

UNIVERSITY OF CALIFORNIA IMPLEMENTATION OF HIPAA PRIVACY RULE

This document summarizes the University of California's implementation of the federal Health Insurance Portability and Account Act (HIPAA) Privacy Rule. The complete Privacy Rule and other useful links provided by the Office of Civil Rights at HHS can be accessed at <http://www.hhs.gov/ocr/hipaa/>

SECTION I: COMPONENTS OF THE "COVERED ENTITY"

For purposes of HIPAA, the University of California, as an academic institution, has designated itself as a "Hybrid Covered Entity" as defined under the Privacy Rule as it is a single legal entity that performs both covered and non-covered functions. The University has substituted the term "Single Health Care Component (SHCC) to delineate those elements of the University that comprise the University's covered entity.

The SHCC includes those entities and workforce members that performed covered functions as a:

1. Health care provider or those entities and workforce members who do not necessarily engage in electronic transactions as currently defined, but do not otherwise meet the definition of a health care provider;
2. UC's self-funded group health plans, and
3. Those entities and workforce members who perform business, legal, administrative and finance activities or functions on behalf of UC's health care providers or plans, when those functions involve the use of protected health information (PHI) that has been created or received by UC's covered entities (health care providers or health plans).

Workforce members often have multiple roles, both covered and non-covered. The determination of those entities and individuals is a dynamic and ongoing process that includes the following criteria:

1. When the use and disclosure of individually identifiable health information (IIHI) is carried out by the SHCC covered entities and workforce members, the individual's health information is defined as PHI, and the Privacy Rule covers those functions and workforce members who carry out those functions;
2. When the use and disclosure of IIHI is covered out by a business, financial, legal or administrative entity of the UC on behalf of or for UC's SHCC, the individuals information is PHI, and the Privacy Rule covers those functions and workforce members who carry out those functions;
3. When the use and disclosure of IIHI is carried out by UC in its capacity as an employer or educational institution, the information is NOT PHI, and those UC functions are not subject to the Privacy Rule, but the confidentiality of the

individuals' health information is protected by other state and federal law as well as UC policy; and

4. When the use of IIHI is by a UC researcher for an IRB-approved protocol, the information is not PHI; however, when the researcher wants to use PHI created, received or maintained by the SHCC for purposes of the approved research, the Privacy Rule mandates that the SHCC receive specific assurances that the individuals health information will be protected once disclosed to the researcher. See Research Guidelines (<http://www.universityofcalifornia.edu/hipaa/research.html>).

Designated Components of the SHCC

The Board of Regents designated the following UC entities and workforce members as part of the UC SHCC and as such, subject to the HIPAA Privacy Rule and the University of California's *System Standards*:

1. The five academic Health Centers, medical centers and clinics at Davis, Irvine, Los Angeles, San Diego and San Francisco;
2. Health professional schools at Berkeley, Davis, Irvine, Los Angeles, San Diego, and San Francisco;
3. Functions within the three UC-administered Department of Energy Laboratories at Berkeley, Livermore, and Los Alamos, including occupational health;
4. Student Health centers at all campuses;
5. Athletic Departments at some campuses;
6. Occupational Health Centers at some campuses;
7. UC self-insured health or group health plans;
8. Certain department sponsored clinics providing health care to the community as part of the education and research missions of those departments (e.g., behavioral health, speech and hearing services, etc.)
9. System and campus Privacy and Compliance Offices, HIPAA Taskforce and Covered Entities' committees (systemwide and campus), and Corporate Compliance Committees (system and campus); and
10. Other UC entities engaged in covered functions and that use and disclose PHI as determined by the Board of Regents.

Members of the UC workforce who perform duties for *both* the SHCC and for those units within UC that are not part of the SHCC may only use and disclose PHI in the course and scope of their job duties as allowed by the Privacy Rule. The workforce member may not use PHI for activities or functions outside of the SHCC unless the individual or patient has provided a written authorization for the disclosure of PHI to non-covered entities within the University.

SECTION II: RESPONSIBILITIES OF THE COVERED ENTITY

The Privacy rule provides the first comprehensive federal protection for the privacy of health information, and creates standards that protect a patient's or health plan member's medical records and personal health information. The Privacy Rule was implemented to:

1. Give patients and plan members more control over their health information;
2. Set boundaries on the use and release of medical records;
3. Establish appropriate safeguards that health care providers and others must achieve to protect the privacy of health information;
4. Hold violators accountable and imposes civil and criminal penalties for violation of a patient's privacy rights;
5. Strike a balance when public responsibility requires disclosure of some forms of data (for example to protect public health); and
6. Establish a "federal floor" of safeguards. State laws with stronger privacy protections take precedence over and above the HIPAA Privacy Rule, *such as, for example, the California Medical Information Act (CMIA (Civil Code 56 et seq))*.

