

2009 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).