HITECH TRAINING QUIZ
PRINT THE QUIZ, READ THE INSTRUCTIONS, THEN ANSWER THE QUESTIONS. SIGN YOUR QUIZ , and fax to 988-7777.

INSTRUCTIONS: Circle the letter of the **most correct** answer

1. HITECH is part of what federal act of 2009?
   a) Social Security Adm Program
   b) Medicare Program
   c) American Recovery & Reinvestment Act of 2009
   d) Americans with Disabilities Act

2. Breach is defined as
   a) the acquisition, access, use, or disclosure of protected health information in a manner not otherwise permitted under the HIPAA Privacy Rule.
   b) The unintentional acquisition of or inadvertent disclosure of PHI from one person authorized to access PHI to another
   c) a place for fun in the sun.

3. Unsecured protected information can include information in any form or medium, including electronic, paper, or oral form.
   a) True
   b) False

4. Which of the following are expected to protect patient information?
   a) Physicians
   b) Nurses working at clinics
   c) Medical records technicians
   d) Reimbursement specialist
   e) All of the above
5. It is acceptable to wait to report a breach of PHI until you return from vacation if you discover one towards the end of your shift.
   a) True
   b) False

6. Who should a breach be reported to?
   a) Co-workers
   b) Your supervisor, the Privacy Official, Security Official, or General Counsel
   c) The dean
   d) The university president

7. A first offense cannot result in termination.
   a) True
   b) False

8. Which of the following is an exception to a breach?
   a) Discharge papers being given to the wrong patient
   b) Files stolen from a workspace
   c) A billing employee reading and retaining an e-mail not intended for him/her and discusses the detailed information with others
   d) An EOB sent to the wrong patient and returned as undeliverable

9. If it is determined a breach has occurred, all of the following may need to be notified except:
   a) state officials
   b) media
   c) secretary of HHS
   d) affected individuals

10. A breach is considered discovered
    a) when the incident becomes known.
    b) when it occurs.
    c) when the covered entity or Business Associate concludes the analysis of whether the facts constitute a Breach.
    d) when the affected individual finds his/her identity stolen.