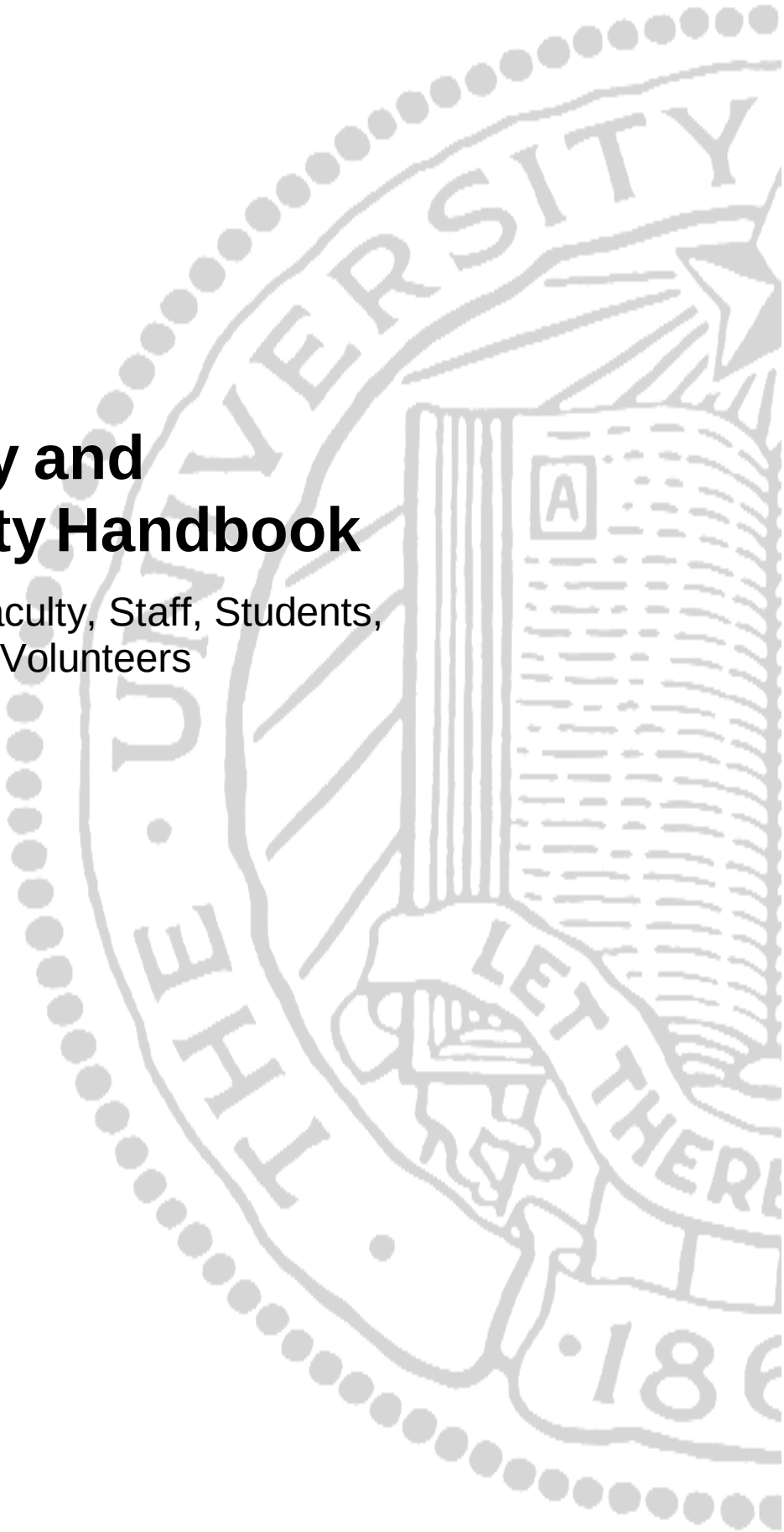
UCSF Privacy and Confidentiality Handbook

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



Revised June 2015

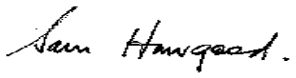
MESSAGE FROM THE CHANCELLOR ON BEHALF OF THE DEANS AND MEDICAL CENTER CHIEF EXECUTIVE OFFICER

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), the Health Information Technology for Economic and Clinical Health Act (HITECH), other Federal and California privacy laws, as well as UCOP and UCSF Policies and Medical Center Administrative Policies and Procedures.

These laws and regulations were promulgated and our policies established in order to protect the confidential personal, medical, and billing information of our patients, human research subjects, workforce, and students. Of particular importance are patients' rights related to access and control of their medical information, and newly enacted personal liability for non-compliance. 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 federal and state 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.



Sam Hawgood, MBBS
Chancellor
Arthur and Toni Rembe Rock Distinguished Professor

Special thanks to…

Privacy Compliance Steering Committee, Legal Affairs, Risk Management, Patient Relations, Health Information Management Services, Development and Alumni Relations, Research (HRPP), Information Technology Security and Policy, Marketing, Medical Center Information Technology Security, and University Relations.

Table of Contents

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), the Health Information Technology for Economic and Clinical Health Act (HITECH), other Federal and California privacy laws, as well as UCOP 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 job responsibilities at UCSF.

It is expected that all UCSF staff, faculty, students, and trainees understand that it is their legal and ethical responsibility to preserve and protect the privacy, confidentiality and security of all confidential information, both patient and non-patient related, in accordance with these laws, policies, and procedures.

All staff, faculty, students, and trainees are expected to access, use, and disclose confidential information only in the performance of their University duties or when required or permitted by law. Additionally, all staff, faculty, students, and trainees must disclose information only to persons who have the right to receive that information.

Please refer to www.hipaa.ucsf.edu for additional privacy educational resources.

HIPAA

Privacy and Confidentiality Overview

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, 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, health plans, their employees and other members of the covered entities’ workforce. HIPAA privacy and security standards were updated in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act and in 2013 by the HIPAA Final Omnibus Rule.

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 (PHI) should be controlled. Privacy standards define what information must be protected, who is authorized to access, use or disclose information, what processes must be in place to control the access, use, and disclosure of information, and patient rights.

The Security Rule defines the standards for covered entities’ basic security safeguards to protect electronic protected health information (ePHI). Security is the ability to control access to electronic information, and to protect it 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

The purpose of the Privacy Rule is 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, including electronic PHI (ePHI), by UCSF faculty, staff, students, trainees, vendors, and volunteers is based on the general principles of "need to know" and "minimum necessary," wherein access is limited only to the patient information needed to perform a job function.

The Privacy Rule also accords certain rights to patients, such as the right to request copies of their health records in paper or electronic format, or to request an amendment of information in their records.

