UCSF Privacy and Confidentiality Handbook

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

Revised June 2013

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

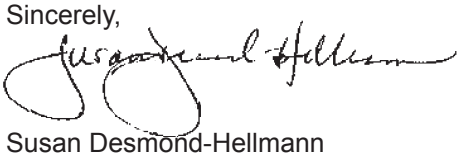
The UCSF Privacy and Confidentiality Handbook is a general introduction to the privacy and security laws and regulations established by the federal Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and the state 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 were established, in order to protect the confidential medical and billing information 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,



Susan Desmond-Hellmann
Chancellor

Table of Contents

MESSAGE FROM THE CHANCELLOR ON BEHALF OF THE DEANS AND MEDICAL CENTER CHIEF EXECUTIVE OFFICER 2

HANDBOOK OBJECTIVES 6

HIPAA 6

Privacy and Confidentiality Overview 6

PRIVACY RULE 7

Purpose of Privacy Rule 7

Highlights of Privacy Rule 7

Potential Consequences of Violating the Privacy Rule 7

WORKFORCE REQUIREMENTS 7

CONFIDENTIAL PROTECTED HEALTH INFORMATION: DEFINITION AND RIGHTS TO ACCESS 8

What is considered confidential protected health information (PHI)? 8

What is not considered PHI? 8

What patient information must we protect? 8

When can a Limited Data Set be used for research, public health, or health care operations? 8

Who is authorized to access confidential PHI? 8

When can students and trainees access PHI? 9

What is the "minimum necessary" standard? 9

When are written patient authorizations required? 9

What if I see someone violate the privacy law? 9

MEDICAL RECORD ACCESS AND CONTROL 9

PATIENT RIGHTS 10

Right to Receive the "Notice of Privacy Practices" 10

Right of Access to Paper or Electronic Copies 10

Right to Request an Amendment or Addendum 10

Right to an Accounting of Disclosures 10

Right to Request Restrictions 10

Right to Complain 10

Facility Patient Directories (In-patients) 11

Criteria for release of information by Provider to Patient 11

Authorization for Release of a Patient's PHI 11

Exceptions to the PHI Disclosure Rules 11

When a Patient is Unable to Authorize the Release of Their PHI 12

BUSINESS ASSOCIATES 12

CLINICAL AND OTHER RESEARCH INVOLVING HUMAN SUBJECTS 13

CHR Application 13

Authorization and Waiver of Authorization 13

De-Identified Information 13

Protection of Information 14

SECURITY RULE 14

Purpose of Security Rule 14

Definition of Security 14

Requirements for Security 14

HOW TO COMPLY WITH THE SECURITY RULE 15

What Steps Must I Take to Safeguard Computer Resources and PHI? 15

Encrypting and Securing Mobile Computing Devices, Smartphones, and Tablets 15

Password Security 16

Document, Workstation, and Mobile Device Security 16

Disposal and Destruction 16

Access and Identification 17

SECURITY OF COMMUNICATIONS CONTAINING PHI 17

Email 17

Fax 18

Voice Mail / Answering Machines / Telephone Communications/ Video Conferencing 18

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) 18

Marketing 18

Fundraising 19

Media 19

Photography 19

OTHER FEDERAL LAWS 20

Family Education Rights and Privacy Act (FERPA) 20

Health Information Technology for Economic and Clinical Health Act (HITECH) 20

Final Omnibus Rule 20

The Genetic Information Nondiscrimination Act of 2008 (GINA) 20

Medicare Conditions of Participation (CoP) 20

Red Flag Rule 20

U.S. Department of Health and Human Services 20

CALIFORNIA STATE LAWS 21

California Health and Safety Code Section 1280.15 21

California Information Practices Act (Civil Code Section 1978) 21

Confidentiality of Medical Information Act (CMIA) 21

Lanterman-Petris-Short Act (LPS) 21

Title 22, California Code of Regulations 21

Potential Consequences of Violating the State Privacy Laws 21

FREQUENTLY ASKED QUESTIONS (FAQs) 22

UCSF RESOURCES 26

POLICY REFERENCE TABLE 27

APPENDIX 1 – PHI DATA ELEMENTS 28

APPENDIX 2 – RESOLUTION OF THE UNIVERSITY OF CALIFORNIA BOARD OF REGENTS: ACADEMIC HEALTH CENTER HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE PROGRAM 29

