

2009 HIPAA Privacy and Security Training Test

Name: _____ Employee ID#: _____ **TEST HAS BEEN REVIEWED**
Unit/Dept: _____ Manager: _____ **AND CORRECTED BY: _____**
Date: _____

1. **HIPAA is a federal law enacted to protect the privacy of a patient's personal and health information and provide for its physical and electronic security.**
 - a. The statement is TRUE
 - b. The statement is FALSE
 - c. HIPAA is NOT a federal law.
 - d. HIPAA allows all healthcare workers to view patient records.

2. **Who has to follow the HIPAA Law?**
 - a. Physicians
 - b. Physicians and all Other Patient Care Providers
 - c. Only supervisors and other administrators
 - d. All University workforce members

3. **What does PHI mean?**
 - a. Physical health injuries
 - b. Patient and hospital incidents
 - c. Personal and health information
 - d. Protected health information

4. **Examples of Protected Health Information (PHI) include:**
 - a. Name, address, birthdate, SS#, email address
 - b. Medical records, diagnosis, treatment, test results
 - c. Billing records, research records, referral authorizations
 - d. All of the above

5. **Under what circumstances are you free to access and share PHI ?**
 - a. Only if you know a patient won't mind
 - b. After you no longer work at the organization
 - c. After a patient dies
 - d. Only if it is part of your job and can only be shared with individuals who need the information

6. **Under HIPAA, patients have certain rights contained in the following document(s):**
 - a. Confidentiality Statement
 - b. Notice of Privacy Practices
 - c. Condition of Admission
 - d. Information Release Form

7. **Your sister's best friend just had triple bypass surgery at the medical center. Your sister asks you to find out his prognosis. What should you do?**
 - a. Ask a nurse on the floor how the patient is doing and pass the information along to your sister.
 - b. Log into Essentris and PCIMS and pass the information along to your sister.
 - c. Explain that it's a violation of the patient's privacy for you to ask around or look at his record.
 - d. None of the above.

- 8. When can the University use or disclose PHI?**
- For treatment of a patient, if the patient has received the University's Notice of privacy practices.
 - For payment of bills, if the patient has received the University's Notice of privacy practices.
 - For teaching activities, if the patient has received the University's Notice of privacy practices.
 - All of the above
- 9. State and Federal laws, as well as health system policy, require what form of patient information to be protected and remain confidential?**
- Written
 - Spoken
 - Electronic
 - All of the above
- 10. Because I have access to confidential patient information as part of my job, I can look up anybody's record, even if they are not my patient, as long as I keep the information to myself.**
- The statement is TRUE
 - The statement is FALSE
 - I can also share this information with my family and close friends.
 - I can access hard copy medical charts, but not electronic records anytime I want.
- 11. You can protect patient information by:**
- Protecting verbal or written information
 - Utilizing safe computing skills
 - Reporting suspected security incidents
 - All of the above
- 12. A 19-year-old UCLA student is admitted through the ER for injuries sustained in a motor vehicle accident. She is in stable condition, but awake and alert. Her father calls from Minnesota asking for information on her condition. You can:**
- Tell the patient's father of her general condition and status
 - Provide no information at all to her father
 - Obtain patient consent to provide more than her general condition and status
 - Both a and c.
- 13. A news reporter comes into the ER and tells the attending physician that there is suspicion that the accident in which the 19-year-old female was injured was caused by a sniper shooting on the freeway and he is doing a story for the nightly news. He wants the patient's name and condition for his report. You can provide him with this information.**
- The statement is TRUE
 - The statement is FALSE
 - Any employee can talk to the news media.
 - Only the patient's name can be released.
- 14. Your supervisor (a physician) is very busy and asks you to log into the clinical information system using her user-ID and password to retrieve some patient reports. What should you do?**
- It's your boss, so it's okay to do this.
 - Ignore the request and hope she forgets.
 - Decline the request and refer to the UC Information Security Policies
 - None of the above

15. 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 co-worker to return before disconnecting him/her; or take a long break until co-worker returns.
- d. Leave your co-worker's computer logged on and find a different computer to use.

16. The entire contents of a celebrity's mobile phone (blackberry) have appeared on the Internet, including private emails, addresses and phone numbers from the phone address book. The mobile network appears to have been hacked. A physician has similar information on her blackberry including a photo of a patient (obtained with patient consent) to download into an educational presentation. How can this MD best protect this information?

- a. Download the photo immediately and delete the image from the phone.
- b. Don't take photos of patients on this type of device.
- c. Only keep information on your mobile phone that you have no problem being posted on a public site.
- d. All of the above

17. Accessing patient information electronically can be tracked back to your User ID and computer and defines the documents and time spent accessing the records.