Potential Consequences of Violating the Privacy Rule

The Privacy Rule imposes penalties for non-compliance and for breaches of privacy. These penalties range from $100 to $1,500,000 per violation, in addition to costs and attorneys' fees, depending on the type of violation. In addition to civil monetary penalties, other consequences may include civil lawsuits, misdemeanor charges, the reporting of individual violators to licensing boards for violations, and imprisonment.

WORKFORCE REQUIREMENTS

UCSF faculty, staff, students, trainees and volunteers are required to review this Handbook and sign the Privacy Confidentiality Statement (Appendix 3). The signed document must be stored in a centralized area in the department and/or Human Resources (HR) for a minimum of six years after the workforce member's last date of service.

UCSF workforce members, whether salaried or non-salaried, are required to complete HIPAA privacy and information security training. This includes faculty, staff, students, trainees, and volunteers, who may have either direct or indirect access to patients or their health information.
Additional training and documents may be required depending on the amount and purpose of contact with patients or protected health information. For guidance, please contact your Supervisor or see the Privacy Office website at http://hipaa.ucsf.edu/education/default.html.

PROTECTED HEALTH INFORMATION: DEFINITION AND RIGHTS TO ACCESS

What is considered protected health information (PHI)?

PHI is individually identifiable health information, in any form, about a past, present, or future physical or mental condition, which is created in the process of caring for the patient. Examples of individually identifiable information include patient name, address, date of birth, age, medical record number, phone number, fax number, and email address. Individually identifiable health information for a deceased patient is still considered PHI until 50 years after the patient's death, when it is no longer PHI.

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 without patient authorization. The de-identification standard provides two methods for which health information can be designated as de-identified. The first method requires the removal of all 18 identifying data elements listed in the regulations (see Appendix 1 for a list of the 18 data elements). If the resulting information cannot be used to identify the individual, then it is no longer PHI. The second method requires an expert to document their determination that the information is not individually identifiable ("Expert Determination").

What patient information must we protect?

We must protect all PHI including, but not limited to, medical records, diagnoses, x-rays, photos and images, recordings, prescriptions, specimens, lab work and other test results, billing records, claim data, referral authorizations, and explanation of benefits. Clinical research records of patient care must also be protected.

When can a Limited Data Set be used for research, public health, or health care operations?

A Limited Data Set (LDS) 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 (DUA) with UCSF. A Limited Data Set still includes some PHI that could potentially be used to identify an individual, and for that reason, it is not considered de-identified data. Certain geographic data (such as city, state, and zip code – but not street address), dates (such as birth, death, admission, discharge, and service), age, and unique identifiers (other than those listed in Appendix 1) may be included. A Limited Data Set may only be used for research, health care operations or public health purposes, and may not be used to re-identify or contact an individual. The "minimum necessary" standard applies to a Limited Data Set, just as it would to other PHI, however the requirement for Accounting of Disclosures of PHI does not apply when a LDS is disclosed. See CHR guidance at the CHR website (http://www.research.ucsf.edu/chr/) for research questions and immediately contact CHR, as well as the Privacy Office (415-353-2750), if you suspect or know of any violations of a DUA.

Who is authorized to access confidential PHI?

PHI may be accessed without patient consent under certain circumstances and for certain purposes, which are further described in the UCSF "Notice of Privacy Practices." Three of these purposes – Treatment, Payment and health care Operations (TPO) – are the most common:

- **Treatment** of the patient, including appointment reminders.
  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.
- **Payment** of health care bills, including claim submission, authorizations, and payment posting.
- **Operations**, including teaching, medical staff quality activities, research (when approved by the Institutional Review Board and with a patient's written consent and authorization, or with a "waiver of authorization"), health care communications between a patient and their physician, patient inclusion in the hospital directory, and other uses.

When can students and trainees access PHI?

Students and trainees in UCSF and affiliated training programs may have access to PHI. Prior to accessing PHI however, students and trainees are required to complete a privacy orientation or training and to sign the UCSF Confidentiality Statement. Students and trainees are not permitted to remove any PHI from UCSF premises.

When PHI is used for educational purposes only (as opposed to use in clinical settings) students and trainees must de-identify the information in accordance with guidance in this Handbook (see "What is not considered PHI" section on page 9).

What is the "minimum necessary" standard?

The minimum necessary standard in the Privacy Rule requires that when a covered entity uses or discloses PHI or requests PHI from another covered entity, it must make reasonable efforts to limit PHI to that which is necessary to accomplish the intended purpose of the use, disclosure, or request. As a UCSF workforce member, you are expected to apply the minimum necessary standard when you access, use, or disclose 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. Similarly, 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 written patient authorizations required?

To use or disclose PHI for almost any reason other than T-P-O, including research and fundraising, you will need to obtain a written authorization from the patient prior to access, use, or disclosure. For releases from the medical record, the signed authorization must be placed in the patient's medical record. Refer to the "Notice of Privacy Practices" (see http://hipaa.ucsf.edu) for a list of exceptions to the authorization requirement related to public health, certain health disease reporting requirements, and law enforcement activities. If you still have questions, ask your supervisor or department chair, or the Privacy Office 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. Immediately report concerns to your supervisor or the UCSF Privacy Office (415-353-2750). Refer to the resource list on page 28 for a list of individuals to contact with specific questions about HIPAA privacy and security.

LEGAL MEDICAL RECORD ACCESS AND CONTROL

Medical records are maintained for the benefit of the patient, medical staff, and the hospital, and shall be made available to any of the following persons or departments upon request:

- Treating physicians
- Non-physicians involved with the patient's direct care (e.g., nurses, pharmacists)
- Any authorized officer, agent, or employee of the Medical Center or its Medical Staff (e.g., Risk Management, Patient Relations)
- UCSF researchers as part of an approved Committee for Human Research (CHR) protocol that involves medical record review
- Any other persons authorized by law to make such a request (e.g., medical examiners, law enforcement, regulatory agencies)
- Patients or their authorized representatives

At UCSF, the appropriate medical records department, such as UCSF Medical Center's 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.

HIMS may also release records in response to a:

- Subpoena
- Court order
- Statute

PATIENT 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 the "Notice of Privacy Practices"**
  Patients have the 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 to Paper or Electronic Copies**
  Patients may request to inspect their medical record and may request paper or electronic copies.
- **Right to Request an Amendment or Addendum**
  Patients may request either or an amendment or an addendum to their medical record.
- **Right to an Accounting of Disclosures**
  Patients have the right to receive an "Accounting of Disclosures," which documents those disclosures of patient medical information for which the patient has not authorized.
- **Right to Request Restrictions**
  Patients have the right to request restrictions on how UCSF will communicate with the patient and how it will the patient's release health information. When a patient pays in full for a UCSF service, and requests a restriction of release of information to their health plan, UCSF must honor their request.
- **Right to Request Confidential Communications**
  Patients have the right to request that UCSF send confidential communications to them in a specific method and manner.
- **Right to Complain**
  Patients have the right to complain if they think that their 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, or the appropriate medical records department, such as UCSF Medical Center's Health Information Management Services (HIMS).