RESPONSIBILITIES OF THE UNIVERSITY AS A COVERED ENTITY

1. Provide information to patients or plan members about their privacy rights and how their information can be used;
2. Adopt clear privacy policies and procedures;
3. Educate all employees regarding privacy policies and procedures
4. Designate a Privacy Official or individual to be responsible for seeing that privacy procedures are adopted and followed, and/or HIPAA Office responsible for receiving and handling complaints;
5. Respond to patient or plan members' requests regarding certain rights provided in the privacy rule (refer to Section III);
6. Secure patient and members' records so that they are available only to those who need them; and
7. Maintain the required administrative documentation demonstrating compliance with the Privacy Rule.

SECTION III: PATIENT RIGHTS SUMMARY

The Privacy Rule entitles patients or members to:

1. Receive a notice of a covered entity's privacy practices governing permitted uses and disclosures of PHI;
2. Authorize release and disclosure of PHI as required in the Privacy Rule;
3. Inspect and/or copy PHI;
4. Request that PHI be amended or appended (if information is incorrect or incomplete);
5. Request and receive an accounting of uses and disclosures of PHI, with certain exceptions;

6. Request additional restrictions on use/disclosure of PHI; and
7. Request confidential communications of PHI.

A. Notice of Privacy Practices (The Notice)

The Privacy Rule gives individuals a right to be informed of the privacy practices of their health care providers and health plans, as well as to be informed of their privacy rights with respect to their personal health information. The Privacy Rule requires the SHCC to describe in detail the uses and disclosure of PHI that may be made by the SHCC, the individual's rights relative to those uses and disclosures, and the SHCC's legal duties with respect to that information. Consequently, all SHCC uses and disclosures of protected health information (PHI) must be consistent with that Notice. The University's Office of the General Counsel, in consultation with the UC HIPAA Taskforce, has prepared the SHCC's Notice. The model Notice contains all Privacy Rule required elements and, for this reason, must not be altered or modified without the express review and approval by UC's Office of the General Counsel. The UC Notice is posted at <http://www.universityofcalifornia.edu/hipaa/notice.html>

Mental Health Notice

The SHCC determined that a separate Notice should be provided to individual's receiving mental health treatment so that patients can be clearly informed about the protections provided for their health information. In many cases, California law provides for more stringent protections of these individuals, and the Mental Health Notice takes into account the complex layers of laws relative to these protections. Questions regarding the use and disclosure for Mental Health Patients should be referred to the Office of the General Counsel, local or system Privacy Officer(s) or Privacy Liaison. The UC Mental Health Notice is available at <http://www.universityofcalifornia.edu/hipaa/notice.html>

B. Patient Access to their Health Information

The SHCC must provide the individual with an opportunity to access, inspect, and obtain a copy of the individual's designated record set (DRS). (*See Section VIII, Definitions*)

The Notice of Privacy Practices provides information to the individual as to how to request access. Requests to access, inspect or copy the DRS must be in writing to an individual or office specified for these purposes. The specified individual will be responsible to grant access to the record within 5 days (California state law) or to advise the individual in writing if the SHCC does not maintain the record.

In order to expedite the response to the written request for access, the SHCC should:

- a. Provide the individual with a *Request for Access* form that allows the individual to specify the scope, format, and the option of purchasing a summary of the PHI requested;
- b. Provide the individual with a list of the fees for summarizing the information, if the individual requests a summary of the DRS;
- c. Provide the individual with convenient times and location for inspecting or obtaining a copy of the information; and
- d. Request the location for mailing the information.

The SHCC is not required to provide access to the following information:

- a. Psychotherapy notes;
- b. Information compiled in anticipation of a civil, criminal or administrative action or proceeding;
- c. Information not available because of restrictions under the Clinical Laboratory Improvements Amendments of 1988 (CLIA);
- d. Oral communications;
- e. The request is to a correctional institution or to the SHCC under the direction of a correctional institution, if release of the information would jeopardize the health, safety, security, custody or rehabilitation of the individual, other inmate or an officer or employee of the correctional institution;
- f. The PHI has been created or obtained by a covered health care provider in the course of research that includes treatment and in the research consent process, the individual has agreed he or she will not be allowed access to that PHI so long as the research is in progress;
- g. Access to information is restricted by the Privacy Act; or
- h. The information was obtained from a third party under a promise of confidentiality.

