

UCSF Privacy and Confidentiality Handbook

*A Handbook for All Faculty, Staff,
Students, Trainees, Vendors, & Volunteers*

Revised May 2009

MESSAGE FROM THE CHANCELLOR ON BEHALF OF THE DEANS AND MEDICAL CENTER CHIEF EXECUTIVE OFFICER

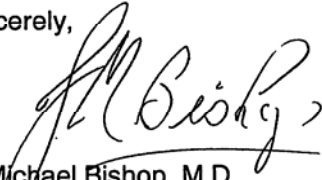
The UCSF Privacy and Confidentiality Handbook is a general introduction to the privacy and security laws and regulations established by the federal Health Insurance Portability and Accountability Act (HIPAA), and the state of California, in addition to University privacy and security policies. These regulations apply to all UCSF faculty, staff, students, trainees, vendors, and volunteers.

These laws and regulations were promulgated, and our policies established, in order to protect the confidential medical and billing records of our patients. Of particular importance are patients' rights related to access and control of their medical information and the new personal liabilities when non-compliance occurs. You are expected to follow these privacy and security laws, regulations, and policies as you perform your daily activities.

Please read this handbook to gain a basic understanding of HIPAA, the California privacy laws, as well as UC policies and the impact on your work at UCSF. Advanced training modules designed to address specific jobs are available to supplement this handbook and will help orient all new and existing faculty, staff, students, trainees, vendors, and volunteers.

We are committed to complying with these privacy laws and regulations because *we value our patients and their privacy.*

Sincerely,

A handwritten signature in black ink, appearing to read "J. Michael Bishop". The signature is fluid and cursive, with a long horizontal stroke at the end.

J. Michael Bishop, M.D.
Chancellor
Arthur and Toni Rembe Rock Distinguished Professor
University Professor

HANDBOOK OBJECTIVES:

This Handbook is a general introduction for all UCSF faculty, staff, students, trainees, vendors, and volunteers to the privacy and security regulations dictated by the federal Health Insurance Portability and Accountability Act (HIPAA) California privacy laws, and UCSF Policies and Medical Center Administrative Policies and Procedures.

In addition, your department or organizational unit may have policies and procedures that supplement this Handbook. Supplemental advanced training modules are available based on your job responsibilities at UCSF. Please refer to <http://hipaa.ucsf.edu/> for advanced training module resources.

TABLE OF CONTENTS

HIPAA	1
Overview: Privacy and Confidentiality.....	1
PRIVACY RULE	1
Purpose of Privacy Rule	1
Highlights of Privacy Rule	1
Potential Consequences of Violating the Privacy Rule	1
WORKFORCE REQUIREMENTS	2
CONFIDENTIAL PROTECTED HEALTH INFORMATION: DEFINITION AND RIGHTS TO ACCESS	2
What is considered confidential protected health information (PHI)?	2
What is not consider PHI?	2
What patient information must we protect?	2
What PHI can be used for research, public health, or health care operations?	2
Who is authorized to access confidential PHI?	2
When can students/trainees access PHI?	3
What is the "Minimum Necessary" Standard?	3
When are patient written authorizations required?	3
What is I see someone violate the privacy law?	3
MEDICAL RECORD ACCESS AND CONTROL	3
PATIENTS' RIGHTS	4
Right to receive a paper copy of the "Notice of Privacy Practices"	4
Right of Access	4
Right to Request an Amendment or Addendum	4
Right to an Accounting of Disclosures	4
Right to Request Restrictions	4
Right to Complain	4
Exceptions to the PHI Disclosure Rules	4
Right to be Included in Facility Patient Directories (In-patient Patients)	5
Right When Patient is Unable to Authorize Release of PHI	5
Right to Authorize Release of Patient's PHI	5
BUSINESS ASSOCIATES	5
CLINICAL AND OTHER RESEARCH INVOLVING HUMAN SUBJECTS	6
CHR Application	6
Authorization and Waiver of Authorization	6
Non-identifiable Information Options	6
Protections of Information	6
SECURITY RULE	7
COMPUTER SYSTEMS AND ELECTRONIC TRANSMISSIONS OF INFORMATION	7
Purpose of Security Rule	7
Definition of Security	7
Requirements for Security	7
How to Comply with the Security Rule	8
What steps Must I take to Safeguard Computer Resources and PHI?	8
<i>Password Security</i>	8
<i>Workstation Security</i>	8
<i>Disposal/destruction methods</i>	8
<i>Facility/physical access and identification</i>	9
PHI and Email/Fax/Voice mail/ Answering Machines/Telephone Communication/Mobile Computing Devices and PDA Security	9
<i>Email</i>	9
<i>Fax</i>	10

Voice Mail / Answering machines/ Telephone Communication	10
Mobile Computing Devices and PDA Security	10
USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)	
(MARKETING, FUNDRAISING, MEDIA, PHOTOGRAPHY).....	11
Marketing	11
Fundraising	11
Media	12
Photography	12
OTHER FEDERAL LAWS	12
Medicare Conditions of Participation (CoP)	12
Red Flag Rule	12
Family Education Rights and Privacy Act (FERPA)	12
Federal Department of Health and Human Services	12
CALIFORNIA STATE LAWS	13
Confidentiality of Medical Information Act (CMIA)	13
Civil Code Sections 1785.11.2, 1798.29, 1798.82, Health & Safety Code Section 130200	13
Health and Safety Code (Section 1280.15)	13
Lanterman-Petris-Short Act (LPS)	13
Title 22, California Code of Regulations	13
Potential Consequences of Violating the State Privacy Laws	13
FREQUENTLY ASKED QUESTIONS (FAQs)	13
UCSF RESOURCE LIST	16
APPENDIX 1: PHI DATA ELEMENTS	17
APPENDIX 2: RESOLUTION OF THE UNIVERSITY OF CALIFORNIA BOARD OF REGENTS:	
Academic Health Center Health Insurance Portability and Accountability Act (HIPAA)	
Compliance Program	18
APPENDIX 3: UNIVERSITY OF CALIFORNIA, SAN FRANCISCO CONFIDENTIALITY OF	
PATIENT, EMPLOYEE & UNIVERSITY BUSINESS INFORMATION AGREEMENT.....	19
Statement of Privacy Laws and University Policy	19
Acknowledgement of Responsibility	20

Special Thanks to...