Facility Patient Directories (In-patients)

UCSF may use and disclose selected PHI, which includes name, location in the hospital, general 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. Patients may opt out of the facility

patient directory, in which case UCSF will not provide this information to requesting individuals. If a patient requests to opt-out of the facility directory, refer the request to the Admitting Department.

Criteria for Release of Information by Provider to Patient

Best practice is to use the central medical records department, such as UCSF Medical Center's Health Information Management Services (HIMS) system for releases of information, however there are certain circumstances in which the provider may use their professional judgment to release certain specific information directly to the patient (e.g. when reviewing specific test results or when the patient needs a copy of the Procedure Report for an urgent appointment with their MD the next morning). Under these limited circumstances, the provider must either have the patient sign a release of information form and place it in the patient's Medical Record, or document in the Medical Record (such as Quick Disclose in APeX) that the patient has been provided with the information. For unique circumstances, professional judgment can be utilized.

Authorization for Release of a Patient's PHI

HIPAA specifies the content of an authorization to disclose PHI. At UCSF, the authorization process is managed by the appropriate medical records department, such as UCSF Medical Center's Health Information Management Services (HIMS). Other than a few narrow exceptions, a written authorization from the patient (or the patient's personal representative) is required to disclose or access PHI for uses other than treatment, payment, or healthcare operations.

- Special authorization is required to access any information pertaining to drug and alcohol abuse, mental health diagnosis or treatment (psychotherapy record), HIV/AIDS test results, and genetic testing.
- An authorization is needed from a patient before any PHI can be released to a UC Department that is not part of the Covered Entity (or that serves a business associate function).
- 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."

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 for public health and safety purposes, government functions, and law enforcement, as well as those based on a judicial request or subpoena, or subject to professional judgment.

Psychotherapy notes require special handling and authorizations. All requests for psychotherapy notes must be routed to the appropriate medical records department, such as UCSF Medical Center's Health Information Management Services (HIMS) or Langley Porter Psychiatric Hospital and Clinics' HIMS department.

PHI may be used for research, fundraising, public information, or health care communications, 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 the appropriate medical records department, such as UCSF Medical Center's Health Information Management Services (HIMS).

When a Patient is Unable to Authorize the Release of Their PHI

If a request for PHI is made by the patient's spouse, parent, child, sibling, or other family member or friend, and the patient is unable to authorize the release of such information, UCSF may give notification of the patient's

presence in the hospital, to the extent allowable 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 the patient's admission. In addition, upon request of a family member only, UCSF may release information about the patient's discharge, transfer, serious illness, injury, or death, unless the patient requests that this information not be provided.

Best practice is to use the central medical records department, such as UCSF Medical Center's Health Information Management Services (HIMS) system for releases of information, however there are certain circumstances in which the provider may use their professional judgment to release certain specific information directly to the patient (e.g. when reviewing specific test results or when the patient needs a copy of the Procedure Report for an urgent appointment with their MD the next morning). Under these limited circumstances, the provider must either have the patient sign a release of information form and place it in the patient's Medical Record, or document in the Medical Record (such as Quick Disclose in APeX) that the patient has been provided with the information. For unique circumstances, professional judgment can be utilized.

BUSINESS ASSOCIATES

A vendor or third party that engages in a function or activity involving the use, access or disclosure of UCSF's patients' 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. The Final Omnibus Rule extends the definition of a BA to include, "one that creates, receives, maintains, or transmits" PHI on behalf of the Covered Entity (CE). The BAA sets forth, in part, the business associate's obligations related to the privacy and security requirements. UCOP has created a standard BAA for the campuses to use for this purpose.

A function or activity involving the use, access or disclosure of individually identifiable health information includes the following:

- Claims processing or administration
- Data analysis, processing, or administration
- Utilization review
- Quality assurance, billing, benefits management, practice management, and re-pricing activities
- Legal activities
- Actuarial activities
- Accounting
- Data aggregation
- Management
- Health Information Organizations
- E-prescribing gateways
- Patient Safety Organizations
- Data storage vendors that maintain PHI, even if access to PHI is limited or non-existent (e.g. carbonate, cloud storage).

Maintenance Services on an Information System or when the vendor will have remote access. This is not an all-inclusive list. For all vendor or third-party relationships that involve patients' individually identifiable health information, or if you are unsure whether the third-party vendor is subject to HIPAA, please contact UCSF Medical Center Purchasing (415-353-4675) or UCSF Campus Procurement and Contracting (415- 476-5761).

CLINICAL AND OTHER RESEARCH INVOLVING HUMAN SUBJECTS

Committee for Human Research (CHR) review is required for all human subject research, including the use of human specimens, information from medical records and databases, and 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 disclose individually identifiable health information if they obtain the appropriate authorizations and approvals for research, which include both of the following:

- CHR approval for research
- Patient authorization for release of medical information for research purposes, and/or a CHR approved Waiver of Authorization

CHR Application

In order to obtain CHR approval for research access to, 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 on the HRPP web site at http://www.research.ucsf.edu/chr/index.asp.

Authorization and Waiver of Authorization

Access to medical records or clinical data systems for recruitment purposes and chart review must meet the Privacy Rule requirements for appropriate research authorization. At UCSF, the appropriate medical records department, such as UCSF Medical Center's Health Information Management Services (HIMS) or the Integrated Data Repository (IDR) controls the release of medical records for chart review or access to medical information and will require both of the following:

- CHR approval for research
- Patient authorization for release of medical information for research purposes, and/or a CHR approved Waiver of Authorization

Refer to UCSF Medical Center Policy 5.01.06, "Control of Access to and Release of Information from UCSF Medical Center Information Systems" for the process of requesting PHI from UCSF Medical Center information systems.

De-Identified Information

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 does not qualify as PHI and, therefore, is not subject to the Privacy Rule. Note: In order to render PHI de-identified, ALL of the 18 HIPAA identifiers (refer to Appendix 1) must be removed. A CHR application will be needed if researchers wish to access identifiable medical information.

Protection of Information

All research investigators are responsible for all aspects of their research study, including adherence to policies and procedures for the protection of privacy and confidentiality of identifiable medical information. Investigators must take appropriate steps, including the usage and storage of research data in a manner that ensures physical and electronic security (e.g., data encryption). Data Use Agreements or Business Associate Agreements may be required to allow for sharing data with parties external to UCSF. The UCSF Integrated Data Repository (IDR) MyResearch space can provide researchers with a secure environment to store and analyze their data. (Link for MyReseach: http://it.ucsf.edu/services/myresearch).