APPENDIX 3 – UNIVERSITY OF CALIFORNIA, SAN FRANCISCO CONFIDENTIALITY OF PATIENT, EMPLOYEE AND UNIVERSITY BUSINESS INFORMATION AGREEMENT 31

Statement of Privacy Laws and University Policy 31

Acknowledgment of Responsibility 32

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.

HANDBOOK OBJECTIVES

This Handbook is a general introduction for 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, and UCSF Policies and Medical Center Administrative Policies and Procedures.

It is expected that 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 and University policy.

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

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.

Please refer to http://hipaa.ucsf.edu for advanced training module 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, or 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 HIPAA 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 which range from $100 to $1,500,000 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, and the potential for 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 last date of service.

The UCSF workforce, 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.

CONFIDENTIAL PROTECTED HEALTH INFORMATION: DEFINITION AND RIGHTS TO ACCESS

What is considered confidential protected health information (PHI)?

PHI is individually identifiable health information which is created in the process of caring for the patient, and is transmitted or maintained in an electronic, written, or oral manner. Examples of individually identifiable information include patient name, address, date of birth, age, medical record number, phone number, fax number, 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 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 all18 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, prescriptions, 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 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 for research and call the Privacy Office with questions (415-353-2750).

Who is authorized to access confidential PHI?

PHI may be accessed without patient consent under certain circumstances, 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, 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, and patient inclusion in the hospital directory

When can students and trainees access PHI?

Students and trainees in all UCSF and affiliated training programs may have access to PHI. Students and trainees are required to complete a privacy orientation or training and to sign a confidentiality agreement. Students and trainees are not permitted to remove any PHI from UCSF premises. Students and trainees may request copies of de-identified data for use in case presentations, however the request for use or disclosure must be coordinated with the appropriate medical records department where they are providing care, such as UCSF Medical Center's Health Information Management Services (HIMS).
It is recommended that students review de-identification guidance in this booklet.

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, a covered entity must make reasonable efforts to limit PHI to that which is necessary to accomplish the intended purpose of the use, disclosure, or request. 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. 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 other reason, 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" for a list of exceptions to the authorization requirement related to public health, 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. Immediately report concerns to your supervisor or the UCSF Privacy Office (415-353-2750). Refer to the resource list on page 25 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 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 based on 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 signed an authorization.

- **Right to Request Restrictions**
  Patients have the right to request restrictions on how we will communicate with the patient or release health information. When a patient pays in full for a UCSF service, and requests a restriction of release to a health plan, UCSF must honor their request.

- **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, the appropriate medical records department, such as UCSF Medical Center's Health Information Management Services (HIMS), the Committee for Human Research (CHR), or the Privacy Office.

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.

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). 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).

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) (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 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, 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, 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 is required to release information about the patient's discharge, transfer, serious illness, injury, or death, unless the patient requests that this information not be provided.

BUSINESS ASSOCIATES

Under HIPAA, a vendor or third party that engages in a function or activity involving the use or disclosure of UCSF's patients' individually identifiable health information 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 business associate to include, "one that creates, receives, maintains, or transmits" PHI on behalf of the Covered Entity (CE). The BAA sets forth, in part, the obligation of the business associate 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 or disclosure of individually identifiable health information may include 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)

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

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. A CHR application will be needed if researchers wish to access identifiable medical information.

Protection of Information

HIPAA mandates that systems and processes 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 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 computer systems and electronic transmissions of information, for the purposes of:

- Ensuring the confidentiality, integrity and availability of all electronic protected health information (ePHI) that is created, received, maintained, or transmitted by the covered entity
- Protecting against any reasonably anticipated threats or hazards to the security or integrity of ePHI
- Protecting against unauthorized uses or disclosures of ePHI
- Ensuring compliance by a covered entity's workforce

Definition of Security

Security is generally 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 for Security

Under HIPAA, UCSF is required to secure all access to electronically stored and transmitted PHI (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 and vulnerabilities.