So long as the individual is allowed a review of the denial, the SHCC may deny access to the DRS in the following circumstances:

- a. A licensed health care professional has determined that access could endanger the life of the individual or another person;
- b. The requested information references another person (except a health care provider) and a licensed health care professional has determined that access is reasonably likely to cause substantial harm to the other person;
or
- c. The request is made by the individual's personal representative, and a licensed health care professional has determined that access is reasonably likely to cause substantial harm to the individual or another person.

The SHCC can only deny access to that portion of the DRS described in a, b, c, above. To the extent possible, the individual must have access to all other information.

If the SHCC denies access, the SHCC must provide a written denial to the individual, and the written denial must:

- a. Be in plain language;
- b. Contains the basis for denial;
- c. Provide for review rights;
- d. A description of how the individual may complain to the SHCC (*see Section VII, Administrative Requirements*); and
- e. The name or title, telephone number of the local or system Privacy Officer designated to receive complaints.

C. Patient Request for Amendment

The individual has a right to request that the SHCC amend the medical record or other information in the DRS. Under California law, the patient also has a right to append information to the medical record. The individual must provide a written request to the SHCC for the amendment and provide the reason to support the requested amendment. The SHCC should maintain the written request for 6 years. The SHCC must act on the individual's request for an amendment no later than 60 days after receipt of such a request by either accepting and making the amendment or denying the request in writing. If the SHCC is unable to act on the amendment within 60 days, it has a one-time delay of no more than 30 days by providing (within the initial 60 days) the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed.

If SHCC accepts the amendment in whole or in part, the SHCC must:

1. Identify the affected records and link the amendment to the affected records in the designated record set;
2. Inform the individual in a timely manner that the amendment has been made;
3. Obtain the individual's identification of and agreement to have the SHCC notify those persons with whom the amendment needs to be shared; and
4. Make a reasonable effort to notify those persons identified by the individual and those persons, including business associates, who the SHCC knows has the designated record set that has been amended and who should amend the DRS because reliance on the unamended designated record set could cause harm to the individual.

The SHCC may deny an individual's request for amendment, if it determines that the record that is the subject of the request:

1. Is accurate and complete without amendment;
2. Is not part of the designated record set;
3. Would not be available for inspection by the individual; or

4. Was not created by the SHCC, unless the individual provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment.

If the SHCC denies the request for amendment, the SHCC must provide in writing:

1. A written denial (in plain language) within the required time limits;
2. A basis for the denial;
3. A description of how the individual can submit a written statement disagreeing with the denial, including the basis for disagreement and the SHCC's accepted length of the statement of disagreement, which should be the same length as required under California law;
4. A statement that if the individual does not submit a written statement of disagreement, the individual may request that the SHCC provide the individual's request for amendment and the written denial with any future disclosure of the PHI subject to the requested amendment; and
5. A description of how the individual can complain to the SHCC, including the title, name, contact number of the Privacy Office or Officer.

The SHCC may also prepare a rebuttal of statement of disagreement, but must provide the individual with a written copy of the rebuttal statement.

Even if the SHCC denies the request for an amendment, the SHCC must link or append all relevant, written documents pertaining to the request to the information that is subject to the request, including the written request, denial, statement of disagreement and rebuttal.

D. Accounting of Disclosures

The individual has a right to receive an accounting of disclosures of PHI that have been made by the SHCC within the last six years, or back to when compliance was first required by HIPAA, whichever occurred last. The individual may request an accounting for any time period less than the six years.

If the individual has not had an opportunity to agree or object or authorize the disclosure, the principle of the Privacy Rule is that the individual has the right to know about the disclosure by requesting an accounting.