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 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

Purpose of Security Rule

The Security Rule encompasses physical, administrative, and technical security, including computer systems and electronic transmissions of information. The rule's purpose is to:

- Ensure the confidentiality, integrity, and availability of all PHI that is created, received, maintained, or transmitted by the covered entity.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.
- Protect against unauthorized uses or disclosures of PHI.
- Ensure compliance of the covered entity's workforce.

Definition of Security

Security is defined as having controls, countermeasures, and procedures in place to ensure the appropriate protection of information assets, and to control access to valued resources. The purpose of security is to minimize the vulnerability of assets and resources.

Requirements and Responsibility for Security

UCSF is required to secure all access to stored and transmitted PHI.

The UCSF IT Security department is responsible for establishing security policies, procedures, and systems that protect University systems from electronic threats and vulnerabilities.

Workforce members are responsible for protecting all of UCSF's electronic information resources that they have under their control by employing appropriate and applicable security controls. Protection of UCSF electronic information resources encompasses:

- Safeguarding PHI from accidental or intentional disclosure to unauthorized persons.

- Safeguarding PHI from accidental or intentional alteration, destruction, or loss.
- Safeguarding systems from viruses and malware.
- Taking precautions that will minimize the potential for theft, destruction, or any type of loss.
- Protecting workstations and mobile devices from unauthorized access and theft (e.g., via encryption, password authenticated access and physical lockdown) to ensure that ePHI is accessed, used, and/or disclosed only by authorized persons.
- Protecting other electronic assets and storage media (e.g., USB thumb drives, external hard drives, CD-ROM/DVD disks, floppy disks, magnetic tapes, videotapes, SD memory cards, etc.) from unauthorized access and theft, to ensure that ePHI contained within is accessed, used, and/or disclosed only by authorized persons.

HOW TO COMPLY WITH THE SECURITY RULE

There are several steps that you must take to protect the privacy and electronic security of PHI. The most critical are listed below; for further instructions, or if you have questions, contact IT Security or the Privacy Office.

Hard Copy PHI

PHI must be protected from accidental loss or theft regardless of the format/media of the data. Refrain from taking hard copy PHI off-site (e.g., home, transport to another UCSF campus). However, if you absolutely must take PHI off-site, de-identify the information as much as possible and never leave the documents unattended. For example, the following are not acceptable means of protection:

- Locking documents with UCSF data in a car or car trunk
- Leaving documents in an unattended bag in a public place (regardless of length of time)

Mobile Computing Devices

”Mobile computing device” has a broad definition and includes all devices and media capable of storing data in electronic format such as laptops, cell phones, iPhones, iPads, Android devices, iPods, memory cards, flash drives, external hard drives, and digital cameras.

Follow the following guidance when working with mobile computing devices:

- Protect all mobile computing devices containing PHI with an approved UCSF data encryption solution. For laptops, hard drives, and flash drives, use encryption, and for smartphones and tablets, use encryption, a PIN lock, and remote wipe. Contact the IT Service Desk at 415-514-4100 for questions regarding encryption and/or using a PIN lock and remote wipe on your device.
- Store the minimum amount of ePHI necessary on mobile computing devices.
- Connect all smartphones and tablets devices used for UCSF business via ActiveSync to the UCSF Exchange email server (see: http://it.ucsf.edu/services/email-mobile-access).
- Never leave devices unattended in an exposed or unsecured area.
- Utilize physical locks for laptops and other mobile computing devices.
- Keep mobile computing devices up-to-date with current operating system security patches and anti-virus software.
- Ensure that the mobile computing device meets UCSF Minimum Security Standards (see http://tiny.ucsf.edu/mss).

- Frequently backup data to a UCSF-controlled server. UCSF IT has a back-up solution to make this effort easy and secure for you.
- Use caution when uploading or downloading files to or from mobile computing devices. Adhere to the "minimum necessary" standard and never transfer ePHI over a network without using encryption.
- Use the virtual private network (see: https://vpn.ucsf.edu) for off-site work. Public WiFi hotspots may not employ proper security controls and may allow your connection and your data to be compromised.
- Download and install applications only from trusted sources. Applications may have the potential to intercept and/or read data on your device. Be cognizant about the requested rights that some applications ask for during installation. Do not "jailbreak" or make any attempt to gain elevated privileges on mobile computing devices as this may weaken the security of the device and expose ePHI.
- Immediately report lost or stolen devices to the UCSF Police Department by filing a police report at 415-476-1414 and notifying UCSF IT Security Department at 415-514-4100.

Password Security

Having a secure password in place is essential to keeping UCSF systems protected. Adhere to the following guidelines for password security:

- Always keep computers password-protected.
- Protect your user ID and password. Commit your password to memory or use an appropriate secure password management solution. Do not share, write down, or post your password under any circumstances!
- Incorporate a combination of letters, numbers and special characters into your password. Avoid dictionary words, personal information, common terms, sport teams, etc. when creating your password. Learn how to select good passwords at https://it.ucsf.edu/policies/how-choose-password.
- Immediately change your password if it is accidentally exposed or compromised.
- Report all password exposures to your department supervisor or manager, and the UCSF IT Service Desk (415-514-4100).
- Adhere to established password management standards. (https://it.ucsf.edu/policies/unified-ucsf-enterprise-password-standard-0).

Workstation Security

At UCSF, workstations are often in areas that are accessible to the public so it is important that you take the following precautions to prevent the unauthorized release of PHI:

- Log off or lock access to computers when you leave, even if only for a moment.
- Ensure that computer screens and displays with access to ePHI are not visible to unauthorized individuals or passersby.
- Lock confidential or sensitive information away when not in use. File documents in locked cabinets or drawers when you have finished with them.
- Be cognizant of your environment.

Disposal and Destruction

The information lifecycle does not end, and the risk of unauthorized access, use, or disclosure is not eliminated, until the information disposed of or destroyed. Therefore, you must destroy all PHI as soon as it is no longer needed. To properly dispose PHI follow these guidelines:

- Securely dispose of all papers that contain PHI. ALWAYS follow the proper paper disposal procedure (e.g., use secure bags, cross-cut shredders, locked 'Shred-It' disposal bins located throughout UCSF,

etc.). Never leave sensitive or confidential information in a trash bin.

- Back up data files to UCSF servers, and follow approved UCSF media destruction procedures before disposing of devices.
- Remove hard drives or other storage media from computers or equipment prior to retiring devices, and ensure they are properly disposed of. Refer to https://it.ucsf.edu/services/drive-tape-and-data-destruction, or contact the IT Service Desk for guidance (415-514-4100). Maintain records to track the movement (transfer or relocation) of devices and media.

