UC SANTA BARBARA POLICY AND PROCEDURE

HIPAA Privacy Policy
Contact: **Student Health Service**
Revised: **September 2010**; Supersedes July 2008
Pages: **6**

IMPLEMENTING GUIDELINES FOR SYSTEMWIDE HIPAA PRIVACY POLICY

I. SCOPE

This policy governs all ancillary and covered components, workforce members, and the implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements at UCSB.

II. DEFINITIONS

Ancillary Components:
Components and workforce members who perform administrative, business, finance, and legal activities or functions on behalf of the University's health care providers or plans when those functions involve the use or disclosure of protected health information that has been created or received by the University's covered components (see Appendix B: UCSB Ancillary Components).

Covered Components:
All health care providers or health plans that use or disclose protected health information and their workforce members (see Appendix A: UCSB Covered Components).

Health Insurance Information (as defined by California Assembly Bill 1298):
An individual's:

1) Health insurance policy number or subscriber identification number, or
2) Any unique identifier used by a health insurer to identify the individual, or
3) Any information in an individual's application and claims history, including any appeals records.

Medical Information (as defined by California Assembly Bill 1298):
Any information regarding an individual's:

1) Medical history, or
2) Mental or physical condition, or
3) Medical treatment or diagnosis by a health care professional.

Protected Health Information (PHI) (as defined by Federal HIPAA legislation):
Information that identifies the individual or it's reasonably believed could identify the individual and is transmitted or maintained in any form or medium **and**:

1) Is created or received by a health care provider, plan, or clearinghouse; **and**
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.

Workforce Members:

Include academic and staff employees, volunteers, trainees, and others "directly controlled" by the covered or ancillary component.

III. POLICY

A. All UCSB covered and ancillary components shall abide by the University of California System-wide HIPAA Standards and implementation Policies (UC HIPAA Privacy Policy) to achieve compliance with the Standards for Privacy of Individually Identifiable Health Information (the HIPAA Privacy Rule). Individual covered or ancillary components may promulgate more stringent requirements.

B. To achieve compliance with the HIPAA Security Rule, all UCSB covered and ancillary components shall abide by the University of California Guidelines for Compliance with the HIPAA Security Rule (UC HIPAA Security Guidelines).

C. Reporting Violations: All known or suspected HIPAA privacy or security violations (accidental or deliberate) involving medical or health insurance information or PHI, must be reported immediately to the UCSB HIPAA Compliance Officer. If the protected information was in an electronic unencrypted format, the UCSB HIPAA Compliance Officer shall notify the UCSB Sensitive Data Incident Coordinator. The UCSB Sensitive Data Incident Coordinator shall coordinate the assessment of reported breaches consistent with UCSB Implementing Guidelines for SB 1386 and AB 1298.

D. Sanctions: The HIPAA Privacy Rule states that individuals who fail to comply with the Rule may be subject to civil or criminal liability, and mandates that the University apply appropriate sanctions for violations. Therefore, a university workforce member who fails to comply with the HIPAA Privacy Rule, the UC HIPAA Privacy Policy, and/or this policy may be subject to, in addition to possible civil or criminal liability, discipline up to and including dismissal pursuant to applicable University policies, bargaining contracts and University processes.

IV. RESPONSIBILITIES

A. General: The Executive Director - Medical Services, Office of the President, has been designated the University's HIPAA Privacy Official.

The Chancellor of each campus is responsible for designating the individual who will be accountable for campus compliance with HIPAA. The Associate Director - Medical Informatics, Student Health Service, has been designated as the UCSB HIPAA Compliance Officer.

B. UCSB HIPAA Compliance Officer is responsible for:

1. Chairing the UCSB HIPAA Committee.

2. Serving as the UCSB liaison to the system-wide HIPAA Taskforce.

3. Receiving, documenting, and tracking the disposition of all complaints regarding the privacy and security of PHI.

4. Documenting and maintaining records that the workforce has completed HIPAA required training.

5. Reviewing risk assessments annually.

6. Maintaining a comprehensive risk analysis.

7. Receiving reports of unauthorized use or disclosure of medical or health insurance information or PHI and notifying the UCSB Sensitive Data Incident Coordinator if the protected information is in an unencrypted electronic format.

C. UCSB HIPAA Committee is chaired by the UCSB HIPAA Compliance Officer and consists of one representative from each covered and ancillary component. Representatives are typically management level employees who report directly to the department or unit head of the component.