Privacy Compliance Steering Committee, Legal Affairs, Risk Management, Patient Relations, Health Information Management Services, University Development, Research- HRPP, Information Technology, OAAIS- Enterprise Information Security, Marketing, and Public Affairs.

POLICY REFERENCE TABLE

Policy Description	Medical Center Policy Number	Campus Policy Number
Academic Affiliation Agreements	1.01.02	100-10
Adverse Publicity or Incidents	1.03.01	
Code of Conduct and Principles of Compliance	1.02.09	
Code of Ethical Behavior	1.02.02	
Confidentiality, Access, Use and Disclosure of PHI and Patient Privacy	5.02.01	
Contracting Ethics	1.03.05	
Electronic Mail	5.01.02	
Identity/ Medical Identity Theft Prevention and Response Policy	Pending	200-29
Information Security and Confidentiality	5.01.04	650-16
Remote Access	5.01.07	
Facsimile Documents Containing PHI	5.01.25	
Fundraising Campaigns		450-13
Fundraising Events		450-16
Gifts and Endowments	3.03.02	
Guidelines for Industry Representatives	3.05.07	
HIPAA Business Associates	1.02.15	200-28
Marketing Ethics	1.03.06	
Organ and Tissue Donation	6.05.08	
Patient Access to Protected Health Information	6.04.03	
Patient Complaints and Grievances	6.04.04	
Patient Participation in Research Protocols	6.07.11	
Patient Rights and Responsibilities	6.04.10	
Press Code	1.03.07	
Research Involving Human Subjects		100-16
Sentinel / Adverse Event Process	3.06.10	
UCSF Foundation		500-11

Medical Center Policies

<http://manuals.ucsfmedicalcenter.org/index.shtml>

Information Technology Policies and Procedures

http://it.ucsfmedicalcenter.org/policies_and_procedures/

Campus Administrative Policies

<http://policies.ucsf.edu>

UCOP Policies

<http://www.ucop.edu/ucophome/coordrev/ucpolicies/>

HIPAA

Overview: Privacy and Confidentiality

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), is a federal law which, in part, protects the privacy of individually identifiable patient information and provides for the electronic and physical security of health and patient medical information, and simplifies billing and other electronic transactions through the use of standard transactions and code sets (billing codes). HIPAA applies to all “covered entities” such as hospitals, physicians and other providers and health plans as well as their employees and other members of the covered entities’ workforce.

Privacy and security are addressed separately in HIPAA under two distinct rules, the Privacy Rule and the Security Rule.

The Privacy Rule sets the standards for how all protected health information should be controlled. Privacy standards define what information must be protected, who is authorized to access, use or disclose this information, what processes must be in place to control the access, use, and disclosure of information, and to ensure patient privacy rights.

The Security Rule defines the standards that require covered entities to implement basic security safeguards to protect electronic protected health information (ePHI). Security is the ability to control access and protect electronic information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss. The standards include administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of ePHI.

PRIVACY RULE

Purpose of Privacy Rule

To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information;

Highlights of Privacy Rule

The Privacy Rule requires that access to **protected health information (PHI)**, which includes electronic PHI (ePHI), by UCSF faculty, staff, students, trainees, vendors, and volunteers be based on the general principles of “need to know” and “minimum necessary,” in which access is limited to the patient information needed to perform a job function.

The HIPAA Privacy Rule also accords certain rights to patients, such as:

- Right to request access to their own health records
- Right to request an amendment of information in their records
- Right to receive an accounting of disclosure of their information

Potential Consequences of Violating the Privacy Rule

The Privacy Rule imposes penalties for non-compliance and for breaches of privacy which range from \$100 to \$50,000 per violation, in addition to costs and attorneys’ fees, depending on the type of violation. Penalties include fines up to a maximum of \$1,500,000 per event potential for civil lawsuits, the potential for misdemeanor charges and reporting the violation to licensing boards for individuals.

Workforce Requirements

All faculty, staff, students, trainees, vendors and volunteers, and contractors are required to review this Handbook and sign the Confidentiality Statement (Appendix 3). The signed document needs to be stored in a centralized area in the department for a minimum of six years after the last date of service.

Additional documents may be required depending on the amount of contact with patients or protected health information. For guidance, please contact your HR or Purchasing department or see the Privacy Office Website.

Confidential Protected Health Information: Definition and Rights to Access

What is considered confidential protected health information (PHI)?

PHI is individually identifiable health information which can be matched with a patient, is created in the process of caring for the patient, and is transmitted or maintained in an electronic, written, or oral manner. Examples of PHI are: patient name, address, birth date, age, medical record number, number, phone and fax numbers, and email address.

What is not considered PHI?

Health information is not protected health information if it is de-identified. De-identified information may be used without restriction and patient authorization. The de-identification rule states that you can disclose health information after it is no longer PHI because the 18 identifying data elements listed in the regulations have been removed. (See Appendix 1 for a list of the 18 data elements).

What patient information must we protect?

We must protect all PHI which includes items such as medical records, diagnoses, x-rays, photos and images, prescriptions, lab work and test results, billing records, claim data, referral authorizations, and explanation of benefits. Research records of patient care must also be protected. If health-related information is de-identified, it is not PHI and may be shared without restriction. De-identification means the removal of all personal identifiers (refer to Appendix 1. PHI Data Elements).

What PHI can be used for research, public health, or health care operations?

A limited data set is a class of PHI that excludes 16 of the 18 identifiers. The limited data set can be used for research, public health or health care operations, as long as the recipient of the data signs a data use agreement with UCSF. See CHR guidance at the CHR website for research and call Privacy Office with questions (415-353-2750).

Who is authorized to access confidential PHI?