- Workforce members are responsible for employing appropriate and applicable security controls to protect all University electronic information resources under their control, such as:

    - Safeguarding PHI from accidental or intentional disclosure to unauthorized persons
    - Safeguarding PHI from accidental or intentional alteration, destruction, or loss
    - Safeguarding computers from viruses and malware
    - Taking precautions that will minimize the potential for theft, destruction, or any type of loss
    - Protecting workstations from unauthorized access and theft (e.g., via 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 portable media (e.g., USB thumb drives, external hard drives, CD-ROM/DVD disks, floppy disks, magnetic tapes, videotapes, SD memory cards, and all other forms of removable media or electronic storage devices) 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

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

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

Encrypting and Securing Mobile Computing Devices, Smartphones, and Tablets

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

1. If at all possible, do not store ePHI on mobile devices.
2. All laptops, smartphones and tablets devices used for UCSF business must be connected via ActiveSync to the UCSF Exchange email server. More information at: http://it.ucsf.edu/services/email-mobile-access
3. If ePHI is stored on a mobile device, the data must be protected with an approved UCSF data encryption solution. For laptops, hard drives, and flash drives, use encryption, and for smartphones and similar mobile devices, use 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.
4. Never leave devices unattended, or in an exposed or unsecured area.
5. Always password-protect and enable encryption on mobile devices including storage cards.
6. Utilize physical locks for laptops and other mobile devices.
7. Keep mobile devices up-to-date with current operating system security patches and anti-virus software.
8. Ensure that the mobile device meets UCSF minimum security standards (see http://it.ucsf.edu/policies/ucsf-minimum-security-standards-electronic-information-resources).
9. Frequently make protected backups of data stored on remote systems to a UCSF-controlled server. UCSF IT has a back-up solution to make this effort easy and secure for you.
10. Use caution when uploading or downloading files to or from mobile devices. Adhere to the “minimum necessary” standard and never transfer ePHI over a network without using encryption.
11. Off-site work requires greater vigilance to maintain the required level of privacy and security.
12. Applications may have the potential to intercept and/or read data on your device. Applications should only be downloaded and installed from trusted sources. Users should 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 devices as this may weaken the security of the device and expose ePHI needlessly.

13. Be alert to recognize and report all actual and suspected privacy and security incidents to your department supervisor or manager, the UCSF Privacy Office (415-353-2750), and to IT for security issues (415-514- 4100).
14. Immediately report lost or stolen devices to the UCSF Police Department by filing a police report (call 415-476-1414). Refer to the Guidance for lost/stolen mobile device and/or media at http://hipaa.ucsf.edu/itsecurity/default.html

Password Security

1. Protect your user ID and password. Do not share, write down, or post your password under any circumstances!
2. Commit your password to memory or use an appropriate secure password management solution.
3. At a minimum, when creating your password, incorporate a combination of letters and numbers. Avoid dictionary words and personal information. Incorporate a combination of upper and lower case letters, numbers, and special characters. Avoid dictionary words, personal information, common terms, sport teams, etc. when creating your password
4. Immediately change your password if it is accidentally exposed or compromised.
5. Report all password exposures to your department supervisor or manager, and the UCSF IT Service Desk (415-514-4100).
6. Adhere to established password management standards. (http://security.ucsf.edu/EIS/Names/UCSFUnifiedPasswordStandard.html)
   Always keep computers password-protected and locked or logged off when not in use. Configure screen savers to lock your computer after several minutes of inactivity.

