Health Insurance Portability and Accountability Act, FERPA Review QUIZ

Name: _______________________________ Date: ________________

1. PHI stands for “personal health identification” T F

2. Most health-care organizations must follow the Privacy Rule T F

3. It is OK to disclose health information as long as you do not use the Patients’ name T F

4. PTO stands for Patient, Treatment, Outcomes T F

5. Keeping file rooms locked and computer monitors turned away from public view are examples of reasonable safeguards T F

6. All employees should have access to patient health information T F

7. Authorization is required to disclose any PHI T F

8. An employee can be held personally responsible for a breach of information T F

9. Everyone is responsible for compliance and patient privacy T F

10. Students rights are protected under FERPA and include privacy Protection of all records, health, education, etc. T F

Signature of Educator: ________________________________

Signature of Student: ________________________________ Date: ________
Confidentiality Statement

As an employee/faculty/medical staff/resident/student/volunteer/trainee/vendor/agent, I agree to protect the confidentiality of any patient information that becomes available or accessible through association with the UTMC. “Patient Information” includes all health information, personal information and financial information pertaining to a patient and the relatives or household members of the patient, as described in Policy No. 3364-15-10 Confidentiality of Patient Information.

I will abide by Federal and State Laws and University policies pertaining to the Confidentiality of Patient Information by:

- Avoiding any inappropriate disclosure of confidential patient information as outlined in Compliance Policy #3364-15-10 Confidentiality of Patient Information and policy 3364-25-01 Standards of Conduct.
- Using confidential files, data and patient information only for the purposes I have been specifically authorized.
- Reporting immediately any unauthorized access or use of confidential patient information to my department director and/or supervisor, or Administration, as applicable.
- Disposing properly of confidential information according to Compliance Policy #3364-15-09, Disposal of Protected Information.
- Accessing, using and disclosing of confidential information which is minimally necessary for the required purposes, as set forth in HIPAA Policy # 3364-100-90-02, Minimum Necessary Guidelines for Use/Disclosure of Protected Health Information.

To ensure compliance with the Federal and State laws and University policies, I will not:

- Share confidential patient information with anyone unless the information is required for patient care, or as authorized by Policy #3364-100-90-1, Release of Information.
- Review and/or access patient information for which I have no authorization or no need to know or allow unauthorized personal access to files, computers, records, and/or other confidential information.
- Make copies of any confidential information except as specifically authorized by my department director and/or supervisor.
- Share my computer password or file access codes with anyone as defined in IT policy 3364-65-02 Access Control.
- Permit others to indicate my authorship for medical records or billing purposes.

I understand that patient information which is personally identifiable is considered confidential and may be protected by Federal and/or state laws. Breaches of confidentiality will be reported to and investigated by the Privacy Officer/Administration in accordance with institutional corrective action/disciplinary procedures.

__________________________
SIGNATURE

__________________________
DATE

__________________________
PRINT NAME

__________________________
PHONE NUMBER

CONFIDENTIALITY OF PATIENT INFORMATION POLICY 3364-15-10