Under certain circumstances, PHI may be accessed without patient consent which are further described in the UCSF "Notice of Privacy Practices." Doctors, nurses, and other licensed providers on the health-care team may access the entire medical record, based on their "need to know." All other members of the workforce may access only the information needed to do their jobs. Moreover, certain uses for the purpose of Treatment, Payment and health care Operations (TPO) are permitted without HIPAA authorizations:

- **Treatment** of the patient, including appointment reminders
- **Payment** of health care bills (claim submission, authorizations, and payment posting)
- Health care **operations** and business operations, including, teaching and medical staff quality activities, research (when approved by the IRB and with a patient's written permission); health care communications between a patient and their physician; and hospital directory

When can students/trainees access PHI?

Students and trainees in all UCSF and affiliated training programs may have access to PHI. Students/trainees are required to complete a privacy orientation and to sign a confidentiality agreement. **Students and trainees are not permitted to remove any PHI from UCSF premises under any circumstances.** Students and trainees may request copies of de-identified data for use in case presentations; however, the request for use/disclosure must be coordinated with UCSF Medical Center's Health Information Management Services (HIMS).

What is the "Minimum Necessary" Standard?

The minimum necessary standard in the Privacy Rule requires that when a covered entity uses or discloses protected health information or requests protected health information from another covered entity, the covered entity must make reasonable efforts to limit protected health information to that which is reasonably necessary to accomplish the intended purpose of the use, disclosure, or request. You are expected to apply the minimum-necessary standard when you access PHI. For example, although physicians, nurses, and care providers may need to view the entire medical record, a billing clerk would likely only need to see a specific report to determine the billing codes. An admissions staff member may not need to see the medical record at all, only an order form with the admitting diagnosis and identification of the admitting physician. You are permitted to access and use only the minimum patient information necessary to do your own job.

When are patient written authorizations required?

To use or disclose PHI for almost any other reason, you will need to obtain a written authorization from the patient prior to access or disclosure. The signed authorization must be placed in the patient's official medical record. Refer to the "Notice of Privacy Practices" for a list of covered exceptions to the authorization requirement related to public policy, certain health disease reporting requirements, and law enforcement activities. (Available at <http://hipaa.ucsf.edu/>.) If you still have questions, ask your supervisor or department chair for guidance.

What if I see someone violate the privacy law?

It is University of California policy that each of us has a responsibility to prevent unauthorized or unapproved access to, or disclosure of, patient information. Report concerns to your supervisor, the UCSF hot line (415-502-8448), or the UCSF Privacy Office (415-353-2750). Refer to the resource list on page 16 for a list of individuals to contact with specific questions about HIPAA privacy and security.

Medical Record Access and Control

Medical records are maintained for the benefit of the patient, medical staff, and the hospital and shall be available upon request of:

- treating physicians;
- non-physicians involved with the patient's direct care (*i.e.*, Nursing, Pharmacy);
- any authorized officer, agent, or employee of the Medical Center or its Medical Staff (*i.e.*, Risk Management, Patient Relations);
- UCSF researchers as part of an approved Committee for Human Research (CHR) protocol that involves medical record review;
- any other person authorized by law to make such a request (*i.e.*, medical examiners, law enforcement, regulatory agencies);
- patient and/or patient's authorized representative.

The Medical Center will maintain ownership of the medical record, and it may be removed from the Medical Center jurisdiction only by:

- subpoena, *or*
- court order, *or*
- statute

At UCSF, Health Information Management Services (HIMS) is responsible for maintaining control of access to medical records. Specific instructions for obtaining access to medical records are provided on the HIMS website at <http://hims.ucsfmedicalcenter.org/>. Authorization forms can be downloaded from this site. Additional details are discussed in the Patients' Rights section on page 4.

Medical records are not to be removed from patient care areas except by authorized HIMS staff

Patients' Rights

Patients' rights under HIPAA are described in the "Notice of Privacy Practices." The notice is made available to patients in many settings including UCSF's Privacy website. These rights include:

- **Right to receive a paper copy of the "Notice of Privacy Practices,"** which informs patients of their rights and how to exercise them. UCSF is required to make this notice available to patients.
- **Right of Access.** Patients may request to inspect their medical record and may request copies.
- **Right to Request an Amendment or Addendum.** The patients may file a request for an amendment or addendum to the medical record.
- **Right to an Accounting of Disclosures.** Patients have the right to receive an accounting of disclosures which documents those disclosures for which the patient has not signed an authorization.
- **Right to Request Restrictions.** Patients have the right to request restrictions on how we will communicate with the patient or release information.
- **Right to Complain.** Patients have the right to complain if they think that privacy rights have been violated.

If a patient requests any of the above, please refer them to the central control point for the specific right as outlined in the Notice of Privacy Practices, such as Patient Relations, Health Information Management Services (HIMS), Committee for Human Research (CHR), or the Privacy Office. (See UCSF Resource List page 16).

Exceptions to the PHI Disclosure Rules

Under HIPAA, there are certain exceptions to the PHI disclosure rules and they are described in the "Notice of Privacy Practices." They include disclosures which are subject to professional judgment, for public health and safety purposes, for government functions, law enforcement and based on a judicial request or subpoena.

Psychotherapy notes require special handling and authorizations. All requests for psychotherapy notes must be routed to HIMS.

PHI may be used for research, fundraising (demographic information only), public information or health care communication, but special rules apply. For guidance refer to the appropriate policies.

If you are unsure whether a request for information is authorized, please check with your supervisor or HIMS ("Request for Release of Patient Record" 415-353-2221). Since these disclosures may be subject to a request for an accounting of disclosures, the requests need to be coordinated, tracked, documented, and archived by HIMS.

Right to be included in Facility Patient Directories (In-patient Patients)

UCSF can use and disclose selected PHI, which includes name, location in the hospital, condition (e.g., good, fair, critical) and religious affiliation in order to create facility patient directories. These directories are for use by the clergy and for responding to those who ask for a patient by name. If a patient opts out of the facility patient directory, the UCSF will not provide this information.