Document, Workstation, and Mobile Device Security

1. Log off or lock access to computers when you leave, even if only for a moment.
2. Keep computer systems up-to-date with current operating system security patches and antivirus definitions.
3. Ensure that computer systems and mobile devices meet UCSF minimum security standards. This includes ensuring the computer is encrypted. See http://it.ucsf.edu/policies/ucsf-minimum-security-standards-electronic-information-resources.
4. Ensure that computer screens and displays with access to ePHI are not visible to unauthorized individuals or passersby.
5. Keep confidential or sensitive information locked away when not in use. File documents in locked cabinets or drawers when you have finished with them.
6. Be alert to recognize and report all privacy and security incidents to your department supervisor or manager. For privacy issues, contact the Privacy Office (415-353-2750), and for IT security issues call UCSF IT Service Desk (415-514-4100).
7. Be cognizant of your environment. Free WiFi hotspots may allow your connection and your data to be compromised.

Disposal and Destruction

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, cross- cut shredders, locked 'Shred-It' disposal bins located throughout UCSF, etc.).
2. Back up data files to approved UCSF servers, and follow approved UCSF media destruction procedures before disposing of devices.
3. 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 ITS Service Desk for guidance (415-514-4100). Maintain records to track the movement (transfer or relocation) of devices and media.

Access and Identification

1. Always follow established visitor and observer security guidelines and procedures.
2. Always wear your security badge or identity badge while at work.
3. 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

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

1. UCSF is increasing the usage of MyChart as another way of communicating electronically with our patients. Patients can also see many of their lab test results, request appointments and medication refills, and use other services. UCSF MyChart is free, secure, and convenient. To have your patients sign up, please email ucsfmychart@ucsfmedctr.org
2. If you are using email to send UCSF confidential or patient information (please see section on UCSF MyChart) then you are responsible for ensuring that this information is processed securely by using UCSF's secure email system. UCSF's 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 website, along with a web link. By clicking on the link and accessing the website, the recipient will be able to retrieve the message over a secure internet connection. Detailed instructions are available at:
   http://it.ucsf.edu/services/secure-email/tutorial/how-secure-email-works
3. For the system to work properly, you must use it correctly.
   a. The start of the subject line must be precise in order to enable security.
   b. 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
4. Do not include actual ePHI in the subject line (e.g. MRNs or patient names)
5. Be careful what you send via email. Do not send confidential information unless absolutely necessary. De-identify the information if possible. Warn patients who communicate with you via email that their confidentiality cannot be ensured.
6. 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.
7. Do not send attachments containing ePHI without encryption.
8. 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..*

9. 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.
10. 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

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 as recipients may have changed locations. Pre-programmed numbers should be reviewed on a regular basis.
3. Use cover sheets 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.

4. Immediately alert the sender of any faxes you receive in error, do not use or disclose the information, and either return or destroy the fax.
5. If you are advised that you sent a fax of 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.

Voice Mail / Answering Machines / Telephone Communications / Video Conferencing

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. Avoid leaving any PHI or other sensitive information.
3. If you use a speakerphone, be aware of your surroundings and sensitive to the messages being replayed. Close the door, lower the volume, and consider picking up the handset.
4. If you are advised that you left PHI on the wrong voice mail, confirm that the recipient deleted the message and did not use or disclose the information. Contact the Privacy Office for next steps.
5. Keep the volume at an appropriate level so that your conversation cannot be overheard.
6. For video conferencing, be aware of your surroundings and make sure you know who is your audience. You may broadcast images to unintended participants.
7. 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. 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) – including physician, department of service, and outcome - without a written Authorization for Fundraising (opt-in). UCSF may only use demographic 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. 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 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 service staff.

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 six 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, contact Risk Management (415-353-1842).

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 the IT Service Desk (*http://it.ucsf.edu/about/teams/ucsf-it-service-desk* or 415-514-4100).

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.

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 5 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.

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 also 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 monitoring compliance with the federal and state privacy laws and regulations, including the reporting of breaches to these agencies. In addition, the Privacy Office orchestrates departmental responses in the event of a breach of privacy, and provides consultation for all privacy related questions. The Privacy Office tracks, analyzes, and reports on all privacy compliance 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 stolen, or was stored on a stolen device (computer or 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 ITS. For disclosures not involving a theft, contact the Privacy Office immediately.

