Berkeley
UNIVERSITY OF CALIFORNIA

Nicholas B. Dirks
CHANCELLOR
PROFESSOR OF HISTORY
PROFESSOR OF ANTHROPOLOGY

200 California Hall #1500
Berkeley, CA 94720-1500
510 642-7464
510 643-5499 FAX
chancellor@berkeley.edu

February 23, 2017

Campus Privacy Officer
Lisa Ho

Dear Lisa,

Effective immediately, and in accordance with Section D of the UC HIPAA Administrative Requirements Policy, I am delegating to you, as the Campus Privacy Officer, the designation of Berkeley Campus HIPAA Privacy Officer.

The Berkeley Campus HIPAA Privacy Officer works in collaboration with the Berkeley Campus HIPAA Security Officer to serve as campus liaison to the UC HIPAA Privacy and Security Officials at the Office of the President. The Berkeley Campus HIPAA Privacy and Security Officers are jointly responsible for campus compliance with the bullet-pointed objectives listed on page 5 of the HIPAA Administrative Requirements Policy, attached.

Sincerely,

[redacted]

Nicholas Dirks

Enclosure:
UC HIPAA Administrative Requirements Policy

cc: Chief Ethics, Risk and Compliance Officer K. Griscavage
Chief Information Officer L. Conrad
Chief Campus Counsel C. Patti
Chief Audit Executive W. Riley
CCRC Coordinator C. Gutierrez
Delegations Coordinator L. DeBerry

University of California Policy

HIPAA Administrative Requirements

Responsible Officer: Senior Vice President/Chief Compliance and Audit Officer

Responsible Office: Ethics, Compliance and Audit Services

Effective Date: September 13, 2010

Next Review Date: September 1, 2013

Who is Covered: All UC HIPAA workforce members

Contents

- **Policy Summary**
- **Policy Definitions**
- **Policy Text**
- **Approval Authority**
- **Compliance and Reporting**
- **Implementation Procedures**
- **Related Documents**
- **Frequently Asked Questions**
- **Revision History**

Policy Summary

Under the provisions of the Health Information Portability and Accountability Act of 1996 (HIPAA), organizations that are subject to HIPAA have certain responsibilities, which are described in this policy. This policy identifies the components of the University of California (UC) that are subject to HIPAA, identifies the roles and responsibilities of privacy officials within UC, and describes mandatory training requirements for HIPAA and requirements for policies, procedures, and documentation.

Policy Definitions

Refer to the document entitled "UC HIPAA Glossary".

Policy Text

The University of California (UC) is a Hybrid Entity, as defined in the HIPAA Privacy Rule. Consequently, this policy identifies and defines the Covered Components of UC as follows.

A. Designation of Covered Components of UC

The following UC entities and members of their workforces collectively form UC's Single Health Care Component (SHCC) and, as such, are subject to the HIPAA regulations and UC's systemwide HIPAA policies:

- The medical centers and clinics at Davis, Irvine, Los Angeles, San Diego, and San Francisco, and any future such entities that may be created;
- Clinical operations of the health professional schools at various campuses that, as individual organizational units, perform covered functions (i.e., as health care providers, engage in covered transactions);
- Student Health/Counseling Centers[1] at all campuses;
- Internal Employee Assistance programs (i.e., staffed by UC employees and operated using UC resources);
- Occupational Health Centers at those campuses that provide clinical services; and
- Any other UC entities that engage in covered functions with Protected Health Information.

The following UC entities and members of their workforces collectively form UC's Single Health Plan Component (SHPC) and, as such, are subject to the HIPAA Privacy Rule and UC's systemwide HIPAA policies for Group Health Plans:

- UC self-insured health or group health plans.