Right When Patient is Unable to Authorize Release of PHI

If a request for PHI is made by the patient's spouse, parent, child, or sibling and the patient is unable to authorize the release of such information, UCSF is required to give notification of the patient's presence in the hospital, except to the extent prohibited by law.

Upon a patient's admission, UCSF is required to make reasonable attempts to notify the patient's next of kin or any other person designated by the patient of their admission, and, only upon request of the family member, provide information on the patient's release, transfer, serious illness, injury, or death, unless the patient requests that this information not be provided.

Right to Authorize Release of Patient's PHI

HIPAA specifies the content of an authorization to disclose PHI. At UCSF, the authorization process is managed by HIMS. A written authorization from the patient (or the patient's personal representative) is required to disclose or access PHI for uses, other than for treatment, payment and/or healthcare operations.

- Special authorization is required to access any psychotherapy record.
- An authorization is needed from a patient before any PHI can be released to a UC Department, which is not a part of the Health Care Enterprise (or serves a business associate function such as the Legal Department of the Office of the President).
- UCSF researchers must also complete request forms to review medical records as part of an approved Committee for Human Research (CHR) protocol which includes either obtaining patient authorization or obtaining a CHR-approved waiver of authorization.

Business Associates

Under HIPAA, a vendor or third party that is exposed to UCSF's PHI in the performance of its services for UCSF is a "business associate" and is required to enter into a business associate agreement (BAA) with UCSF pursuant to the HIPAA regulations. The BAA sets forth, in part, the obligation of the business associate related to the privacy and security requirements. UCOP has created standard agreements for the campuses to use for this purpose.

BAAs are required for companies or persons who engage in a function or activity involving the use or disclosure of individually identifiable health information, such as:

- claims processing or administration,
- data analysis, processing or administration,
- utilization review,
- quality assurance, billing, benefit management, practice management and re-pricing; Legal,
- actuarial,
- accounting,
- data aggregation,
- management

This is not an all-inclusive list. For all vendor or third-party relationships that involve PHI or if you are unsure whether the third-party vendor is subject to HIPAA, please contact, the UCSF Medical Center Purchasing (415-353-4701) or the Campus Purchasing (415-476-5761).

Clinical and Other Research Involving Human Subjects **(Including the use of human specimens or information from medical records and databases)**

Committee for Human Research (CHR) review is required for all human-subject research including the creation and administration of research data registries and repositories which contain identifiable information. At UCSF, the CHR is part of the UCSF Human Research Protection Program (HRPP) and serves as the Institutional Review Board (IRB) and the Privacy Board to safeguard the rights and welfare of human research subjects.

Under the Privacy Rule, UCSF may use or disclose PHI for research purposes and researchers may obtain, create, use and/or disclose individually identifiable health information if they obtain the appropriate authorizations and approvals for research, which include:

- IRB approval for research, *and one or both of the following:*
- Patient authorization for release of information, *and/or*
- A CHR approved Waiver of Authorization.

CHR Application

In order to obtain CHR approval for research access to, and collection of, and use of identifiable medical information, a research application must be submitted to the CHR. In the CHR application, research investigators must describe their plan to protect participants' privacy and confidentiality, describe or indicate the source of identifiable medical information collected or accessed for the research, the processes to use or disclose information as well as the protections for the identifiable medical information. If a Waiver of Authorization is requested, this request must be made explicitly in a separate section of the CHR application.

These requirements apply to any UCSF human research study, and all investigators are expected to adhere to the Privacy Rule standard for collecting only the minimum necessary data and identifiers required to achieve the research aims. More information about the CHR application process can be found at the HRPP web site: <http://www.research.ucsf.edu/chr/index.asp>.

Authorization and Waiver of Authorization

Access to medical records/clinical data systems for recruitment purposes and chart review must meet the Privacy Rule requirements for appropriate research authorization. At UCSF, Health Information Management Services (HIMS) controls the release of medical records for chart review or access to medical information and will require the following:

- CHR approval letter, *and*
- Patient authorization for release of medical information for research purposes, *or*
- CHR approval of Waiver of Authorization.

Non-identifiable Information Options

Alternatively, researchers can choose to collect coded or de-identified data without obtaining an individual's authorization and without further restrictions on use or disclosure because de-identified data is not PHI and, therefore, not subject to the Privacy Rule. A CHR application will be needed if researchers need access to identifiable medical information.

Protections of Information

HIPAA mandates that systems and processes must be in place to protect the confidentiality and privacy of patient information. As such, all research investigators are responsible for all aspects of their research study, including adhering to policy and procedures for the protection of privacy and confidentiality of identifiable information. Investigators must take appropriate steps which include using and storing research data in a manner that ensures physical and electronic (*e.g.*, encryption) security. Data Use Agreement or Business Associate Agreement may be required to allow for the sharing of data outside of UCSF.

HRPP guidance on information security is posted on the CHR website. With prior CHR approval, clinical databases, data repositories, and tissue and specimen banks can be developed for research purposes and to be maintained in perpetuity, as long as they are HIPAA compliant and have current CHR approval. Additional HRPP Guidance on the CHR website includes:

- [Applying and Reporting to the CHR](#)
- [HIPAA and Human Research](#)
- [Information Security and Human Subjects Research](#)

SECURITY RULE

Computer Systems & Electronic Transmissions of Information

Purpose of Security Rule

- To ensure **confidentiality, integrity** and **availability** of all electronic protected health information (ePHI) that is created, received, maintained or transmitted by the covered entity.
- To protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
- To protect against any reasonably anticipated uses or disclosures of ePHI.
- To ensure compliance by its workforce.

Definition of Security

Security is generally defined as having controls, counter-measures, and procedures in place to ensure the appropriate protection of information assets and control access to valued resources. Security is minimizing the vulnerability of assets and resources.

Requirements for Security

Under HIPAA, UCSF is required to secure all access to electronically stored and transmitted protected health information (ePHI).