The SHCC is *not required to provide an accounting* to the individual for the following uses and disclosures:

1. To carry out treatment, payment, and health care operations (TPO), including the SHCC's teaching activities;
2. To the individual or the individual's personal representative;

3. Those disclosures authorized by the individual, including marketing or media relations that have been authorized;
4. As part of a limited data set (treatment, payment and operations only) so long as a data use agreement is in place;
5. Incidental uses and disclosures, so long as the minimum necessary standard is met and appropriate safeguards are in place;
6. For the facility's directory;
7. Persons involved in the individual's care;
8. For notification purposes to family members, relatives, friends, etc.;
9. For fundraising purposes, as long as the SHCC has only used or disclosed the individual's demographics and dates of service, or the individual has provided an authorization;
10. Disaster relief purposes;
11. To a health oversight agency, law enforcement official so long as:
 - a. They provide the SHCC with a written statement that says an accounting to the individual could reasonably impede the agency's activities and provides for a time limit to the suspension of the accounting; or
 - b. If the statement is made orally, the SHCC must document the state and identify of the official making the statement and limit the suspension to no more than 30 days unless a written statement is subsequently submitted during the 30 days;
12. National security or intelligence purposes;
13. To correctional institution; and
14. Information that was used or disclosed prior to April 2003.

The SHCC must provide the individual with a written accounting that meets the following requirements:

1. The date of the disclosure;
2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. A brief description of the PHI disclosed;
4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; and
5. If there have been multiple disclosures of the individual's PHI to the same person or entity for a single purpose, the accounting may include the information required for the first disclosure, date of the last disclosure and the number of disclosures made during the accounting period.

E. Right to Request Restrictions

An individual has the right to request restrictions on how the SHCC will use and disclose PHI for treatment, payment or health care operations as described in the Notice. The SHCC must provide the individual with an opportunity to request restriction of uses and disclosures of PHI and to disclosures to family members, relatives, friends and others. The SHCC has no obligation to agree to the

requested restrictions, but will honor all reasonable requests that involve celebrity, patient safety or social stigma. If the SHCC does agree, it must honor the agreed-to-restrictions unless and until they are revoked, except if the individual is in need of emergency treatment. In an emergency, restricted information may be used for treatment, but no further disclosures may be made.

The decision to accept a restriction may be an administrative one, covered by policy, or may require review. The campus or system Privacy Officer should review all requests for restrictions that are not authorized by policy or of a questionable nature. The SHCC should implement local procedures that provide a systematic way of communicating restrictions to staff. Never include sensitive information in postcard mailings or send PHI to an unsecured fax machine.

If the requested restrictions interfere critically with patient care, treatment or operations, and the patient is unwilling to modify the request, the entity within the SHCC may decide to refuse to care for the individual. Issues arising from implementation of this policy will be referred to the Privacy Officer for adjudication.

F. Facility Directory—Right to Opt Out

A facility directory is the information resource maintained by a covered entity to provide visitors, callers and others with information concerning a patient's location in the medical facility. So long as the SHCC provides the individual with Notice that certain information will be included in the entity's Facility Directory and provides the individual with the opportunity to restrict the disclosures, the SHCC may include the individual's name, location and condition in a facility directory and disclose that information to others who ask for the individual by name. The SHCC may also provide the individual's religious affiliation to clergy, unless the individual objects.

The SHCC must honor an individual's request to opt out of the Facility Directory.

In emergency treatment circumstances that do not require the SHCC to provide Notice to the individual, the individual's information contained in the Facility Directory may be used or disclosed in accordance with the patient's prior expressed preference or in the patient's best interest as determined by the SHCC. In such circumstances, the individual must receive the Notice as soon as practicable and if the individual then objects to use of PHI in the Facility Directory, the SHCC must comply with that request.

G. Confidential Communications

The SHCC must permit individuals to request and must accommodate reasonable requests to receive communications of PHI from the SHCC by alternative means of communication or to alternative locations. The SHCC cannot require the individual to explain the reason for the request.

The SHCC will accommodate requests if:

- a. Requests are in writing to the responsible SHCC individual with specific instructions as to location, address or fax number and include individual's signature and dated;
- b. The request is for electronic communications via e-mail or fax, so long as the individual has provided a signed request for electronic communications; and
- c. When the requests are for mailed communications, other than standard first class mail, the individual provides payment in advance for all costs of mailing to one or more alternative locations (e.g., Federal Express, express mail, etc.).

