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.

9. What if you know that a patient’s PHI has been leaked to an unauthorized party?
a) Report it to the newspaper.
b) Call the patient at home and report it to him.
c) Report it to your supervisor or the Privacy Official.
d) Call the HIPAA Oversight and Compliance Committee.

10. How do I protect our patients’ PHI from unauthorized individuals?
a) Log off computer terminals and/or have password-protected screen-savers.
b) Don’t give out your computer log-on and/or password to anybody.
c) Position printers and computer terminals so that information is not accessible to or viewable by unauthorized viewers.
d) All of the above.

PART 2 – HIPAA SECURITY TRAINING

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

1. 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)

2. Your sister sends you an email at work with a screen saver she says you would love. What should you do?
a) Download it onto your computer, since it’s from a trusted source.
b) Forward the message to other friends to share it.
c) Call Information Technology (Help Desk), and ask them to help you install it.
d) Delete the message.
3. 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

4. Your supervisor (a physician) is very busy and asks you to log into the clinical information system, using his/her User-ID and password, to retrieve some patient reports. What should you do?
   a) It’s your boss, so it’s okay to do this
   b) Ignore the request, and hope he/she forgets
   c) Decline the request, and refer to the HIPAA Security/Privacy policies

5. You are personally responsible for implementing safeguards that protect the confidentiality, integrity, and availability of ePHI on mobile devices or media.
   a) True
   b) False

---

**Part 3 – HITECH TRAINING**

**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) Your supervisor
   b) The Privacy Official, Security Official, or General Counsel
   c) Co-workers
   d) The dean
   e) 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.