HIPAA/HITECH PRIVACY AND SECURITY TRAINING

TEST

1. What are some steps you can take to help ensure you protect your online accounts?
   a. Use different passwords on different accounts
   b. Turn a sentence into a mnemonic password (example: Ihw@HCAf6y!)
   c. Include letters, punctuation, symbols, and numbers in your passwords
   d. Make your passwords as long as possible
   e. All of the above

2. Only workforce members with a legitimate “need to know” may access, use or disclose PHI, regardless of the extent of the access provided.
   a. True b. False

3. What does the “e” stand for in ePHI?
   a. Extended
   b. Electronic
   c. Employed
   d. Email

4. When you email, IM or text, which of the following are ways that you could lose your information?
   a. It might be viewed, stored in memory, archived on back-up tapes, and inspected along the path to its recipient
   b. It can be printed, circulated, forwarded, posted on Web sites or blogs, and stored in numerous paper and electronic files
   c. It could accidentally be sent to the wrong person
   d. All of the above

5. Who do your direct your questions regarding information security, potential information security, and/or information security complaints to?
   a. Facility Information Security Official
   b. Division Information Security Official
   c. Information Protection Department
   d. All of the above

6. In the Confidentiality & Security Agreement (CSA) that all workforce members sign, which of the following are you agreeing to NEVER do?
   a. Keep passwords, PINs, and access codes private
   b. Access and use confidential information only as necessary to perform job-related duties
   c. Take reasonable safeguards to protect conversations from unauthorized listeners
   d. Publish or disclose any confidential information to others using personal email or any Internet blogs or sites, including social media

7. Who do you direct your questions regarding privacy matters, patient privacy complaints, and/or potential patient privacy issues to?
   a. Facility Protection Office
   b. Facility Piracy Officer
   c. Facility Privacy Official
   d. None of the above