SECTION IV: PERMITTED USE AND DISCLOSURE OF PHI

A. Permitted Uses and Disclosures *without* authorization

So long as the SHCC's Notice of Privacy Practices includes a description of these practices, the SHCC may use or disclose PHI for the following purposes without the individual's authorization:

1. To the individual or to the Department of Health and Human services to investigate compliance with the Privacy Rule, without limitation;
2. For its own treatment, payment and health care operations (TPO) so long as the SHCC has provided the individual with Notice and made a good faith effort to obtain the individual's signed Acknowledgment;
3. For the treatment activities of any health care provider, including those not covered by the Privacy Rule;
4. To another covered entity or a health care provider (including those not covered by the Privacy Rule) for the payment activities of the entity or provider that receives the PHI;
5. To another covered entity for certain health care operations of the entity that receives the information when
 - a. Each entity has or had a relationship with the individual who is the subject of the information and the information pertains to the relationship; and
 - b. The disclosures is for those health care operations activities and include quality-related health care operations, teaching activities or for purpose of health care fraud and abuse detection or compliance;
6. With a limited data set or deidentified data set;

7. For psychotherapy treatment by the originator of the psychotherapy notes (all other uses and disclosures require the individual's authorization); or
8. For certain functions related to government or public health activities.

Unwarranted access by a SHCC employee to a fellow employee's PHI is a violation of the Privacy Rule and UC policy. The Privacy Rule allows access for treatment, payment and some healthcare operations. If an employee is not required by his or her job responsibilities to carry out these activities, then the UC SHCC policy prohibits access, unless the patient/employee provides written authorization.

When the SHCC's covered health care providers have a teaching relationship with another covered entity and the covered entity's patients under a UC teaching affiliation agreement or other legal agreement that describes the teaching relationship, the covered entities may share PHI regarding the individual so long as:

1. Both covered entities have a teaching relationship with the individual;
2. Each covered entity's Notice states that PHI may be exchanged by those entities for both teaching and treatment purposes when the institutions have a teaching relationship with the individual;
3. The minimum necessary standard applies; and
4. The covered entity's affiliation agreement contains language that restricts disclosures to those permitted under the Rule.

B. Permitted Uses and the Minimum Necessary Standard

The minimum necessary standard requires the SHCC to evaluate its practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI. The minimum necessary standard does not apply to:

1. Disclosures to or requests by a health care provider for treatment purposes;
2. Disclosures to the individual who is the subject of the information;
3. Uses and disclosures that have been authorized in writing by the individual;
4. Uses and disclosures required for compliance with HIPAA Administrative Simplification Rules;
5. Disclosures to the Department of Health and Human Services (HHS) for Privacy Rule enforcement purposes; or
6. Uses or disclosures that are required by law.

The covered entity within the SHCC must have a method to categorize and identify the persons or classes of persons who need access to PHI and the categories or types of PHI needed and the conditions appropriate to such access. Except for those purposes where the minimum necessary standard applies, all requests for the entire medical record or designated record set should be justified; otherwise, the request and disclosure by the SHCC may be a violation of the Rule. The SHCC may rely on the presumption that the requested PHI is minimum necessary when a request is from a public official, researchers with appropriate documentation from an Institutional Review Board (IRB), another

covered entity or a professional who is a member of the UC workforce or a business associate

Application of the Minimum Necessary Standard to the Use of PHI for Treatment Purposes. The minimum necessary standard applies to the use of PHI for treatment purposes, with use defined as “the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.” The SHCC determined that the patient’s health care team, including doctors, nurses, and housestaff may use the individual’s full medical record, without limitation, so that the patient has access to treatment protocols that provide for quality of care and so that the institutional and individual providers can comply with all state and other laws regarding appropriate and timely treatment.

Incidental Uses and Disclosures. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule. The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied *reasonable safeguards* to protect PHI and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure.

Each SHCC workforce member must be aware of those types of oral or written communications that pose some risk of incidental use or disclosure of PHI. Workforce members must take responsibility for maintaining confidentiality, where reasonably possible, when engaging in activities such as the following:

1. Face-to-face or telephone discussion of a patient’s condition or lab tests with other health care staff and providers, the patient or family members or others involved in the patient’s care;
2. Calling out a patient’s name in a waiting room; and
3. Discussing a patient’s condition during teaching rounds.