- The Information Security departments of UCSF and UCSF Medical Center are responsible for establishing security policies, procedures and systems that protect University computers from threats or vulnerabilities.
- Workforce members are directly responsible for employing appropriate and applicable security controls to protect University electronic information resources that are in his or her control:
 - By properly safeguarding PHI from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss;
 - By safeguarding the University's computers from computer viruses and intrusive computer software;
 - By taking precautions that will minimize the potential of theft, destruction or any type of loss of such assets;
 - By ensuring that access to workstations, ePHI and portable media, such as floppy disks, tapes, CD-ROM disks, PCMCIA cards, memory sticks/ thumb drives and all other forms of removable media and storage devices, cannot be inappropriately viewed or used by unauthorized persons.

How to Comply with the Security Rule

What Steps Must I Take to Safeguard Computer Resources and PHI?

There are several steps that you must take to help protect the privacy and electronic security of PHI, a few of which are listed below:

- ***Password Security***

1. Protect your user ID and password. Do not share or post passwords under any circumstances!
2. Commit your password to memory.
3. When choosing passwords, at a minimum, incorporate a combination of letters and numbers into the password.
4. Immediately change your password if it is accidentally exposed or compromised.
5. Report all password exposures to your department supervisor or manager, the UCSF hot line (415-502-8448), or the UCSF IT Customer Support Line at 415-514-4100 (Medical Center option 1 or Campus option 2).
6. Adhere to established password management guidelines by changing your password periodically and by following instructions when you think your password has been compromised.
7. Always keep computers password-protected and under lock and key when not in use.

- ***Workstation Security***

1. Log-off or lock access to computers when you leave, even if only for a moment.
2. Keep the system up-to-date with current operating system security patches and antivirus definitions.
3. Keep confidential or sensitive information locked away when not in use. File documents in locked cabinets or drawers when you have finished with them.
4. Ensure that systems meet UCSF minimum security standards.
5. Ensure that displays of computer stations with access to ePHI are not visible to unauthorized individuals.
6. Be alert to recognize and report all privacy and security incidents to your department supervisor or manager, the UCSF hot line (415-502-8448), or the UCSF Privacy Office (415-353-2750), and for IT security issues call the UCSF IT Customer Support Line 415-514-4100 (Medical Center option 1 or Campus option 2).

- ***Disposal/destruction methods***

1. Never leave sensitive or confidential information in a trash bin. Securely dispose of all papers that contain PHI. ALWAYS follow the proper paper disposal procedure (e.g., use secure

bags, shredders, locked 'shred-it' bins, etc.). Locked, shredder disposal bins are located throughout UCSF.

2. Back up data files and securely store backup media; and follow approved UCSF media destruction before permitting devices and media to be transferred, sold or donated. Maintain records to track the movement (transfer or relocation) of devices and media.

- **Facility/Physical Access and Identification**

1. Always follow established visitor security procedures.
2. Always wear your security badge/identity badge when at work.

PHI AND EMAIL / FAX / VOICE MAIL / ANSWERING MACHINES / TELEPHONE COMMUNICATION/ MOBILE COMPUTING DEVICES AND PDA SECURITY

- **Email**

Email systems are not secure unless you have explicit information that the system is encrypted or in other ways secure.

1. If you are using email to send UCSF confidential or patient information then you are responsible for ensuring that this information is processed securely by using UCSF Secure Email. UCSF Secure Email system works by placing your outbound email message on a secure web site called UCSF Secure Messenger. The recipient receives an email message from the Secure Messenger indicating that there is a secure email message waiting for them at the UCSF secure website, along with a web link to the UCSF secure web site. By accessing the web link, the recipient will be able to retrieve the message over a secure link. Detailed instructions are available at:
 - i. Medical Center Information Technology
http://it.ucsfmedicalcenter.org/secure_email/
 - ii. Office of Academic and Administrative Information Systems(OAAIS)
<http://oaais.ucsf.edu//OAAIS/171-DSY.html>
 - iii. School of Medicine Information Services Unit (ISU)
http://www.medschool.ucsf.edu/help/Troubleshooting/secure_email.htm
2. How to use the secure email system correctly:
 - i. The start of the subject line must be precise in order to enable security.
 - ii. The subject line should begin with ePHI, PHI, or Secure followed by a colon and then a space. Examples of appropriate email subject lines:

ePHI: Your Appointment
PHI: Your Appointment
Secure: Your Appointment
3. Be careful what you send via email. Do not send confidential information unless you can de-identify it. Warn patients who communicate with you via email that their confidentiality cannot be ensured.
4. Use the same care in sending emails that you would with a letter. Do not write anything in an email that you might regret later. Assume emails are never erased.

5. Do not send attachments containing ePHI without encryption.
6. Add a confidentiality message footer to your messages, such as:

***CONFIDENTIALITY NOTICE** This email communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.*

7. If you identify PHI was sent in error, contact the sender. Do not extend the breach of information by forwarding the identified ePHI to others.
8. If you are advised that you sent an email of PHI to the wrong recipient, confirm the recipient destroyed all copies and did not forward the information. Immediately contact the Privacy Office for next steps.

- **Fax**

1. Never fax PHI to an unsecured fax machine. (A secure fax is one located in a restricted environment.) Call ahead to ensure that the intended recipient will pick up the fax.
2. Always check the destination fax number before faxing.
3. Use cover sheets containing a confidentiality statement, such as:

***CONFIDENTIALITY NOTICE** This communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.*

4. Return items which you have received in error (faxed to the wrong location or improperly faxed) and advise sender of the error.
5. If you are advised that you sent a fax of PHI to the wrong number, confirm the recipient destroyed all copies and did not share the information. Immediately contact the Privacy Office for next steps.

- **Voice Mail / Answering Machines / Telephone Communication**

1. Consider who has access to your voice mail or answering machine so others do not access that PHI.
2. Take care what messages you leave on answering machines and voice mail.
3. If you use a speakerphone, be aware of your surroundings and sensitive to the messages being replayed.
4. If you are advised that you left PHI on the wrong voice mail, confirm the recipient deleted the message and did not forward the information. Contact the Privacy Office for next steps.

