open under his own username and password. Terry is responsible for all activity that occurs under his username and password in the electronic medical record.

15. Transmitting email containing Protected Health Information to a Hotmail or Yahoo! account is allowed by hospital policy and HIPAA.
    - A. True
    - B. False

16. When is it ok to share your passwords?
    - A. When it is your close friend or associate.
    - B. When it is an emergency.
    - C. When it is asked by a LAN administrator or Ohio State IT staff member.
    - D. Never.

17. Where is the best place to store documents with sensitive information?
    - A. On my unencrypted USB Key.
    - B. On a Secure Local Area Network.
    - C. On my desktop.
    - D. In the My Documents folder.

18. Which workstation security safeguards are YOU responsible for using and/or protecting?
    - A. User ID
    - B. Password
    - C. Log-off programs
    - D. Lock-up office or work area (doors, windows, laptop)
    - E. All of the above

19. Why is Security of information so important?
    - A. Proper security measures help keep patient information safe.
    - B. Proper security measures can protect against loss or theft of equipment.
    - C. Proper security measures can help protect against viruses, “hacks” and other attempts to harm our computer systems.
    - D. All of the above

20. You receive an e-mail with an attachment from an unknown source. The e-mail reads that your computer has been infected with a virus and you need to follow the directions and open the attachment to get rid of the virus. What should you do?
    - A. Follow the instructions ASAP to avoid the virus.
    - B. Open the e-mail attachment to see what it says.
    - C. Reply to the sender and say “take me off this list”
    - D. Delete the message from the unknown source.

21. Your co-worker has been absent from work for a couple of weeks. You care about your coworker. You have access to the Medical Center’s electronic medical record, so you decide to you it to see if you coworker has been hospitalized at OSU, and you discover that she has been. You decide to read her discharge summary and lab results, as you know, she wouldn’t mind. Have you violated hospital policy?
    - A. Yes
    - B. No

22. Select the true statements. Select all that apply.
    - A. HIPPA laws now impose greater penalties, including larger fine and potential litigation.
    - B. Employees who breach privacy are disciplined, up to and including termination.
    - C. Employees who breach privacy could be sued, lose their professional license, and be reported to the Office of Civil Rights.
    - D. Even if you do not work directly with patients, patient confidentiality should be taken seriously.

23. Select the option(s) that best answers the question. Select all that apply.
    - A. On your Facebook page
    - B. In a text or email message to people who know the patient.
    - C. With friends and relatives who have the patient's permission.
    - D. To staff who have a job-related need to know.

24. Select the option(s) that best answers the question. You took care of a patient. The patient was transferred to another provider in your unit. After you were no longer responsible for treating the patient, you looked up the patient's medical record to check on his progress. Is this a problem? Select all that apply.
    - A. No. You were involved in the patient's care at one time, therefore, you should be able to review the patient's chart after he leaves your area and he is no longer your patient.
    - B. No. You can access/view any patient's chart due to your employment at the university.
    - C. Yes, you no longer had a business need to review the patient's chart. You access/viewed the patient's chart because you were "curious" to know how the patient was doing. Curiosity is never a good reason to access/view a patient's chart.

25. You are a researcher and you receive a grant from an entity outside of the university to purchase a Mac computer to use with the research project. The data you store on the computer is a mixture of research data and data retrieved from the electronic medical record regarding the patient's care at OSUWMC. You do not encrypt the computer. Should the laptop be encrypted? Select all that apply.
    - A. No, because the laptop was not purchased by OSUWMC and is considered my "personal" computer.
    - B. Yes. Even if the laptop was purchased with funds from an entity outside of OSUWMC, if data stored on the laptop is generated from the medical records of patients from OSUWMC, the laptop should be encrypted
    - C. No. The laptop is utilized for research purposes, not for patient care purposed, therefore encryption is not necessary
    - D. Yes. Laptops containing patient information should be encrypted. If any data stored in the laptop contains information generated from the patient's medical chart, the laptop must be encrypted.