C. Authorization of Patient Required for Use/Disclosure

The SHCC must obtain a signed authorization for uses and disclosures that are not otherwise permitted by the Privacy Rule or required by law, including the following:

1. Use or disclosure of psychotherapy notes, *except*:
 - a. Use by the originator of the notes for treatment;
 - b. Use or disclosure by the SHCC of its own training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling; or
 - c. Use or disclosure by the SHCC to defend itself in a legal action or other proceeding brought by the individual; and

- d. Use or disclosure that is required or permitted with respect to oversight of the originator of the notes.
2. For marketing of PHI to third parties and the authorization must state whether the SHCC receives any direct or indirect remuneration from the third party. authorization is *not required* for:
 - a. Communications that are conducted face-to-face between the SHCC and the individual;
 - b. Communications that describe the SHCC's own products or services to an individual; or
 - c. Promotional gifts from the SHCC to the individual;
3. IRB-approved research protocol that requires informed consent and the individual's authorization;
4. Use of research data that was obtained prior to April 2003 with an IRB-approved Waiver of Consent, but the IRB has subsequently determined that the protocol post-April 2003 requires informed consent and/or the researcher wants to enroll new subjects and the criteria for a HIPAA required Waiver of authorization cannot be met;
5. Disclosure of PHI to the patient's employer (including those situations when the patient is a UC employee and the disclosure is to UC), *except*:
 - a. When the use and disclosure is for public health activities;
 - b. To conduct an evaluation relating to medical surveillance of the workplace; or
 - c. To evaluate whether the individual has a work-related illness or injury.
6. Use of a list for fundraising activities that has been created using disease or treatment PHI or that clearly identifies an individual and his/her specific disease or treatment;
7. Use and Disclosure of PHI to the media or through other forms of external communications;
8. Creation of disease or treatment specific databases (that have not been de-identified or with limited data sets) for purposes of institutional advancement or external communications activities;
9. Use of disease or treatment-specific databases (that are not de-identified or limited data sets) created prior to April 2003 if those databases were not created with specific legal permission from the individuals whose PHI is included in the database;
10. The SHCC may not disclose PHI to another covered entity without authorization or the use of a limited or deidentified data set for the following operational activities of the other entity: resolution of internal grievances, customer service, medical review or auditing activities; or
11. In the cases of state civil subpoenas, the SHCC must be served either with the patient's authorization or a Notice to Consumers, along with the subpoena. For judicial and administrative proceedings in response to a court order, subpoena, discovery request or other lawful process, the SHCC should make sure that the requesting entity provides an authorization or has made reasonable efforts to notify the patient of such disclosure, has allowed time for the patient to object, that the patient has authorized or the court has resolved the issue through issuance

- of an appropriate order including a protective order. Seek the advice of the Office of the General Counsel when it is not clear if an authorization is required. The PHI should be returned or destroyed on completion of its use by the court or other requesting entity;
12. The SHCC must obtain authorization or use a deidentified data set when disclosing PHI to an Organ Procurement Organization (OPO) for purposes other than the purpose of facilitating organ, eye or tissue donation and transplantation; or
 13. When PHI regarding an injured worker's previous condition is not directly related to the claims for compensation.

When a member of the workforce is uncertain as to whether an authorization is required prior to disclosing PHI, he/she must consult with either the campus Health Information Management Service, the HIPAA Privacy Officer, University HIPAA Privacy Official, or the UC Office of the General Counsel.

D. Authorization Form

The SHCC must have written and specific authorization from an individual for uses and disclosures of PHI, unless the use or disclosure is required or permitted. In most cases, the SHCC may use or disclose PHI for treatment, payment and operations. A valid authorization must include an identification of the PHI to be used or disclosed, by whom (name or class of person), to whom, and an expiration date. A research authorization may state as the expiration date: "the end of the study" or "none" if the authorization is to establish a database for future use. The authorization must also include the following notifications to the individual:

1. The individual may revoke the authorization in writing and indicate how to do so;
2. Treatment, payment, enrollment or eligibility for benefits may not be conditioned on an authorization;
3. PHI may be redisclosed by the person receiving PHI, and in that case, the confidentiality of the PHI is no longer protected; and
4. When the authorization is for marketing purposes, the authorization must notify the individual of any direct or indirect remuneration to the SHCC from another party.

The UC model authorization form (available at <http://www.universityofcalifornia.edu/hipaa/auth.html>) should be used by all SHCC workforce members and entities in a 14-point Font. This authorization form, prepared by the Office of General Counsel in consultation with the HIPAA task force, contains all elements required by the rule and includes the required notifications in plain language. If the SHCC's authorization does not contain the required elements or if the information provided to the individual to sign is false (i.e., a deliberate misrepresentation of the truth), the authorization is not valid under the privacy Rule. Any use or disclosure of any PHI under those circumstances is a violation of the Privacy Rule.