B. Designation of UC Workforce Members Who May Provide Business, Finance, Legal or other Services to Covered Entities

The following entities and their workforce members in the UC Office of the President (UCOP), and at UC campuses may provide business, legal, financial or administrative functions on behalf of the SHCC or SHPC and are part of the SHCC or SHPC when performing those functions that require the use and/or disclosure of PHI on behalf of the SHCC or SHPC:

- Board of Regents and the President's Immediate Office;
- Business Operations;
- Office of the General Counsel;

---

[1] Note that student records covered by FERPA are excluded from the definition of Protected Health Information, and therefore are not subject to the HIPAA Privacy and Security Rules, unless the Student Health/Counseling Center Notice of Privacy Practices has made an affirmative representation to students that their records will be protected under the HIPAA Privacy and Security Rules. Student Health/Counseling Centers are subject to the Rules with respect to non-student records, if they bill electronically for services rendered to non-students.

- Institutional Review Boards (IRBs);
- Health Sciences and Services;
- Information Resources and Communications;
- External Relations;
- Institutional Advancement or Development Office(s);
- Risk Services;
- Innovation Alliances and Services; and
- Other UC entities that perform functions on behalf of entities within the SHCC or SHPC using PHI.

When the same workforce members perform functions on behalf of non-covered entities within UC, these functions are not performed on behalf of the SHCC or SHPC and are not covered by HIPAA. Workforce members must never disclose PHI to non-covered UC entities without the member's authorization or as otherwise allowed or required by applicable laws, regulations, and policies.

C. UC Entities and Individuals Who May Use or Disclose an Individual's Identifiable Health Information (IIHI), but Are Not Part of the SHCC

The Privacy Rule does not apply to employment functions or certain academic administrative functions[2] of UC, or to employment and student records. When UC is carrying out its role as employer, those workforce members providing these services are not subject to HIPAA, except when UC, the plan sponsor, has certified to the insured health plans that PHI will be protected as defined in the plan documents. With certain exceptions,[3] UC must obtain written authorization from individuals in order to obtain PHI from covered components within the SHCC or SHPC and in order to carry out employment-related activities. Examples of UC entities and workforce members that are not part of the SHCC or SHPC, and are not covered by HIPAA are student admissions offices, and disability and worker's compensation functions.

However, in all circumstances, either state or federal law and/or UC policy provides for confidentiality of that information and prohibits the use of an individual's health information for employment-related decisions. The fact that the Privacy Rule does not apply does not lessen

---

[2] For example, UC employees who work in the campus admissions office or student assistance offices may use individually identifiable health information in their capacity as admissions officers to provide services to students requesting special academic, housing or meal accommodations for medical reasons. UC has determined that those are non-covered activities under HIPAA, although state and federal law regarding the protection of student records will apply.

[3] The SHCC may disclose PHI to the employer under limited circumstances (e.g., medical surveillance of the workplace or to evaluate work-related injury or illness, or its obligations under 29 CFR parts 1904-1928, 30 CFR parts 50-90, or state law) so long as the covered health care provider gives notice in the Notice of Privacy Practices that this disclosure will occur and provides an accounting of this disclosure to the individual if the individual requests an accounting. Privacy Regulation Text, October 2002, p. 16.

any current protections for that information. In the case of those individuals, such as benefits managers, customer service representatives or health care facilitators, who may use health information to provide services to UC group health plan members, the UC plan sponsor must certify to the health plan that the information will not be used for employment-related decisions and that those individuals will provide the HIPAA-required protections for an individual or member's health information.

D. UC HIPAA Official(s), and Chancellor-appointed HIPAA Officials
The University of California must designate UC HIPAA Privacy and Security Officials (may be one individual) who will also serve as the HIPAA-required contact person(s) and contact office(s) for systemwide issues. The UC HIPAA Privacy and Security Official currently reports directly to the Senior Vice President /Chief Compliance and Audit Officer within the Office of the President.

The responsibilities of the UC HIPAA Privacy and Security Official(s) include:

- Overseeing all ongoing activities related to the development, implementation, maintenance of and adherence to UC's policies and procedures covering the privacy of and access to patient health information in compliance with HIPAA;
- Maintaining current knowledge of applicable federal and state privacy laws and coordinating with other UC divisions regarding federal and state laws and the institution's privacy practices that may impact the University's compliance with HIPAA;
- Posting, modifying and updating all systemwide HIPAA policies and the text of the systemwide Notice of Privacy Practices, in consultation with the Office of the General Counsel and SHCC and SHPC HIPAA Officers. Modifications and updates will be implemented if they are required by changes in federal or state law or as needed to respond to UC policy changes;
- In consultation with the SHCC and SHPC HIPAA Officers, developing mechanisms that provide assurance to the Board of Regents that HIPAA-required documentation is accomplished and maintained by the appropriate covered entities within the SHCC and SHPC and at the system level;
- Coordinating with SHCC Compliance Officers, the Office of the General Counsel, Risk Services, Internal Audit, HIPAA Officers and others as necessary to provide a response to individual complaints, identify and mitigate potential violations, respond to breaches, provide further information about matters covered by the Notice of Privacy Practices and apply and document appropriate sanctions for failures by the workforce to comply with HIPAA, State privacy laws and regulations, and UC HIPAA policies;
- In coordination with the SHCC and SHPC HIPAA Officers, developing processes for using complaints, incidents, and breaches as evaluative and improvement tools;
- Developing, in coordination and consultation with the SHCC and SHPC HIPAA Officers, workforce training, assuring that it is developed, and developing a process to provide assurance to the Board of Regents that required training and documentation has been accomplished;

- Organizing and managing a systemwide HIPAA privacy and security governance structure; and
- Reporting to executive management at the local and system level, as appropriate, and to the Board of Regents, when appropriate or necessary.

The Chancellor of each campus must designate the individual(s) who will be accountable to the Chancellor or his or her designee for each covered component's compliance with HIPAA, serve as the campus liaison(s) to the UC HIPAA Privacy and Security Official(s), and carry out the following responsibilities in coordination with the efforts of the SHCC HIPAA Officers and UC's HIPAA Privacy and Security Official(s):

- Manage the development, implementation, and revisions of the covered component's policies and procedures necessary for carrying out the requirements of the federal HIPAA requirement and UC HIPAA policies;
- Ensure that all required HIPAA training is accomplished and documented in written or electronic form, and retain the records for at least six years;
- Provide information on required HIPAA training compliance to the systemwide privacy official upon request;
- Serve as the covered component's liaison to UC's HIPAA Privacy and Security Official(s);
- Serve as the covered component's contact person responsible for resolving HIPAA complaints, managing HIPAA investigations, responding to incidents and breaches, and providing information regarding the covered component's HIPAA program to senior executives, UCOP, and external regulatory agencies such as OCR;
- Serve as the covered component's individual(s) responsible for assuring that HIPAA-required mitigation, complaint, and sanction policies and procedures are implemented and documented;
- Assure that HIPAA- required documentation (see Section F, below) is accomplished and records are maintained by the covered component, and provide requested reports to UCOP and campus management;
- Responsible for periodic reporting to and prompt notification of significant HIPAA incidents or issues to campus management, and to the UC HIPAA Privacy and Security Official(s);
- Responsible to ensure appropriate HIPAA breach response activities and associated external notifications occur, as required.

E. Mandatory Training Required for HIPAA

Each covered component within the SHCC and the SHPC must train its workforce members on the systemwide HIPAA policies and any relevant local procedures necessary for workforce members to perform their assigned job functions.

Each covered component within the SHCC and SHPC shall provide a program to train new employees, faculty, trainees, students, volunteers and other workforce members to ensure that

they complete their required HIPAA training prior to gaining access to Protected Health Information soon after they join the University, but no later than 90 days thereafter. When significant changes occur in the job description of current employees or to policy and/or procedure, the affected workforce members will be trained as soon as possible after such changes.

Each covered component is responsible to determine whether other personnel such as individuals under affiliation agreements, staff of a business associate, or a contracted organization that is not a business associate (such as cleaning services), or infrequent volunteer-type personnel, such as holiday choirs, entertainers, students exploring careers, etc., are required to complete the covered component's HIPAA training or their own organization's HIPAA training, sign a confidentiality agreement or the like, or execute a business associate agreement, if appropriate.

HIPAA training provided by any covered component of the SHCC meets the HIPAA training requirements under this policy for all other SHCC covered components. However, covered components are still required to provide training on unique local policies, procedures, or job functions, as necessary.