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

- Date and time the breach was discovered
- Name and contact information of the person who discovered the breach
- The specific information disclosed
- The number of individuals who had their information disclosed
- How the breach 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, patient notification and follow-up, determining and implementing corrective actions and changes in process, following-up with third party vendors, retraining personnel, and documentation, as needed. Please note that only the Privacy Office can determine if notification is required.

Privacy breaches need to be reported to the Privacy Office as soon as they are discovered, even if the person who discovered the breach was not involved. Any delay in reporting to the UCSF privacy office delays UCSF reporting to the state and to patients. Delayed reporting to the state and patients beyond the 5 day timeframe exposes you and the University to financial liability in the way of administrative fines and penalties.

You will not be penalized for reporting breaches, nor does the reporting of a breach necessarily implicate you in any way.

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

Refer to the Education and Training section of the Privacy Office website. Remember, all members of a department need to have some type of training, including volunteers, and all training must be documented. Human Resources and/or the workforce member's Department is responsible for ensuring its staff members are properly trained, and for maintaining documentation of such. 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. Additionally, 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. See the Fundraising section for details. Any use of the UCSF logo associated with another organization needs to be approved by University Relations (415-476-9117).

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

According to the Notice of Privacy Practices, 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. In all other cases, or if no contact person exists, you are not authorized to release any information other than whether or not the patient is in the hospital and his or her general condition (e.g., good, fair, critical). If the patient is hospitalized, certain limited information can be found in the hospital directory so that family, friends, and clergy can locate the patient. Good practice involves requiring the requestor to provide the patient's full name, verifying their identity and relationship to the patient, and only supplying 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.

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 patient's preference for follow-up or appointment communication during the initial contact.

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?

As long as the patient has not requested otherwise, you may do so but only by following the secure email guidelines in this handbook. Best practice includes making sure the patient prefers this form of communication and understands the risks associated with it.

May I send unencrypted emails to communicate with my patients?

You should use the secure patient portal, MyChart, in lieu of email to communicate with your patients electronically. If the patient does not use MyChart, then you should use secure email to communicate with your patients. However, if they prefer unencrypted email, then you may send unencrypted emails only after you advise the patient of the privacy and security risk. This should be documented in the patient's record.

How much information may I give an insurance company?

According to the Notice of Privacy Practices, we may use and disclose medical information for the purpose of obtaining payment. Best practice is to provide only what is needed for this purpose. For example, lab values are not required for billing purposes, and therefore should not be provided to the insurance company. However, if the patient has submitted an Authorization allowing the use and disclosure of his or her information to the insurance company, the minimum necessary standard would no longer apply.

My patient's insurance company is requesting information in relation to a Worker's Compensation claim. What information may I provide?

You are authorized to disclose PHI in order to comply with Worker's Compensation law. In fact, HIPAA generally allows for the disclosure of patient information to comply with any judicial or administrative proceeding in response to a court order, subpoena, or other legal process.

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.

Do I need written authorization to disclose immunization records to a patient's school?

No. You may disclose proof of immunization to a school where state or other law requires the school to have such information prior to admitting the student. Although written authorization is not required, the parent or guardian must agree, which may be orally, to the disclosure of immunization records.

How much information may I give to a police officer?

You may disclose protected health information for law enforcement purposes, although you must first verify the identity and authority of the officer requesting the information. In addition, you should limit the PHI released to only the minimum required.

What information may be faxed?

Always send the minimum information necessary. Best practice is to confirm the correct fax number prior to sending, to include a cover sheet with a confidentiality statement, and to ensure receipt via phone call.

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. Best practice is to mail only the minimum required, to confirm the correct address with the patient prior to sending, to seal the envelope or package well, and to make sure it does not have any identifying information on the outside besides UCSF.

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. Use the matrix at http://hr/forms/compliance.pdf to determine what the compliance requirements are in your particular case. Links to additional forms and information can be found at http://hipaa.ucsf.edu/education/visitors. Questions and requests for guidance should be directed to Privacy, Risk Management, Occupational Health, and/or Human Resources.

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.

I purchased a new laptop. May I use it for work purposes? And if so, how do I protect it?