The SHCC must obtain the individual's signature on the authorization form and provide the individual with a copy of the signed authorization form. When another individual has authority to sign on an individual's behalf, the SHCC must verify and document that person's authority to sign such legal permission. The SHCC must document and retain all signed authorizations for six years, including those provided by a researcher when obtaining PHI for an IRB approved protocol.

A patient has a right to revoke or modify an authorization for use or disclosure of PHI, and the SHCC will be bound by the revoked or modified authorization from that date forward, except to the extent that the SHCC has taken action in reliance on the authorization or if the authorization was obtained as a condition of obtaining insurance coverage and other laws give the insurer the right to contest the claim or policy. The revocation has no effect on actions taken prior to the date of the revocation.

SECTION V: TRAINING

Training must be provided to all workforce members by the compliance effective date of April 2003 as relevant to their job responsibilities. Each campus and academic health center shall develop a training program for all new employees, faculty, trainees, students volunteers and others as reasonably soon after they join the University, but not later than 90 days.

Five separate UC HIPAA Privacy training modules have been developed as follows:

1. Basic Module for the general workforce on the basic principles of the Privacy Rule;
2. Provider Module for workforce members directly providing care to patients;
3. PHI Management Module designed to provided detailed information on policies and procedures for staff who disclose or provide access to PHI as part of their job functions, or interact with patients regarding their health information requests or questions;
4. Research Module with a focus on research implication of the Privacy Rule; and
5. Media/Fundraising and Marketing Module for staff working in the specialized areas of media relations, marketing and the Development Offices.

SECTION VI: MITIGATION

When an improper use or disclosure of PHI is the result of an innocent mistake, rather than neglect or deliberate disregard, Department of Health and Human Services (DHHS) expects that the SHCC will demonstrate that policies and procedures have been implemented to minimize such occurrence in the future and that steps have been taken to mitigate the impact of that disclosure. The SHCC must have in place a mitigation process to minimize the effect on the individual of improper uses and disclosures and to

comply with state law regarding the notification of individuals. This process will include, where workable and practicable, efforts to:

1. Contain the damage and stop further use or disclosure;
2. Utilize violations as a means to identify system lapses and to modify policies or procedures; and
3. Inform patients, where appropriate, of any improper use or disclosure arising from a violation of HIPAA regulations.

SECTION VII: ADMINISTRATIVE REQUIREMENTS

The Privacy Rule mandates the following administrative requirements:

1. Train the workforce members and document the training;
2. Implement reasonable institutional and individuals safeguards to protect PHI;
3. Provide a process for individuals to make complaints to the SHCC;
4. Establish and apply appropriate sanctions against workforce members who fail to comply with the Privacy Rule or UC policy and document applied sanctions;
5. Mitigate to the extent possible any known harmful effects of a violation of the Privacy Rule or policies;
6. Refrain from intimidating or retaliatory acts; and
7. Establish policies and procedures.

The Privacy Rule requires the SHCC to document and retain for six years the documentation of the following:

1. Business Associate Agreements—document and maintain copies of all Business Associate agreements;
2. Authorizations—document and maintain copies of all signed patient authorizations and document that there has been verification of the person's right to sign on behalf of the patient;
3. Waiver of authorizations for Research purposes—documentation of certification from the researcher requesting PHI that the IRB has approved a Waiver of authorization and met the HIPAA required criteria for a Waiver of authorization
4. Notice of Privacy Practices—maintain copies of the Notice, written acknowledgement of the receipt of the Notice, and document a good faith effort to obtain written acknowledgement when the patient refuses to provide written acknowledgement.
5. Restrictions on practices described in the Notice—document any agreed to restrictions;
6. Access or copying of the DRS—document that the DRS that is subject to access by individuals and the titles of the persons or offices responsible for receiving and process requests for access by individuals; document responses to requests for access or copying as required;

7. Amendments—document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals; document responses to requests for amendment as required;
8. Accounting—document the information required to be in an accounting, the written accounting that is provided to the individual, the titles of the persons or offices responsible for receiving and processing requests for an accounting; statement of the law enforcement or health oversight agency or official (if made orally) who has requested that the SHCC temporarily suspend accounting because it could impede the agency’s activities; document responses to request for an accounting as required;
9. Personnel designations—document the privacy official and contact person or office who is responsible for receiving complaints;
10. Training—document that the SHCC has provided training to all members of the workforce on the policies and procedures as necessary and appropriate for the members to carry out their function within the covered entity;
11. Complaints—document all complaints received and their disposition, if any;
12. Sanctions—document any sanctions that are applied against members of the workforce who fail to comply with the privacy policies and procedures of the SHCC;
13. Changes to policies and procedure or privacy practices as described in the Notice—document any changes to policies and procedures prior to the effective date of the change and make appropriate changes to the notice; and
14. SHCC’s HIPAA Policies and procedure—document system and local policies and procedures.