Access and Identification

Unauthorized visitors pose a risk to UCSF from both a security and confidentiality standpoint. Visitors at UCSF are controlled in a number of ways including security checkpoints, locked doors, and ID badges. To prevent unauthorized visitors to your work area follow these best practices:

- Always follow established visitor and observer security guidelines and procedures.
- Always wear your security badge or identity badge while at work.
- If you suspect that an unauthorized individual is in a protected area or accessing protected information, ask them to identify themselves. Alert your Supervisor and contact Security (415- 885-7890).

SECURITY OF COMMUNICATIONS CONTAINING PHI

Email

When transmitting UCSF ePHI via email, only use your UCSF email. Do not use other email systems (e.g., Gmail, Yahoo, etc.) as they may not be secure. When first setting up your UCSF email, add a Confidentiality Notice footer to your messages, such as:

***CONFIDENTIALITY NOTICE** This e-mail communication and any attachments are for the sole use of the intended recipient and may contain information that is confidential and privileged under state and federal privacy laws. If you received this e-mail in error, be aware that any unauthorized use, disclosure, copying, or distribution is strictly prohibited. If you received this e-mail in error, please contact the sender immediately and destroy/delete all copies of this message.*

Email communications with patients should be conducted via UCSF MyChart wherever possible, as it is secure and the communications are centrally stored in the patient's APeX medical record. Patients can also see many of their lab test results, request appointments and medication refills, and use other services. To have your patients sign up, please email ucsfmychart@ucsfmedctr.org

To send other confidential email containing ePHI or other sensitive content use UCSF's Secure Messenger service (https://it.ucsf.edu/services/secure-email). To "trigger" email security, the subject line must begin with either "ePHI", "PHI", or "Secure", directly followed by a colon. Capitalization of the trigger words and the use of a space after the colon are optional. Examples of appropriate email subject lines that will trigger a secure email are:

- ePHI: UCSF Financials
- PHI: UCSF Financials
- Secure: UCSF Financials

Even when using the secure email system, be sure you are adhering to the following rules:

- Do not include actual PHI in the subject line (e.g. MRNs or patient names) – use only patient initials.

- Be careful what you send via email. Do not send confidential information unless absolutely necessary. De-identify the information if possible.
- 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.
- Do not send attachments containing ePHI without encryption.

If you identify PHI that was sent in error, contact the sender. Do not extend the breach of information by forwarding the identified ePHI to others. Securely dispose of or destroy the information after alerting the sender. If you are notified that you sent an email containing PHI to the wrong recipient, obtain written attestation that the recipient destroyed all copies and did not use or disclose the information. Immediately contact the Privacy Office for next steps.

Fax

While a large percentage of communication occurs over phone or email, a substantial amount still occurs through fax. When faxing documents containing PHI use a cover sheet containing a confidentiality statement, such as:

CONFIDENTIALITY NOTICE: This communication and any attachments are for the sole use of the intended recipient and may contain information that is confidential and privileged under state and federal privacy laws. If you received this fax in error, be aware that any unauthorized use, disclosure, copying, or distribution is strictly prohibited. If you have received this fax in error, please contact the sender immediately and destroy all copies of this message.

Prior to faxing a document always check the destination fax number as recipients may have changed locations. Also, call ahead to ensure that the intended recipient is near the fax machine and will pick-up the document when it arrives.

If you are alerted that you sent a fax containing PHI to an incorrect recipient immediately notify the Privacy Office and get a confirmation from the recipient that they have not further used or disclosed the information they received and have destroyed the document. If you receive a fax that is not meant for you, alert the sender immediately.

Voice Mail / Answering Machines / Telephone Communications / Video Conferencing

When making phone calls identify all of the participants on the other end of the line, limit the amount of PHI needed for the conversation and keep the volume of your voice at an appropriate level so that your conversation cannot be overheard. When talking on a speakerphone, be aware of your surroundings, close the door, lower the volume, and consider picking up the handset.

Do not leave any PHI or sensitive information in voicemails – instead simply identify yourself and ask that the patient call you back. Also, consider who has access to your voice mail or answering machine so others do not access that PHI.

When leading or participating in video conferencing, be aware of your surroundings and make sure you know your audience. You may broadcast images to unintended participants.

If you intend to record the conversation or video conference, ask before recording. California is a two-party state (both parties are required to acknowledge the recording before starting).

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)

Marketing

Use of PHI for marketing purposes as defined by HIPAA will require the patient's prior written authorization. This includes use of photos as well as patient stories. While the majority of UCSF marketing communications do not involve financial remuneration, the Final Omnibus Rule further clarifies that if they do, patient authorization is required, even if for purposes of treatment or health care operations. 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, contact the Director of Marketing (415- 353-2716). To help ensure compliance with both PHI and marketing guidelines, departments producing documents for external use are strongly encouraged to contact the Marketing Department in advance of production.

Fundraising

Although HIPAA and CMIA do not prohibit fundraising efforts that target patients, UCSF policy (Administrative Policy 450-10) strictly prohibits the use of Protected Health Information (PHI) without a written Authorization for Fundraising (opt-in). UCSF may only use demographic information, physician, department of service, and outcome information for fundraising communications. A patient's demographic information is defined as name, date of birth, gender, ethnicity, insurance status, address and other contact information.

It is necessary to secure an Authorization for Fundraising from a patient when PHI is used or disclosed for fundraising purposes. Only the patient's health care provider may request that the patient sign the authorization. After this initial request, a staff member may complete the process. Authorizations for Fundraising must be forwarded immediately to University Development and Alumni Relations (UDAR). UDAR is the office of record for fundraising opt-ins and opt-outs.

All fundraising efforts must be coordinated through UDAR and must be HIPAA compliant. Examples of fundraising efforts include individual gift solicitations, fundraising event invitations, and endowed chair campaigns. All fundraising mailing lists must be vetted against the UDAR opt-out database prior to mailing. Please call (415-476-6922) 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 UCSF, please contact: Records Manager, UCSF, Box 0248, San Francisco, CA 94143-0248 or email HIPAAOptOut@support.ucsf.edu or call 1-888-804-4722."

The address shown in the above opt-out statement should not be altered, as this is the UCSF office of record for opt-outs, Opt-outs received via phone, email, or personal contact by UCSF staff 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. Reporters, photographers, camera crews, and other media representatives cannot be in clinical areas without supervision from News service staff. Any inquiries from reporters, photographers, or other media representatives should be referred to the News Office (415-476-2557), which is covered 24/7, (every day, including 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 urgent inquiries and other situations that involve communication to the media.

Photography

Photography for treatment and safety purposes: Every patient must sign the Terms and Conditions (T & C consent) of Admission document in order to obtain treatment at UCSF. This document allows photography of patients only for the purposes of treatment and safety. 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. However, photography of a patient for use in a patient services brochure would not be covered by the T & C Consent.