- **Mobile Computing Devices and PDA Security**

A mobile computing device has a broad definition and includes all devices/media capable of storing data in electronic format such as laptops, PDAs, cell phones, blue tooth devices, memory sticks/thumbdrives, external hard drives, and digital cameras.

1. If at all possible, do not store ePHI on mobile devices.

2. If ePHI is stored on a mobile device, the data must be encrypted with an approved UCSF data encryption solution.
3. Never leave devices in an exposed or unsecured area.
4. Always password-protect mobile devices.
5. Utilize physical locks for laptops and other mobile devices.
6. Keep mobile devices up-to-date with current operating system security patches.
7. Ensure that the mobile device meets UCSF security minimum standards.
8. Frequently make protected backups of data stored on remote systems.
9. Use caution when uploading or downloading files to/from mobile devices, such as PDAs and laptops. Adhere to the "minimum necessary" standard and never transfer ePHI over a network to/from a mobile device without using encryption.
10. Off-site work requires greater vigilance to maintain the required level of privacy and security.
11. Be alert to recognize and report all privacy and security incidents to your department supervisor or manager, the UCSF hot line (415-502-8448), or the UCSF Privacy Office (415-353-2750) or for IT security issues call CSC (415-514-1400).
12. Immediately report lost or stolen devices to the UCSF Police Department by filing a police report. Call 415-476-1414 to report a lost or stolen mobile computing device. Refer to the Lost/stolen mobile device flowchart at http://isecurity.ucsf.edu/content/pdfs/Flowcart_A.pdf.

Use and Disclosure of Protected Health Information (PHI) **(Marketing, Fundraising, Media, Photography)**

Marketing

Use of PHI for marketing purposes as defined by HIPAA will require the patient's prior written authorization. However, UCSF marketing department activities are considered health care communication activities and not "marketing" activities as defined by HIPAA. All projects conducted by the Marketing Department must still comply with all other laws and UCSF guidelines for use of PHI. If you are unsure about what PHI may be disclosed for marketing purposes, call the Director of Marketing at (415-353-2716). To help ensure compliance with both PHI and marketing guidelines, departments producing documents for external use are encouraged to contact the Marketing Department in advance of production.

Fundraising

Although HIPAA does not prohibit fundraising efforts that target patients, it strictly limits the use of PHI to only demographic information for fundraising. A patient's demographic information is defined as name, date of birth, gender, ethnicity, insurance status, address and other contact information, and only this demographic information can be used for fundraising without prior written authorization.

To ensure full compliance with HIPAA, UCSF policy requires physicians, departments, divisions and all other UCSF entities to secure approval from the centralized opt-out database of University Development and Alumni Relations (UDAR) for all fundraising efforts that target patients (e.g., individual major gift solicitations, direct mail appeals, fundraising event invitations, etc.). All mail files must be run against the UDAR opt-out database prior to the fundraising mailing. Please call (415-514-0508) for assistance.

HIPAA specifies that all fundraising materials that target patients must include a clear and simple way for the recipients to opt out of future solicitations. The following language has been approved by UCSF legal counsel for this purpose:

If you do not wish to receive further fundraising communications from, please contact: Records Manager, UCSF Box 0248, San Francisco, CA 94143-0248 or call (888-802-4722). Note that UDAR is the UCSF office of record for opt-outs. For this reason, the address shown in the above opt-out language should not be altered. Opt-outs received via phone, email, or personal contact must be forwarded to UDAR immediately.

When it is necessary to secure an authorization for fundraising, the patient's health care provider must initiate the process by asking the patient if s/he is willing to sign the authorization. After this initial conversation, a staff member may complete the process. Note that UDAR is the office of record for fundraising authorizations. Signed fundraising authorizations must be forwarded to UDAR immediately.

Media

The UCSF News Services Office is responsible for overall management of media relations for the campus and Medical Center. Any inquiries from reporters, photographers, or other media representatives should be referred to the News Office at (415-476-2557), which is covered 24 hours a day, weekends, and holidays. After regular business hours (8 a.m.-5 p.m.), a News Office staff person is on-call and available to handle inquiries and other situations that involve communication to the media. Reporters, photographers, camera crews, and other media representatives cannot be in clinical areas without supervision from News Office staff.

Photography

- Photography that is covered by the terms and conditions of admission: this document, which every patient must sign in order to obtain treatment at UCSF, is limited to photography for treatment and safety purposes only. For example the photography that is done on 15 Long for the safety of newborns is permitted, as is a photograph of a wound for placement in the Medical Record.
- Non-treatment photography: All other uses require the patient's consent, and the department needs to maintain the recorded consent for six years beyond date of last use. Even though you have consent or its use is allowed under HIPAA, it is always best practice to de-identity the photograph completely.

Other Federal Laws

In addition to HIPAA, there are other federal laws which govern the release of information, mandate that information be protected, and in some cases require that individuals be granted certain rights relative to control of and access of their information.

- The Medicare Conditions of Participation (CoP) require that hospitals promote each patient's rights, including privacy (42 CFR Section 482.13).
- The Federal Trade Commission charged with protecting consumers requires banking and other industries to implement "red flag" standards (12 CFR Part 681) to detect and prevent identity theft related to customer and service accounts. These red flag rules extend to health care institutions.
- The Family Education Rights and Privacy Act (FERPA) governs the protection of education records which include student health records (20 USC 1232g). HIPAA specifically exempts individually identifiable health information in education records. As FERPA records are exempt from HIPAA, all releases from education records must be in accordance with FERPA regulations.
- Federal Department of Health and Human Services as well as multiple federal agencies require the protection of the privacy and confidentiality of participants in research clinical trials.