While not specifically required in the Privacy Rule, the SHCC determined that it is in the best interest of the patient, and UC to remain documentation of:

1. Data use agreements;
2. Verification of identify of public officials requesting information;
3. Patient written requests for restrictions;
4. Patient written requests for access to or copies of the DRS, SHCC response to the patient’s request, written denial of the request, written statement of any delays in taking timely action on the request;
5. Patient request for amendments to PHI, SHCC’s written denial of the amendment, written statement for reasons for delay in responding to requests, patient’s written statement disagreeing with the denial of the amendment, SHCC’s written rebuttal
6. Patient written requests for an accounting, written statement of the reasons for delay in responding to request;
7. Patient written requests for confidential communications of PHI and SHCC response;
8. SHCC’s training materials;
9. Written documentation of a law enforcement or health oversight agency request to temporarily suspend a disclosure to law enforcement from the accounting provided to a patient;
10. Researcher’s request for PHI, including requests for decedent information.

SECTION VIII: DEFINITIONS

Protected Health Information (PHI) is an individual's health information that is:

1. Created or received by a health care provider, plan, or clearinghouse;
2. Relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual;
3. Identifies the individual, or is reasonably believed could identify the individual; and
4. Is transmitted or maintained in any form or medium.

Analyzing when an individual's health information is PHI. The key determinant as to whether or not information is PHI and protected is the *function* being performed by the University and the purpose for which the University has the medical information, not its record keeping practices. For example, the results of a fitness for duty exam are PHI when UC as a provider and part of the SHCC administers the test to a UC employee. When the employee authorizes UC, the health care provider, to turn over the information to UC, the employer, it is a part of the employee's employment record. The information is no longer PHI and not protected by the Privacy Rule. It is important to note that in most circumstances (see UC's Notice of Privacy Practices), the employee must provide a signed authorization to the UC health care provider to release the information to the UC employer.

The Designated Record Set (DRS) is a group of records that *includes* PHI and is maintained, collected, used or disseminated by or for a covered entity (e.g., the UC's SHCC) for each individual that receives care from a covered individual or institution and is:

1. The medical records and billing records about individuals maintained by or for a covered health care provider (can be in a business associates records);
2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
3. Used, in whole or in part, by or for the covered entity (SHCC) to make decisions about individuals.

The SHCC creates a deidentified data set by removing the following 18 identifiers of the individual or of relatives, employers, or household members of the individual:

1. Name;
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census;

- (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
 4. Telephone numbers;
 5. Fax numbers;
 6. Electronic mail addresses;
 7. Social security numbers;
 8. Medical record numbers;
 9. Health plan beneficiary numbers;
 10. Account numbers;
 11. Certificate/license numbers;
 12. Vehicle identifiers and serial numbers, including license plate numbers;
 13. Device identifiers and serial numbers;
 14. Web Universal Resource Locators (URLs);
 15. Internet Protocol (IP) address numbers;
 16. Biometric identifiers, including finger and voiceprints;
 17. Full face photographic images and any comparable images; and
 18. Any other unique identifying number, characteristic, or code.

Under HIPAA's "safe harbor" standard, information is considered deidentified if all of the above identifiers have been removed, and there is no reasonable basis to believe that the remaining information could be used to identify a person.

The covered entity may assign a code or other means of record identification to allow deidentified information to be reidentified, if the code is not derived from, or related to, the removed identifiers. (Only the covered entity will have the re-linking information and must provide for the security of the code.)

Alternatively, under the "statistical" standard, a covered entity may determine that health information is not individually identifiable (and thus protected) health information if:

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and that person documents the methods and results of the analysis that justify such determination.

As an alternative to using fully deidentified information, HIPAA makes provisions for a “limited data set” from which direct identifiers (like name and address) have been removed, but not indirect ones (such as age). Limited data sets require a “data use agreement” with the party to which/whom it is provided. [45 CFR 160.103, 45 CFR 164.502(d)].