Photography for all other purposes: All other photo uses require the patient's consent, and the department needs to maintain the recorded consent for ten years beyond date of last use. Even if patient consent is obtained and use of the photo is allowed under HIPAA, it is always best practice to de-identity all patient images completely. To locate the proper consent form for the intended use refer to http://communicators.ucsf.edu/resources/#media.

Storage devices for photos, such as camera flash cards, CF cards, and smart phones, should use encryption when possible. If encryption is not available, the photo should be transferred to a secure location as soon as practically possible and then deleted from the storage device. For any questions on the storage, transfer, or deletion of images, please contact IT Security.

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 the control of and access to their information.

Family Education Rights and Privacy Act (FERPA)

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.

Health Information Technology for Economic and Clinical Health Act (HITECH)

The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 (42 CFR Parts 412, 413, 422 and 495, and 45 CFR Subtitle A Subchapter D) widened the scope of privacy and security protections required under HIPAA to address such things as business associate services and marketing activities, widened and increased the potential liabilities and consequences for non-compliance including civil and criminal penalties and fines, and provides for enhanced enforcement of the Privacy and Security Rules.

Final Omnibus Rule

The Final Omnibus Rule (45 CFR Parts 160 and 164) greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law. It implements a number of provisions of HITECH to strengthen the privacy and security protections for health information established under HIPAA. It also extends responsibilities to Business Associates, clarifies self-pay restrictions, further defines marketing and fundraising activities, and more.

The Genetic Information Nondiscrimination Act of 2008 (GINA)

This Federal law prevents employers and health insurers from discriminating based on genetic information.

Medicare Conditions of Participation (CoP)

The Medicare Conditions of Participation (CoP) require that hospitals promote each patient's rights, including privacy (42 CFR Section 482.13).

Red Flag Rule

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.

U.S. Department of Health and Human Services

The U.S. Department of Health and Human Services, along with other federal agencies, has established guidelines and requirements to protect the privacy of clinical research trial participants.

Common Rule

The Common Rule is a federal policy regarding human subject protection that applies to 17 Federal agencies and offices, one of which includes the Department of Health and Human Services. The main elements of the Common Rule include:

- Requirements for assuring compliance by research institutions
- Requirements for researchers' obtaining and documenting informed consent
- Requirements for Institutional Review Board (IRB) membership, function, operations, review of research, and record keeping.

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, and personal identification numbers (PINs), as well as medical and insurance information. Major state privacy laws include:

California Health and Safety Code Section 1280.15

The California Health and Safety Code Section 1280.15 mandates that licensed facilities report any unlawful or unauthorized access, use, or disclosure of a patient's medical information no later than 15 business days after the breach has been detected. The institution is to report to both the Department of Public Health and the affected patient(s). See also California Health and Safety Code Section 130200. However, at UCSF it is policy that you report any known or suspected privacy breaches immediately.

California Information Practices Act (Civil Code Section 1798)

Codifies right to privacy as a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy of information pertaining to them; for example, names, social security numbers, physical description, home address, home telephone number, education, financial matters, and medical or employment history.

Confidentiality of Medical Information Act (CMIA)

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.
- Health care institutions notify California residents of breaches of electronic social security number, access codes to financial accounts, and medical and insurance information.
- Health care institutions implement safeguards to protect the privacy and confidentiality of medical information and define personal liability for breaches of privacy.

These laws establish that individuals, not just institutions, are liable for any unauthorized access, use, disclosure, or viewing of medical information, and impose various civil penalties against an individual such as personal fines, civil liability, licensure sanctions, and/or criminal penalties. (See California Civil Code Sections 1785.11.2, 1798.29, and 1798.82).

Lanterman-Petris-Short Act (LPS)

The 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

Title 22, California Code of Regulations, Section 70707(b)(8), requires acute care hospitals to protect patients' rights for 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. If you have any questions, you should contact the Privacy Office (415-353-2750).

FREQUENTLY ASKED QUESTIONS (FAQs)

What is the Privacy Office and what do they do?

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

When is it OK to share PHI?

While it's prudent to be cautious about sharing and releasing PHI, it's also important to remember that HIPAA allows for the exchange of PHI with patient authorization and for certain purposes – namely **treatment, payment, and operations ("TPO").** The HIPAA Privacy Rule is intended to protect patients' health information, but not to impede or interfere with patient care or safety. Thus, HIPAA permits uses and disclosures of PHI as needed to provide quick, effective, and high quality healthcare; to bill and receive payment for healthcare services; and to conduct healthcare operations.

Examples of permissible **treatment** related uses and disclosures include:

- Sharing PHI with the ambulance while the patient is in transport to UCSF.
- Consulting with the patient's other healthcare providers.
- Providing PHI when referring or transferring a patient to a laboratory, nursing home, or outside provider or hospital.
- Sharing patient information with other UCSF workforce members involved in the patient's care.
- Discussing the patient's condition or treatment regimen in the patient's semi-private room.
- Providing therapy to patients in group settings.

Examples of permissible **payment** related uses and disclosures include:

- Determining eligibility, reviewing services, and adjudicating claims.
- All billing and collection activities, including those of another provider or Covered Entity for its treatment of the patient.
- Utilization review.
- Speaking with the patient's guardian or representative regarding bill payment.

Examples of permissible **operations** related uses and disclosures include:

- Case management and care coordination.
- Quality assessments.
- Accreditation, certification, licensing, and credentialing.
- Legal, audit, privacy, compliance.
- Business planning and development.
- Administrative activities, including customer service, employee relations activities, transfer of assets, and fundraising.
- Education and training programs.
- Abuse and neglect investigations.

If you're unsure about whether a scenario is considered TPO, simply contact your Manager or the Privacy Office for guidance.

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

Notify the Privacy Office as soon as you discover the incident (see instructions below). California law allows for a very short period of time in which to notify affected patients, as well as applicable regulatory agencies, of data breaches. Failure to notify both the patient and the regulatory agencies within the allowed time results in penalties for UCSF, and potentially the person who discovered the breach and failed to notify the Privacy Office in a timely manner. Therefore it is important that you notify the Privacy Office of the incident as soon as possible.

You will not be penalized for good faith reporting of a potential breach. If you believe that you are being treated unfairly as a result of making a report, report this to the Compliance Hotline at (415) 502-8448.

The Privacy Office will aid the department to conduct the investigation, draft and send patient notification and follow-ups, determine and implement corrective actions and changes in process, follow-up with third party vendors, retrain personnel, document the event, and other required actions. However, the responsibility of

responding to an incident (e.g., speaking with/notifying the patient(s), contacting individuals' to confirm facts) remains with the department in which the incident occurred. Please note though, that only the Privacy Office can determine if notification is required.

If the compromised information was stolen, or was on a stolen device (laptop, smartphone, tablet, for example), immediately contact UCSF Campus Police (415-476-1414) and the UCSF Privacy Office (415-353-2750) to report the theft. The UCSF Campus Police will contact Information Technology Security (ITS). For disclosures not involving a stolen device, contact the Privacy Office.

