STATEMENT OF PRIVACY LAWS AND UNIVERSITY POLICY

It is the legal and ethical responsibility of all UCSF faculty, staff, house staff, students, trainees, volunteers, and contractors to use, protect, and preserve personal and confidential patient, employee, and University business information, including medical information for clinical or research purposes (referred to here collectively as "Confidential Information"), in accordance with state and federal laws and University policy.

Laws controlling the privacy of, access to, and maintenance of confidential information include, but are not limited to, the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the HIPAA Final Omnibus Rule, the California Information Practices Act (IPA), the California Confidentiality of Medical Information Act (CMIA), and the Lanterman- Petris-Short Act (LPS). These and other laws apply whether the information is held in electronic or any other format, and whether the information is used or disclosed orally, in writing, or electronically.

University policies that control the way confidential information may be used include, but are not limited to, the following: UCSF Medical Center Policies 05.01.04 and 05.02.01, LPPI Policies, UCSF Policy 650- 16 Minimum Security Standards, UC Personnel Policies PPSM 80 and APM 160, applicable union agreement provisions, and UC Business, UC Business and Finance Bulletin IS-3 Electronic Information Security, and Finance Bulletin RMP 8.

"Confidential Information" includes information that identifies or describes an individual, the unauthorized disclosure of which would constitute an unwarranted invasion of personal privacy. Examples of confidential employee and University business information include home address, telephone number, medical information, date of birth, citizenship, social security number, spouse/partner/relative names, income tax withholding data, performance evaluations, proprietary/trade secret information, and peer review/risk management information and activities.

"Medical Information" includes the following no matter where it is stored and no matter the format: medical and psychiatric records, photos, videotapes, diagnostic and therapeutic reports, x-rays, scans, laboratory and pathology samples, patient business records (such as bills for service or insurance information), visual observation of patients receiving medical care or accessing services, and verbal information provided by or about a patient. Medical information, including Protected Health Information (PHI), is maintained to serve the patient, health care providers, health care research, and to conform to regulatory requirements.

Unauthorized use, disclosure, viewing of, or access to confidential information in violation of state and/or federal laws may result in personal fines, civil liability, licensure sanctions and/or criminal penalties, in addition to University disciplinary actions.

UCSF Confidentiality of Patient, Employee, and University Business Information Agreement

University Privacy Policy and Acknowledgement of Responsibility

I understand and acknowledge that:

- It is my legal and ethical responsibility as an authorized user to preserve and protect the privacy, confidentiality and security of all confidential information relating to UCSF, its patients, activities and affiliates, in accordance with applicable laws and University policy.
- I will access, use or disclose confidential information only in the performance of my University duties, when required or permitted by law, and disclose information only to persons who have the right to receive that information. When using or disclosing confidential information, I will use or disclose only the minimum information necessary.
- I will discuss confidential information for University-related purposes only. I will not knowingly discuss any confidential information within hearing distance of other persons who do not have the right to receive the information. I will protect confidential information which is disclosed to me in the course of my relationship with UCSF.
- Special legal protections apply to and require specific authorization for release of mental health records, drug abuse records, and any and all references to HIV testing, such as clinical tests, laboratory or others used to identify HIV, a component of HIV, or antibodies or antigens to HIV. I will obtain such authorization for release when appropriate.
- My access to all University electronic information systems is subject to monitoring and audits in accordance with University policy.
- My User ID(s) constitutes my signature and I will be responsible for all entries made under my User ID(s). I agree to always log off of shared workstations.
- It is my responsibility to follow safe computing guidelines.
    - I will use **encrypted** computing devices (whether personal or UCSF-owned), such as desktop computers, laptop computers, tablets, mobile phones, flash drives, and external storage, **for any UCSF work purpose** which involves the use, exchange, or review of Protected Health Information or Personally Identifiable Information, including but not limited to, clinical care, quality reviews, research, educational presentations/conferences, and financial or personnel-related records. Encryption must be a UCSF-approved solution.
    - **I may be personally responsible** for any breach of confidentiality resulting from an unauthorized access to data on an unencrypted device due to theft, loss or any other compromise. I will contact the UCSF IT Service Desk at (415) 514-4100 for questions about encrypting my computing device.
    - I will not share my **Login or User ID and password** with any other person. If I believe someone else has used my Login or User ID and password, I will immediately report the use to the UCSF IT Service Desk at (415) 514-4100 and request a new password.
- Under state and federal laws and regulations governing a patient's right to privacy, unlawful or unauthorized access to or use or disclosure of patients' confidential information may subject me to disciplinary action up to and including immediate termination from my employment/professional relationship with UCSF, civil fines for which **I may be personally responsible**, as well as criminal sanctions.

By signing below:

- **I attest that I have encrypted or will encrypt all of my personal computing devices before using them for any UCSF work purpose, unless I have an encryption exception approved by the UCSF Information Security Officer. I will not use an unencrypted computing device for UCSF work purposes without an approved exception.**
- **I attest I have read, understand, and acknowledge all of the above STATEMENTS OF UNIVERSITY PRIVACY POLICY and the ACKNOWLEDGEMENT OF RESPONSIBILITY.**

_____ Signature	_____ Date
_____ Print Name	_____ UCSF Department
_____ UCSF Employee Number	_____ Signature of Manager or UCSF Representative
❑ Non-UCSF Employee	_____ Print Manager or UCSF Representative Name