HIPAA PRIVACY & SECURITY; HITECH TRAINING QUIZ

PRINT THE QUIZ, READ THE INSTRUCTIONS FOR EACH SECTION, AND THEN ANSWER THE QUESTIONS.
SIGN YOUR QUIZ, and fax to 988-7777.

PART I – HIPAA PRIVACY TRAINING

INSTRUCTIONS: Circle the letter of the most correct answer.

1. What does “HIPAA” stand for?
   a) Health Insurance Portability and Accountability Act
   b) Healthcare Industry Privacy and Accountability Act
   c) Health Insurance Privacy and Administration Act
   d) None of the above

2. What is PHI (Protected Health Information)?
   a) Covered transactions (eligibility, enrollment, health care claims, payment, etc,) performed electronically.
   b) Information about past or present mental or physical condition of a patient.
   c) Information that can be used to identify a patient.
   d) All of the above.

3. What does HIPAA do?
   a) Protects the privacy and security of a patient’s health information.
   b) Provides for electronic and physical security of a patient’s health information.
   c) Prevents health care fraud and abuse.
   d) All of the above.

4. Under the right to Access, healthcare employees have the right to access their own medical records directly, utilizing job-related access such as hospital information and medical records.
   a) True
   b) False

5. When can you use or disclose PHI?
   a) For the treatment of a patient, if that is part of my job.
   b) For obtaining payment for services, if that is part of my job.
   c) When the patient has authorized, in writing, its release.
   d) All of the above.

6. How does a patient learn about privacy under HIPAA?
   a) He looks it up on the internet.
   b) He asks his doctor or nurse.
   c) At his first visit he is given the Provider’s Notice of Privacy Practices, and signs an acknowledgement that he has received a copy of it.
   d) The Government sent this out in the mail to every U.S. Citizen prior to April 14, 2003.
7. **Who at Tulane has to follow HIPAA Law?**
   a) Every Tulane Employee.
   b) Physicians and Clinicians of the Tulane University Medical Group.
   c) University employees who provide management, administrative, financial, legal, or operational support to the Tulane University Medical Group, if they use or disclose individually identifiable Health Information.
   d) b) and c).

8. **May you fax a patient's Protected Health Information?**
   a) Yes, in a medical emergency, and if you use a cover sheet containing a Confidentiality Statement.
   b) Faxing PHI is never appropriate.

---

**PART 2 – HIPAA SECURITY TRAINING**

**INSTRUCTIONS:** Select the best answers for the following questions (there may be more than one correct response).

9. **A co-worker is called away for a short errand and leaves the clinic PC logged onto the confidential information system. You need to look up information using the same computer. What should you do?**
   a) Log your co-worker off and re-log in under your own User-ID and password.
   b) To save time, just continue working under your co-worker’s User-ID.
   c) Wait for the co-worker to return before disconnecting him/her; or take a long break until the co-worker returns.
   d) Find a different computer to use.
   e) a) and/or d)

10. **Which workstation security safeguards are YOU responsible for using and/or protecting?**
    a) User ID
    b) Password
    c) Log-off programs
    d) Lock up the office or work area (doors, windows, laptops)
    e) All of the above

11. **To guard against unauthorized access to electronic Protected Health Information (ePHI) that being sent via email to non-Tulane email address, you must encrypt the message by using the word Secure: at the subject line.**
    a) True
    b) False

12. **In Microsoft Outlook, setting the sensitivity of e-mail messages to Confidential is not enough to protect ePHI in an e-mail to the outside world.**
    a) True
    b) False

13. **Starting on Feb 15, 2009, E-mail between Tulane.edu and HCAHealthcare.com is automatically encrypted,**
    a) meaning users must type Secure: in the subject line.
    b) meaning users must set message sensitivity to Confidential.
    c) hence users do not have to use previously stated encryption procedures.
    d) hence users should never send confidential information via e-mail to HCA.
14. To protect ePHI that is being transmitted within Tulane network, you must do the following:
   a) For Microsoft Outlook Office Client: Check the "Encrypt data between Microsoft Office Outlook and Microsoft Exchange Server." option.
   b) For other client such as MAC Mail, Entourage, and OWA: The encryption is done automatically using Secure Socket Layer (SSL).
   c) Both a and b
   d) You cannot protect ePHI. Do not transmit it via e-mail.

Part 3 – HITECH TRAINING

INSTRUCTIONS: Circle the letter of the most correct answer

15. HITECH, part of the American Recovery & Reinvestment Act of 2009, defines a breach 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.

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

17. 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

18. 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

19. 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

20. 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.