F. Documentation and Retention of HIPAA Policies and Procedures
Covered components must maintain their local policies and procedures required by HIPAA or UC HIPAA policy in written or electronic form for six years. UC HIPAA policies may be accessed at the University's HIPAA website: http://www.universityofcalifornia.edu/hipaa, or by contacting the UC HIPAA Privacy and Security Official(s), or the UCOP Office of Ethics, Compliance, and Audit Services.

G. Documentation and Retention of HIPAA-Required Documentation
HIPAA requires the SHCC and SHPC to document and retain for six years the following:

- Business Associate Agreements—all signed Business Associate Agreements;
- Authorizations—all signed Patient Authorizations and, if appropriate, verification of the person's right to sign on behalf of the patient;
- Waiver of Authorizations for Research Purposes—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;
- Notice(s) of Privacy Practices—copies of the Notices, written acknowledgements of receipt, and documentation of good faith effort to obtain written acknowledgement when the patient refuses to provide written acknowledgement;
- Patients' Requests for Restrictions—all agreed-to restrictions;
- Access or copying of the Designated Record Set (DRS)—document the DRS that is subject to access by individuals and the titles of the persons or offices responsible for receiving and processing requests for access by individuals; document responses to requests for access or copying, as required;

- Amendment—document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals; document responses to request for an amendment, as required;
- Accounting of Disclosures—document the information required to be provided if an accounting of disclosures is requested;
- Personnel Designations—document the privacy official and contact person or office who is responsible for receiving complaints;
- Training—documentation demonstrating that each individual workforce member has completed his/her required HIPAA training on the policies and procedures as necessary and appropriate for the members to carry out their functions within the covered component;
- Complaints/Investigations—document all complaints received and their disposition, if any;
- Sanctions—document any sanctions that are applied against members of the workforce who fail to comply with HIPAA policies and procedures, if any;
- HIPAA Policies and Procedures---document local policies and procedures, and any changes to the policies and procedures; and
- Any other communication, action, activity or designation that, under the Privacy Rule, must be maintained in writing or otherwise documented.

While not specifically required in the Privacy Rule, UC has determined that it is in the best interest of the patient, the member, and UC to retain documentation for the following (note: HIPAA requires that the covered entity provide written responses in all of the following circumstances involving patient requests, but does not require the patient or member to provide written requests):

- Data Use Agreements;
- Verifications of identity of public officials requesting information;
- Patient written requests for restrictions;
- Patient written requests for access to or copies of the DRS, the SHCC's response to the patient's request, written denial of the request, written statement of the reason for a delay in taking timely action on the request, written rebuttal statement, and any other written actions;
- Patient written requests 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;
- Patient written requests for an accounting of disclosures, written statement for reasons for delay in responding to requests;
- Patient written requests for confidential communications of PHI and SHCC response;

- SHCC's and SHPC's training materials;
- When a law enforcement or health oversight agency has submitted a written request to temporarily suspend accounting of disclosures, the SHCC or SHPC must document the written request;
- Notification of victims of abuse, neglect or domestic violence—notify the individual of any disclosures to governmental agencies or, if the professional determination has been made not to notify the individual or individual's personal representative, document the reason for the determination;
- Permitted disclosures for judicial and administrative proceedings—documentation required from a party seeking PHI in a judicial or administrative proceeding must be maintained by the SHCC; and
- Researcher's request for decedent information—SHCC may request documentation from researcher of death of subject.

Approval Authority

Implementation of the Policy: Senior Vice President/Chief Compliance and Audit Officer
Revisions to the Policy: Senior Vice President/Chief Compliance and Audit Officer
Approval of Actions: not applicable

Compliance and Reporting

N/A

Implementation Procedures

UC Organizational Units subject to HIPAA are responsible for implementation.

Related Documents

45 CFR 164.504, 164.514, 164.530

Business and Finance Bulletin RMP-2, *Records retention and disposition*

Business and Finance Bulletin IS-3, *Electronic Information Security*

Frequently Asked Questions

FAQs may be found on the UC HIPAA website.

Revision History

HIPAA Privacy Rule: University of California Systemwide Standards and Implementation Policies (System Standards), April 2003.