University of California
San Francisco

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 only 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**, including but not limited to, clinical care, quality reviews, research and educational presentations/conferences. 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/or password** with any other person. If I believe someone else has used my Login or User ID and/or 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 all of my personal computing devices used for any UCSF work purpose are ENCRYPTED. I will not use an unencrypted computing device for UCSF work purposes.**
- **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 ______________________