California State Laws

California has multiple statutes and regulations which require the protection of the privacy of its residents' confidential information such as credit cards, social security numbers, personal identification numbers (PINs), as well as the protection of their medical and insurance information. Major state privacy laws include:

- Confidentiality of Medical Information Act (CMIA) (Civil Code Section 56 *et seq.*) requires:
 - that confidentiality of medical information be protected and establishes the protections against disclosures of individually identifiable medical information.
 - that institutions notify California residents of breaches of electronic social security number, access codes to financial accounts, medical and insurance information.
 - that healthcare institutions implement safeguards to protect the privacy and confidentiality of medical information and defines personal liability for breaches of privacy in which both individuals and institutions are liable for any unauthorized access, use, disclosure, or viewing of medical information. These laws impose various civil penalties against an individual such as personal fines, civil liability, licensure sanctions, and/or criminal sanctions.
- See also: Civil Code Sections 1785.11.2, 1798.29, 1798.82, Health & Safety Code Section 130200
- Health & Safety Code Section 1280.15 mandates that licensed clinics and health facilities report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information no later than 5 calendar days after the breach has been detected. The institution is to report to both the Department of Public Health and the affected patient(s).
- Lanterman-Petris-Short Act (LPS) (Welfare and Institutions Code Section 5328 *et seq.*) provides special confidentiality protections for medical records containing mental health or developmental disabilities information.
- Title 22, California Code of Regulations, Section 70707(b)(8), requires acute care hospitals to protect patient rights to the confidential treatment of all information related to their care and stay at the hospital.

Potential Consequences of Violating the State Privacy Laws

The California privacy laws impose administrative penalties and fines for non-compliance and for breaches of privacy which range from \$100 to \$250,000 per violation for both individuals and the University.

Frequently Asked Questions (FAQs)

What is the Privacy Office and what do they do?

The Privacy Office is responsible for monitoring compliance with the federal and state privacy laws and regulations. The Privacy Office is responsible for orchestrating departmental responses in the event of a breach of patient privacy. Additionally, the Privacy Office provides consultation on requests for all privacy related questions. The Privacy Office tracks and analyzes all privacy activities, and develops training and risk mitigation programs for the entire UCSF enterprise.

There has been a breach of patient privacy in my department. What do I do?

If the personally identifiable information was on a stolen device (computer, PDA, for example), immediately contact [UCSF Campus Police](#) (415-476-1414) to report the theft and if personal health information is involved, contact the Privacy Office (415-353-2750). The UCSF Campus Police will contact Enterprise Information Security (EIS). For disclosures not involving a stolen device, contact the Privacy Office immediately.

In every circumstance, you will need to provide the following information:

- Date and time breach was discovered

- Name of and contact information for person who discovered breach
- The specific patient information disclosed
- The number of patients who had their information disclosed
- How it happened
- Actions taken following detection
- The department contact for follow-up

The department is responsible, under the direction of the Privacy Office, for the follow-up including, but not limited to, the investigation, following up with patients, determining and implementing corrective steps and changes in process, following up with 3rd party vendors and mailing patient notification letters, as needed. Please Note: Only the Privacy Office can determine if notification is required.

The above information needs to be reported ASAP. Any delay in reporting the above information to the Privacy Office delays UCSF reporting to the state and to patients. Delayed reporting to the state and patients beyond the 5-day time frame exposes you and the University to financial liability in the way of administrative fines and penalties.

How do I know what HIPAA and privacy training people in my department should receive?

Refer to the [Education and Training](#) section of the Privacy Office website. Remember, all members of a department need to have some type of privacy training, including volunteers.

I want to provide a flyer to a specific patient population, produced by an outside organization (i.e., the American Heart Association). Can I do this?

You can post the flyer in the clinic waiting room for interested patients to take the training. Additionally, any mass mailings that go out to patients for fundraising purposes must be approved by the Development Office as there are certain restrictions related to the format of the mailings. Any use of the UCSF logo associated with another organization needs to be approved by Public Affairs (415-476-8252).

How much personal information can be released to family members over the phone?

According to the [Notice of Privacy Practice](#), you may release personal information to anyone that the patient has identified as the recipient of such information. Refer all others to the contact person the patient designates.

What is my responsibility related to the vendors that I bring into the Medical Center?

Before allowing vendors' access to the Medical Center, they need to check in with Material Services. Once this is complete, they should be wearing the Visitor ID at all times while in the Medical Center. Do not leave vendors alone in areas with PHI that they do not need to have access to i.e., clinic work areas. It is recommended that they wait in the waiting room.

My patient does not answer the phone directly. How can I leave a HIPAA compliant message with someone else or a voice mail?

Leave the minimum amount of information needed: your name, phone number and that you are from UCSF. A recommended best practice would be to obtain the patients preference for follow up or appointment communication at the initial point of contact.

My patient is now on another unit. Can I access his or her record?

If you do not have a legitimate need to access their record, then you should not access the record.

Can I email my patient related to his or her care?

You can do so but only by following the secure email guidelines on page 9 of this Handbook. Best practice includes making sure the patient prefers this form of communication and understands the risks associated with it.

How much information can I give an insurance company?

According to Notice of Privacy Practice, we may use and disclose medical information for the purpose of obtaining payment. Best practice is to only provide what is needed for this purpose. For example, providing lab values is not usually information that should be provided for billing purposes.

How much information can I give a Skilled Nursing Facility (SNF) or Home Health Agency (HHA)?

If the patient is being referred to either of these types of facilities, then you have a patient care need to disclose PHI. You should provide all PHI that you feel they need to know to provide continuity of safe patient care.

What information can be faxed?

Always send the minimum information necessary. Best practice is to confirm the correct fax number prior to sending, include a cover letter with a confidentiality statement and call to follow up on receipt.

Can I mail my patient's information?

If you have a patient care need to do so, yes. Best practice is to confirm the correct address with the patient prior to sending and make sure it does not have any other identifying information on the outside, other than UCSF.

Someone wants to come into a clinical area and observe. How can I make this happen?

There are a few forms that are required depending on the number of days of observation and/or whether the observer will interact with patients. Use the Matrix on the [Visitors and Observers](#) page on the Privacy Office website for guidance.

Our patients sign in on a clip board. Is that ok?

