1. Which of the following constitutes protected health information in electronic form?
   a. Email attachments that contain protected health information
   b. Electronic Medical Records
   c. Electronic files or documents that contain protected health information
   d. All of the above

2. The HIPAA Security Rule requires us to establish the following to protect electronic protected health information (e-PHI):
   a. Administrative Safeguards
   b. Technical Safeguards
   c. Physical Safeguards
   d. All of the above

3. The HIPAA Security Rule requires us to protect electronic protected health information (e-PHI) when:
   a. We are at work
   b. We use e-PHI, transmit e-PHI or store e-PHI
   c. We think someone else might be looking
   d. We feel like it

4. How can we safeguard electronic protected health information (e-PHI)?
   a. Protect all our devices that contain e-PHI with complex passwords
   b. Lock our computer screens when we step away from our computer
   c. Be aware of our surroundings when accessing e-PHI to ensure unauthorized persons cannot view e-PHI
   d. All of the above

5. Where is the best place to store electronic protected health information (e-PHI)?
   a. Email inbox
   b. Flash Drive
   c. Within the secure confines of the Electronic Medical Record
   d. Password protected computer/laptop/tablet

6. When we must transmit electronic protected health information (e-PHI) via email, the following steps must be followed:
   a. None: ETSU/MEAC Personnel are prohibited from transmitting e-PHI via email
   b. The subject line must contain the trigger word—encrypt—and all e-PHI must be in the message or attachment of the email (the subject line must not contain e-PHI as the subject line itself is not secure)
   c. The body of the email message must only contain the patient’s date of birth, social security number and diagnosis
   d. None: ETSU email is secure and ETSU/MEAC Personnel can email any e-PHI they wish
HIPAA Security Rule Quiz Cont.
Please choose the best answer.

7. ETSU/MEAC Personnel must:
   a. Keep anti-virus software enabled and up-to-date
   b. Identify and guard against threats to e-PHI
   c. Alert ITS and the HIPAA Compliance Office if they have any reason to think their device containing e-PHI has been compromised
   d. All of the above

8. True or False: ETSU/MEAC Personnel may check their email and browse the web while within the remote desktop session inside the electronic medical record environment.

9. True or False: ETSU/MEAC Personnel may leave their laptop or other mobile device that contains electronic protected health information or accesses e-PHI locked in the trunk of their car.

10. When is the appropriate time for ETSU/MEAC Personnel to notify the HIPAA Compliance Office of a breach of protected health information?
    a. After you have confirmed that information has been compromised
    b. After a patient notifies the Clinic they are a victim of identity theft
    c. Immediately after becoming aware that a breach has or potentially has occurred
    d. Never