How to Keep Patient Data and Beaumont Information Safe and Secure Post Test

1. True or False
   I may use my clinical access to look at my own medical record.
   a. True, because it's my personal information.
   b. True, because my doctor told me I could do it whenever I wanted.
   c. True, because my manager told me it's okay to look at my own medical record.
   d. False, because this is not permitted as it violates HIPAA Security rules and Beaumont policy.

2. One of my coworkers has a face book account and had posted conversations about a patient she is caring for at Beaumont. She did not identify the patient by name. Is this a violation of the HIPAA Security rule?
   a. No, because the patient's identity has not been disclosed.
   b. No, because her face book has limited viewers.
   c. Yes, because the information provided could allow a co worker to identify the identity of the patient.
   d. No, because she didn't post this information on face book during her work hours at Beaumont.

3. A patient is admitted into the hospital under an alias; the patient is well known to the public and has been recently in the news. Can I text my friends that this celebrity is now a patient at Beaumont?
   a. No, because you have not been authorized to disclose this information.
   b. Yes, the person is a public figure and has on privacy rights.
   c. Yes, because the media is in the hospital interviewing the patient's doctor along with strategic communications.
4. A person who claims to be a vendor has requested access to an electronic device that may contain patient information. The vendor does not have an Beaumont vendor badge. What should I do?
   a. Allow the vendor to access the electronic device using my ID and Password
   b. Not allow the access until I contact my manager/supervisor for further guidance

5. True or False
   I don't need to worry about security of patient's electronic medical record because IT Security is the only one responsible for keeping patient's data safe.
   a. True, because IT monitors the system 24/7.
   b. False, because most security breaches occur when we are not as vigilant with following security practices.

6. It is okay for me to email sensitive Beaumont patient information over the internet?
    a. Yes, because Beaumont IT automatically encrypts all sensitive data going through to the internet**.**
    b. No. In order to send sensitive patient data I need to use Send Secure button on my Beaumont email system.
    c. Yes, because Beaumont only uses virtual private networks.
    d. No, it is only IT role to send patient data over the internet.

7. True or False
   Sharing my ID and Password with a co worker who forgot theirs for the day is okay and does not affect the security system.
    a. True. Since your coworker does not want to call the Help Desk its okay for you to allow them to use your temporarily.
    b. False. Sharing your ID and Password may allow others to access systems or information that they are not allowed to access. Also, an audit trail is created whenever your ID and Password are used.

8. Using a password with a letters, numbers and symbols is *unnecessary.*
    a. True, because it's best to use the same word for all your passwords.
    b. False, using a strong password of letters, numbers and symbols makes it more challenging for identify thefts to use to obtain access to sensitive information.

9. I have a difficult patient situation and I discuss it with one of my colleagues seeking their help. Did I violate HIPAA**?**
    a. Yes, because you are not allowed to speak with anyone regarding the care of a patient.
    b. No, because HIPAA permits colleagues to consult with each other to provide patient care

10. Can I be held personally responsible for a privacy security breach?
    a. Yes, through HR action.
    b. Yes, through action by professional board.
    c. Yes, by the patient that was harmed by the breach of disclosure of confidential information.
    d. All of the above.

11. "A red flag are warning signs that something may not be right with a person's account. They could include inconsistencies with personal data, or other indications that alert the provider to pursue the possibility of identity theft.
    a. True
    b. False

12. There are _____ red flag categories.

a) Five
b) Six
c) Seven

Correct Answer a. Five. There are five (5) Red flag categories

14. The greatest number of medical identity theft occurrences is done by _____

a) Insiders.
b) Patients.
c) External hackers.

Correct answer is a) Insiders. The greatest number of medical identity theft occurrences is committed by insiders. In fact, some identity thieves seek to obtain employment with the sole purpose of stealing patient information.

15. You should notify your supervisor if you see someone using a travel drive to copy patient information without authorization.

a) True
b) False

Correct answer is a) True. Please notify your supervisor if you see someone using a travel drive to copy patient information without authorization.