Be prepared to provide the following information (if you don't have all of the information below, you may provide preliminary information to the Privacy Office):

- Date and time the breach was discovered
- Name and contact information of the person who discovered the breach
- Nature of information involved
- Number of individuals who had their information disclosed
- How the breach happened
- Actions taken following detection
- Department contact information for follow-up

For Medical Center-related privacy incidents, how do I file an incident report (IR)?

The Incident Reporting system, RLSolutions, tracks all Medical Center-related patient adverse events (whether actual or near miss). To file an IR click on the "Incident Reporting" link in UCSF's CareLinks page, which can be accessed from any UCSF Medical Center computer by typing "carelinks" into the address bar in Internet Explorer. After logging-in using your UCSF username and password you will be directed to a website with icons for reporting a variety of incidents. Choose the "Confidentiality/Healthcare Information" (green icon) income and fill in the following information:

- Date and time the breach was discovered
- Name and contact information of the person who discovered the breach
- The specific information lost, misplaced, stolen, or disclosed
- The number of individuals affected by the incident
- How the breach happened
- Actions taken following detection of the incident
- The department contact for follow-up

How do I know what privacy and security training I should complete or should be provided to the people in my department?

Refer to the Education and Training section of the Privacy Office website. Remember, all members (including volunteers) of a department need to have some type of privacy and security training and all training must be documented. Training includes:

- Modules
- Privacy and Confidentiality Handbook
- Confidentiality Statement

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

You can post the flyer in the clinic waiting room for interested patients. Any mass mailings that go out to patients for fundraising purposes must follow the established UCSF process and be approved by UDAR as there are certain restrictions and required inclusions. Refer to UCSF Policy 450-10 "Authority to Solicit Gifts and Private Gifts". Any use of the UCSF logo associated with another organization needs to be approved by University Relations (415-476-8252).

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

According to UCSF's Notice of Privacy Practices, you may release personal information to anyone that the patient has identified as an authorized recipient of such information. Refer all other people to the contact person (or people) the patient designates. In all other cases, or if no contact person exists, you may not release any information other than "directory information." Directory information is whether or not the patient is in the hospital and his or her general condition (e.g., good, fair, critical), so long as the patient has not opted out of the directory. For requests of information over the phone have the requestor provide the patient's full name, verify the requestor's identity and relationship to the patient, and only supply the minimum amount of information necessary.

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

Before allowing vendors access to the Medical Center, they must check in with Material Services. Once this is complete, they should be wearing a 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 or in a designated conference room.

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

Guidelines have been developed by HR, Risk Management, and Privacy to ensure the consistent and appropriate handling of visitors and observers. Various forms, screenings, badges, and/or orientations may be required based on the number of days of observation, the type of observation, and/or whether the observer will interact with patients. Refer to the Privacy Office website at http://hipaa.ucsf.edu/education/visitors for more information. Questions and requests for guidance should be directed to Privacy, Risk Management, Occupational Health, and/or Human Resources.

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. Do not state what department you are calling from or what you are calling about; just ask that the patient call you back.

A recommended best practice would be to obtain the patient's preference for follow up or appointment communication at the initial point of contact (e.g., preferred phone number and whether UCSF may leave a detailed message on that voicemail).

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

You may access the patient's record only if you have a legitimate need to do so (for treatment, payment, or health care operations). Otherwise, you should not access the record.

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

For Medical Center patients, the preferred method of patient electronic communication is via APeX MyChart. If the patient does not want to communicate via MyChart, or for non-Medical Center patients that wish to communicate via email, you may email their personal health information via secure, encrypted email. Refer to the IT website for more information about secure email.

However, if the patient does not want to communicate via secure email, you may send them unencrypted emails only after meeting the following:

- **Notify** the patient of the risks of sending unencrypted email. Consider using the following standard language to notify patients of the risks of sending unencrypted email: "*While UCSF strives to communicate with patients in a secure manner, UCSF cannot guarantee secure delivery of email transmissions sent outside of the UCSF MyChart system and the UCSF Secure Email system, and the unencrypted information in the email could be read by a third party. Should you still wish for your correspondence with UCSF to be sent in an unencrypted format, we will honor your request.*"
- If the patient still prefers unencrypted email, **document** that in the patient's record

How much information may I give an insurance company?

According to the Notice of Privacy Practice, we may use and disclose medical information for the purpose of obtaining payment. This means that you should only provide what is needed for payment purposes. For example, if you are talking to an insurer about a lab test, you may need to state the type of test that was performed. However, the lab values are not required for billing purposes, and therefore should not be provided to the insurance company.

How much information may 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.

How much information may I give to a police officer?

PHI may be disclosed for law enforcement purposes; however, it must be limited to the minimum necessary and the law enforcement official's identity must be verified before releasing the information. Best practice is to refer the law enforcement official to Security Services.

What must I consider before faxing PHI or confidential information?

Always send the minimum information necessary. Be sure to include a fax cover sheet containing a confidentiality statement and confirm the correct fax number prior to sending. After sending the fax you should also ensure receipt via phone call. For faxes involving Medical Center patient information, best practice is to send the information via APeX (the fax contents, sender, destination are centrally tracked, and APeX automatically attaches a UCSF-approved cover sheet).

May I mail my patient's information?

Yes, as long as the patient has not requested otherwise, and you have a patient care need to do so. Be sure to mail only the minimum information required, confirm the correct address with the patient prior to sending, seal the envelope or package well, and make sure it does not have any identifying information on the outside besides UCSF. Department names that are indicative of a diagnosis should be omitted from the envelope, package, or post card.

We use a sign-in sheet for our patients. Is that OK?

It is OK, however reasonable safeguards and the minimum necessary standard must be met. For example, if using a patient sign-in sheet, do not request any medical information not required for sign-in. Also, consider a pull-off label system or a thick black marker to cross off names as patients are called in for their appointments, such that patient names do not accumulate throughout the day for subsequent patients to view.

What information may be listed on dry erase whiteboards?

The use of whiteboards is allowed as long as reasonable safeguards are implemented, as appropriate. Listing only last name and first initial in the department is adequate, whereas full first and last name are permitted for safety reasons in the operating room. 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.

May I access the medical record of my family member?

You are not authorized to access any medical record for which you do not have a business need. This means you should not access the medical record for personal reasons, such as inquiring about a family member's current condition. The patient should contact the appropriate medical records department, such as HIMS, to authorize a release of their information. For Medical Center patients, they may also access their records via MyChart or authorize you as their MyChart proxy. Alternatively the patient can ask their provider to release their records via QuickDisclose.

For additional FAQs related to HIPAA, please refer to the U.S. Department of Health and Human Services HIPAA Frequently Asked Questions.