- a. The statement is TRUE
- b. The statement is FALSE
- c. User ID and computer cannot be tracked.
- d. None of the above

18. An email attachment with an unencrypted list of HIV patients was sent in error to 10 individuals outside the organization (names, MRN's, SSN's and diagnoses). What actions should be taken?

- a. The user should notify Computer Services immediately.
- b. Computer services staff should act on the notice immediately.
- c. UCLA Leadership should notify the 10 recipients. Incident and corrective actions should be documented and reported within 5 days to the CA Department of Public Health and the affected patients/legal representatives.
- d. All of the above.

19. I do not work with patients or have access to medical records, however, I see patients pass by my desk in the clinic. Can't I talk about the patients with my coworkers, family and friends even if it has nothing to do with my job?

- a. You may only talk about the patients with your coworkers only
- b. You may only talk about the patients with your family and friends
- c. You may discuss the patients with coworkers and family & friends
- d. You may NOT discuss any patient information with anyone unless they need the information to complete their job.

20. Which workstation security safeguards are YOU responsible for using and/or protecting?

- a. User ID
- b. Password
- c. Logging out of programs that access PHI when not using them.
- d. All of the above

CONFIDENTIALITY STATEMENT

The protection of health and other confidential information is a right protected by law and enforced by fines, criminal penalties as well as UCLA Health System policy.

Safeguarding confidential information is a fundamental obligation for all employees, clinical faculty, house staff, students and volunteers.

Your signature on this statement will commit you to that obligation, and **WILL** be used as proof that you understand basic duties and facts regarding privacy.

Read it carefully.

What you agree to in signing this statement:

1. I agree to protect the privacy, and security of confidential information at all times, both during and after my employment with the University of California has terminated.
2. I agree to a) access confidential information to the minimum extent necessary for my assigned duties and b) disclose such information only to persons authorized to receive it.
3. I agree that I understand the following:
 - a. The UCLA Health System tracks all user IDs used to access electronic records. Those IDs enable discovery of inappropriate access to EITHER employee records or patient records.
 - b. Inappropriate access and unauthorized release of protected information will result in disciplinary action, up to and including termination of employment, and will result in a report to authorities charged with professional licensing, enforcement of privacy laws and prosecution of criminal acts. The Office of Health Information Integrity (OHII) may levy penalties to **individuals** or providers of healthcare of **\$2,500 - \$25,000 per violation**.
 - c. User IDs cannot be shared. Inappropriate use of my ID (**whether by me or anyone else**) is **my** responsibility and exposes me to severe consequences.

Signature: _____ Date: _____

Print Name: _____ Supervisor's or Chair's Initials _____

CONFIDENTIALITY STATEMENT

SUPPLEMENTARY INFORMATION

Confidential Health Information includes but is not limited to:

Any individually identifiable information in possession or derived from a provider of health care regarding a patient's medical history, mental, or physical condition or treatment, as well as the patients and/or their family members records, test results, conversations, research records and financial information. (Note: this information is defined in the Privacy Rule as "protected health information.") Examples include, but are not limited to:

- Physical medical and psychiatric records including paper, photo, video, diagnostic and therapeutic reports, laboratory and pathology samples;
- Patient insurance and billing records;
- Mainframe and department based computerized patient data and alphanumeric radio pager messages;
- Visual observation of patients receiving medical care or accessing services; and
- Verbal information provided by or about a patient.

Confidential Employee & Business Information includes but is not limited to:

- Employee home telephone number and address;
- Spouse or other relative names;
- Social Security number or income tax withholding records;
- Information related to evaluation of performance;
- Other such information obtained from the University's records which if disclosed, would constitute an unwarranted invasion of privacy; or
- Disclosure of Confidential business information that would cause harm to UCLA Health System.

Relevant Regulatory Provisions:

- Peer review and risk management activities and information are protected under California Evidence Code section 1157 and the attorney-client privilege.
- The federal Health Insurance Portability Accountability Act ("HIPAA" or the "Privacy Rule") (45 Code of Federal Regulations Part 160, et. seq.) defines the federal standards for the protection of health information.
- California Confidentiality of Medical Information Act (California Civil Code § 56 et seq.) and the Lanterman-Petris-Short Act (California Welfare & Institutions Code § 5000 et seq.) govern the release of patient identifiable information by hospitals and other health care providers.
- The State Information Practices Act (California Civil Code sections 1798 et seq.) governs the acquisition and use of data that pertains to individuals.
- SB541 and AB211 mandates unauthorized access, review, viewing or disclosure of protected health information or personal information be reported to the Department of Health and to the patient within 5 days of detection. Monetary fines and penalties against UCLA and the individual staff member may be imposed and the incident may be reported to the individual's licensing board (e.g., Medical or Nursing Board).