You should avoid using any personal devices for work purposes. If you must use your personal laptop for work purposes, discuss it with your Manager first and consult with IT before use to ensure proper security through encryption, firewalls, passwords, anti-virus software, regular software updates, and more (see the UCSF Campus ITS website, or the UCSF Medical Center IT website). Always follow best practices, including the physical security of your device at all times, regular backups of data, storage of only the very minimum necessary patient information, and the permanent deletion of all data and files the moment they are no longer needed. Remember, it is your responsibility to encrypt and safeguard your device, and you may be held personally liable for breaches of patient information due to an unencrypted, personal device that does not comply with University policy.

May I access the medical record of my family member? What if they ask me to?

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.

May I take PHI off-site?

Federal and state regulations, as well as UCSF policy, require you to protect the privacy and confidentiality of PHI in any format, including verbal, electronic, and paper. Best practice is to refrain from taking PHI off-site, and to use alternative methods for accessing information remotely, such as accessing UCSF systems via Virtual Private Network (VPN).

If your job requires you to transport PHI between UCSF sites, consider other options (e.g., email, fax, or scan the PHI prior to going off-site). If the other options are not available to you, remember you are still responsible for securing the PHI and keeping it in your possession at all times. Do not leave the PHI unattended in your bag, briefcase, folder or your car, even if it's locked in the trunk. If you transport PHI, you must remember to remove it from your bag, briefcase, folder, car, etc. once on-site and secure it in your office or work area.

If you have any questions about protecting and/or handling PHI, please contact your manager or the Privacy Office.

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	353-4675	N/A
Procurement & Business Contracts (Campus)	Manager	502-3047	http://cpbc.ucsf.edu
Development & Alumni Relations			
University Development & Alumni Relations (UDAR)	Senior Director, Annual & Special Giving	502-6225	http://support.ucsf.edu
Education & Training			
Human Resources (Medical Center)	Director	353-4688	http://hr.ucsfmedicalcenter.org
Human Resources (Campus)	Director	476-1645	http://ucsfhr.ucsf.edu
Medical Records			
Health Information Management Services (HIMS)	Director	353-2885	http://hims.ucsfmedical center.org
Patient Services			
Patient Relations	Management Service Officer	353-1936	http://serviceexcellence.ucsfmedical center.org/patientrelations
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	476-9840	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 Center IT Security	514-8855	http://it.ucsfmedicalcenter.org
ITS –ITS Security and Policy (Campus)	Director, Security and Policy	502-1593	http://its.ucsf.edu/main/home.html
ISU – Information Services Unit (School of Medicine)	Chief Technology Officer	502-4004	http://medschool.ucsf.edu/isu

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	
Control of Access to and Release of Information from UCSF Medical Center Information Systems for Research Purposes	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 for Industry Representatives	3.05.07	
HIPAA Business Associates	1.02.15	200-28
Identity / Medical Identity Theft Prevention and Response Policy	1.02.21	200-29
Information Security and Confidentiality	5.01.04	650-16
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	
Privacy Investigation Policy		200-30
Remote Access	5.01.07	
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

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, death).

HIPAA Security Compliance. The HIPAA Security Rule, effective April 20, 2005, requires that workforce member 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 compromise 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.

This page is intentionally left blank.

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 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.

Acknowledgment 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 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 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.
- 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.
  - **I agree that I will only use computing devices, such as desktop computers, laptop computers, tablets, mobile phones and external storage, that are encrypted with an approved UCSF solution before using them for any purposes involving PHI and/or Confidential Information. I understand that I may be <u>personally responsible</u> for any breach of confidentiality resulting from an unauthorized access to data on that device due to theft, loss or any other compromise. I will contact the IT Service Desk at (415) 514-4100 for questions about encrypting my computing device.**
  - 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 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 IT Service desk at (415) 514-4100 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 may be personally responsible**, and criminal sanctions.

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

DocuSigned by:
Chad Ingram
Signature
Signature: 03FE10405...

Date

Chad Ingram
Print Name

UCSF Department

UCSF Employee Number

Signature UCSF Representative

Print UCSF Representative Name

❑ Non-UCSF Employee