UCSF RESOURCES

Department	Title	Phone	Websites
Business Associates			
Purchasing (Medical Center)	Manager	353-4701	N/A
Procurement & Business Contracts (Campus)	Manager	476-5761	http://cpbc.ucsf.edu
Development & Alumni Relations			
University Development & Alumni Relations (UDAR)	Senior Director, Annual & Special	476-4723	http://support.ucsf.edu
Education & Training			
Human Resources (Medical Center)	Director	353-4688	http://hr.ucsfmedicalcenter.org
Human Resources (Campus)	Director	476-1645	https://hr.ucsf.edu/hr.php?AT=cm&org=c
Medical Records			
Health Information Management Services (HIMS)	Director	353-2473	http://hims.ucsfmedical center.org
Patient Services			
Patient Relations	Management Service Officer	353-1936	http://serviceexcellence.ucsfmedicalcenter.org/patient-relations.html
Police			
UCSF Police Department	Chief of Police	476-1414	http://www.police.ucsf.edu
Privacy & Confidentiality			
Privacy Office	Chief Privacy Officer	353-2750	http://hipaa.ucsf.edu
Research			
Human Research Protection Program (HRPP)	Director, HRPP	476-1814	http://www.research.ucsf.edu/CHR/index.asp
Risk Management			
Risk Management (Medical Center)	Director	353-1842	http://rm.ucsfmedicalcenter.org
Risk Management & Insurance Services (Campus)	Director	476-2498	https://www.rmis.ucsf.edu
Technology & Security (Electronic / Physical)			
IT – Information Technology (Medical Center)	Director, Medical	885-7403	http://it.ucsf.edu/
ITS –ITS Security and Policy (Campus)	Director, Security and Policy	502-1593	http://it.ucsf.edu/
ISU – Information Services Unit (School of Medicine)	Chief Technology Officer	514-1377	http://isu.ucsf.edu/

POLICY REFERENCE TABLE

Policy Description	Medical Center Policy Number	Campus Policy Number	UCOP Policies
Affiliation Agreements	1.01.02	100-10	
Adverse Publicity or Incidents	1.03.01		
Authority to Solicit Gifts and Private Gifts		450-10	
Campus Administrative Policies		X	
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	5.02.01		
Contracting Ethics	1.03.05		
Control of Access to and Release of Information from UCSF Medical	5.01.06		
Electronic Mail Policy	5.01.02		
Facsimile Documents Containing PHI	5.01.25		
Fundraising Campaigns		450-13	
Fundraising Events		450-16	
Gifts and Endowments	3.03.02		
Guidelines or HIPAA Security Rule Compliance			X
Guidelines for Industry Representatives	3.05.07		
HIPAA			X
HIPAA Administrative Requirements			X
HIPAA Authorization Forms			X
HIPAA Breach Response			X
HIPAA Business Associates	1.02.15	200-28	X
HIPAA Information Security			X
HIPAA Patients' Rights			X
HIPAA Uses and Disclosures			X
HIPAA Uses and Disclosures for Fundraising			X
HIPAA Uses and Disclosures for Marketing			X
HIPAA Uses and Disclosures for UC Group Health Plans			X
Identity / Medical Identity Theft Prevention and Response Policy	1.02.21	200-29	
Information Security and Confidentiality	5.01.04	650-16	

Informed Consent	6.02.02		
Legal Document Acceptance (Subpoenas, Summons & Complaints)	3.06.06		
Legal Medical Record Policy			X
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		
Privacy Investigation Policy		200-30	
Regulatory Agencies Reportable Events	1.01.18		
Remote Access	5.01.07		
Reporting Improper Governmental Activities and Protection Against Retaliation (Whistleblower Policy & Whistleblower Protection Policy)		150-23	
Research Involving Human Subjects		100-16	
Safeguarding the Privacy and Confidentiality of UCSF Information & Data	5.02.26		
Sentinel / Adverse Event Process	3.06.10		
UC Health and Welfare Plans-Notice of Privacy Practices			X
UC HIPAA Glossary			X
UC Implementation of HIPAA Privacy Rule IS-2 Inventory, Classification and Release of University Electronic Information IS-3 Electronic Information Security			X X X
UCSF Foundation		500-11	
Unified UCSF Enterprise Password Standard			
Vendor Visitation Policy	3.05.07		
Workforce Sanctions for Patient Privacy Violations		200-32	

Medical Center Policies http://manuals.ucsfmedicalcenter.org/index.shtml
Information Technology Policies and Procedures https://it.ucsf.edu/security/policies
Campus Administrative Policies http://policies.ucsf.edu
UCOP Policies http://www.ucop.edu/ucophome/coordrev/ucpolicies

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 codes 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 numbers
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) addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photographs and any comparable images
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.

In May 2002, the Board of Regents designated the University of California as a HIPAA hybrid covered entity and determined that UC would be a Single Health Care Component for the purposes of complying with the HIPAA rule. All of the entities at UC covered by the HIPAA Privacy and Security Rules - medical center, medical clinic, health care providers, health plans, student health centers - are a single entity for purposes of compliance with HIPAA. However, the research function is excluded from HIPAA coverage at UC. Accordingly, research health information that is not associated with a health care service is not subject to the HIPAA Privacy and Security Rules. Other state and federal laws govern privacy and confidentiality of personal health information obtained in research.

HIPAA Privacy Compliance. The HIPAA Privacy Rule, effective April 14, 2003, established national standards to guard the privacy of patient's protected health information. Protected health information includes:

- Information created or received by a health care provider or health plan that includes health information or health care payment information plus information that personally identifies the individual patient or plan members and
- Personal identifiers include: a patient's name and email, web site and home addresses; identifying numbers (including social security, medical records, insurance numbers, biomedical devices, vehicle identifiers and license numbers); full facial photos and other biometric identifiers; and dates (such as birth date, dates of admission and discharge, date of death).

HIPAA Security Compliance. The HIPAA Security Rule, effective April 20, 2005, requires that workforce members adhere to controls and safeguards to: (1) ensure the confidentiality, integrity and availability of confidential information; and (2) detect and prevent reasonably anticipated errors and threats due to malicious or criminal actions, system failure, natural disasters and employee or user error. Such events could result in damage to or loss of personal information, corruption or loss of data integrity, interruption of University activities, or compromises to the privacy of the University patients or employees and its records.

Scope - Who is subject to HIPAA at UC? HIPAA regulations apply to employees, health care providers, trainees and volunteers at UC medical centers and affiliated health care sites or programs and employees who work with UC health plans. HIPAA regulations also apply to anyone who provides financial, legal, business, or administrative support to UC health care providers or health plans.

APPENDIX 3 – UNIVERSITY OF CALIFORNIA, SAN FRANCISCO CONFIDENTIALITY OF PATIENT, EMPLOYEE AND 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 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.

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