It is ok, if you are using a pull-off label system, so that patient names do not accumulate throughout the day for subsequent patients to view. Alternatively, you can use a thick black marker to cross off the name, so the next person cannot see the previous patients' names.

For white boards or marker boards, what information can be listed?

The use of last names and first initials on the board within the department is appropriate. In the operating room, first and last names are permitted for safety reasons. The important considerations are: whether the board is visible to passers-by and whether it contains PHI. If yes to both, consider whether there are other ways that the protected data (including demographic data) could be "reasonably" limited to the minimum necessary to allow the unit to safely manage patient care.

For additional FAQs, related to HIPAA please refer to the [U.S. Department of Health & Human Services HIPAA Frequent Questions](#).

UCSF RESOURCE LIST

<u>Department</u>	<u>Title</u>	<u>Phone</u>	<u>Websites</u>
Privacy and Confidentiality (HIPAA)			
Privacy Office	Chief Privacy Officer	353-2750	http://hipaa.ucsf.edu/default.html
Education and Training			
Human Resources (Medical Center)	Director	353-4688	http://hr.ucsfmedicalcenter.org/
Human Resources (Campus)	Director	476-1645	http://ucsfhr.ucsf.edu/
Technical & Security (Electronic/Physical)			
Information Technology Department (Medical Center)	Director, Infrastructure SVC	353-4474	http://it.ucsfmedicalcenter.org/
OAAIS-Enterprise Information Security (Campus)	Information Security Officer	502-1593	http://oaais.ucsf.edu/OAAIS/home.html
Business Associates			
Purchasing (Medical Center)	Manager	353-4675	N/A
Campus Procurement & Business Contracts (Campus)	Assistant Procurement Manager	502-3047	http://cpbc.ucsf.edu/
Research			
Human Research Protection Program	Director, HRPP	476-9840	http://www.research.ucsf.edu/CHR/HIPAA/chrHIPAA.asp
Medical Record Access and Control			
Health Information Management Services (HIMS)	Director	353-2885	http://hims.ucsfmedicalcenter.org/
Patient Services			
Patient Relations	Management Service Officer	353-1936	http://serviceexcellence.ucsfmedicalcenter.org/patient_relations/
Risk Management			
Risk Management (Medical Center)	Director	353-1842	http://rm.ucsfmedicalcenter.org/index.html
Risk Management & Insurance Services (Campus)	Director	476-2498	https://www.rmis.ucsf.edu/Default.aspx
Development			
University Development	Manager, Annual Giving	514-0508	http://www.ucsf.edu/support/givingOpportunities/index.html
Police			
UCSF Police Department	Chief of Police	476-1414	http://www.police.ucsf.edu/

APPENDIX 1

PHI Data Elements

1. Names
2. All geographic subdivisions smaller than a State, except for the initial three digits of the ZIP Code if the geographic unit formed by combining all ZIP Code with the same three initial digits contains more than 20,000 people
- *3. All elements of dates, except year, and all ages over 89 or elements indicative of such age
4. Telephone numbers
5. Fax number
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full-face photographs and any comparable images; and
- *18. Any other unique, identifying number, characteristic or code, except as permitted for re-identification in the Privacy Rule.

* Data elements that are allowed in a Limited Data Set.

APPENDIX 2

Resolution of the University of California Board of Regents: Academic Health Center Health Insurance Portability and Accountability Act (HIPAA) Compliance Program

May 16, 2002

The University's individual and institutional providers of health care recognize and respect a patient's expectation that the privacy and security of individual health information will be protected. The University is committed to implementing policies and practices that will enable it to reasonably and appropriately protect its patients' privacy while carrying out its mission of care, service, education, and research. Compliance with the mandates of The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and Security Regulations requires a thoughtful balance between the rights of the University's patients to privacy of their Protected Health Information, the patient's expectation that quality care will be delivered in a cost-effective and timely manner, and society's expectation that academic health centers will continue to teach and perform leading-edge research.

The Board of Regents recognizes and supports the efforts of the members of the University's System-wide Corporate Compliance Committee: Academic Health Center Taskforce to implement a HIPAA Compliance Program that will provide for compliance by developing, where appropriate, system-wide privacy and security policies; demonstrate a commitment and leadership across the organization to the principles embodied in HIPAA; minimize disruption to the care, research, and teaching missions of the University; and enhance patient confidence in the institutions that serve them.

APPENDIX 3

University of California, San Francisco Confidentiality of Patient, Employee & University Business Information Agreement

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 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 Policy 05.01.04 & 05.02.01, LPPI Policy, UCSF Policy 650-16 Minimum Security Standards, UC Personnel Policies PPSM 80, APM 160, applicable union agreement provisions, and UC Business and Finance Bulletin RMP 8.

Business and employee 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 and telephone number; medical information; birth date; citizenship; social security number; spouse/partner/relative's 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, or 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 sanctions, in addition to University disciplinary actions.

ACKNOWLEDGEMENT OF RESPONSIBILITY

I understand and acknowledge that: (Read each item)

- 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 the 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 the hearing 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.
- Because special protections by law 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 otherwise, used to identify HIV, a component of HIV, or antibodies or antigens to HIV, I will obtain such authorization for release when appropriate.
- I understand that my access to all University electronic information systems is subject to audit in accordance with University policy.
- It is my responsibility to follow safe computing guidelines. To this end, I agree not to share my Login or User ID and/or password with any other person. I am responsible for any potential breach of confidentiality resulting from access made to UCSF electronic information systems (including mobile devices) using my Login or User ID and password. If I believe someone else has used my Login or User ID and/or password, I will immediately report the use to the appropriate information technology department and request a new password.
- 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.
- 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 will be personally responsible**; and criminal sanctions.

I have read, understand and acknowledge all of the above **STATEMENT OF PRIVACY LAWS AND UNIVERSITY POLICY** and the **ACKNOWLEDGEMENT OF RESPONSIBILITY**:

Signature

Date

Print Name

UCSF Department

Employee Number or

Print UCSF Representative's Name

Non-UCSF Employee

UCSF Representative Signature