1. Representatives of covered components are responsible for

a. Attending all meetings of the committee or sending a delegate.
b. Implementing HIPAA policies and procedures within the component.
c. Monitoring workforce training within the component to ensure workforce members complete their required training.
d. Maintaining a file of signed confidentiality statements.
e. Forwarding HIPAA Reminders to workforce members.
f. Updating a security assessment annually.
g. Completing annual surveys requested by the UC Privacy Official.
h. Maintaining required documentation for their component.
i. Receiving reports from their workforce members of unauthorized use or disclosure of medical or health insurance information or PHI and immediately notifying the UCSB HIPAA Compliance Officer.

2. Representatives of ancillary components are responsible for:

a. Identifying workforce members who may come into contact with PHI.
b. Monitoring workforce training within their component.
c. Maintaining a file of signed confidentiality statements.
d. Forwarding HIPAA Reminders to workforce members.
e. If they are an information technology service provider, updating a security assessment annually for the components for which they provide services.

D. Workforce Members of covered components and those workforce members of ancillary components that may come into contact with medical or health insurance information or PHI are responsible for complying with this policy, including:

1. Completing the training materials, developed by the system-wide HIPAA Taskforce, that are necessary to carry out their individual job responsibilities for the use and disclosure of medical or health insurance information or PHI.

2. Signing the required Confidentiality Agreement (see Appendix C) and protecting sensitive information including, medical and health insurance information and PHI. Individual covered or ancillary components may require a more stringent agreement than the generic Confidentiality Statement. To be consistent with the

prevailing community standard for full service medical and mental health practices, the departments of Student Health and Counseling Services also require workforce members to sign a Security Agreement (see Appendix D).

3. Seeking assistance from their HIPAA Committee representative if they have questions or concerns regarding the use and disclosure of PHI.

4. Immediately reporting known or suspected violations (accidental or deliberate) to their HIPAA Committee representative.

V. Required Documentation

A. Business Services maintains the repository of HIPAA related Business Associate Agreements and Amendments (BAA). All agreements and amendments must be reviewed by the appropriate department administrator, approved by the UCSB HIPAA Compliance Officer and authorized on behalf of the Regents by the Director, Business Services. Data exchange shall not take place until the Director, Business Services has signed the BAA.

B. Covered components shall retain the following records for six years:

1. Patient Authorizations that have been signed by the patient. When the authorization has been signed by someone other than the patient, additional documentation is required that verifies the signatory's right to sign on behalf of the patient.

2. Waiver of Authorizations for Research Purposes that certify a) the IRB has approved a Waiver of Authorization from a researcher requesting PHI and b) HIPAA-required criteria for a Waiver of Authorization has been met.

3. Notice of Privacy Practices and concomitant written acknowledgements of their receipt or records demonstrating a good faith effort to obtain written acknowledgement when patient refuses to provide written acknowledgement.

4. Agreed to restrictions on privacy practices described in the Notice.

5. Documentation of a) the titles of the persons or offices responsible for receiving and processing requests for access by individuals; b) responses to requests for access or copying of the DRS; and c) to whom access to or copying of the Designated Record Set (DRS) was granted.

6. Amendments, including the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and responses to requests for an amendment as required.

7. Accounting (see 164.503 (j)), including the written accounting that is provided to the individual; 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 covered component temporarily suspend accounting because it could impede the agency's activities; responses to requests for an accounting as required.

8. Confidentiality Statements. Individual covered or ancillary components may require a more stringent agreement than the generic Confidentiality Statement. To be consistent with the prevailing community standard for full service medical and mental health practices, the departments of Student Health and Counseling Services also require a signed Security Agreement (see Appendix D).

9. HIPAA Training Reports that reflect who has/has not completed the mandatory training in the covered or ancillary component.

C. UCSB HIPAA Compliance Officer shall retain the following records for six years:

1. HIPAA Training records for all affected workforce members.

2. Complaint Log of all complaints and their disposition.

3. Annual Risk Assessments reviewed by the UCSB HIPAA Compliance Officer.

4. A comprehensive Risk Analysis by the UCSB HIPAA Compliance Officer.

5. Sanctions applied against members of the workforce who fail to comply with the privacy policies and procedures.

VI. REFERENCES

A. UCSB HIPAA Administration

B. UCSB HIPAA Compliance Officer

C. UCSB Sensitive Data Incident Coordinator

D. HIPAA Privacy Rule

E. HIPAA Security Rule

F. Just Cause

G. UC HIPAA Privacy Policy

H. UC HIPAA Security Guidelines

I. UCSB HIPAA Confidentiality Agreement

J. UCSB HIPAA Security Agreement

VII. APPENDICES

A. UCSB Covered Components

1. Autism Research Center, Gevirtz Graduate School of Education

2. Counseling Services

3. Hosford Counseling & Psychological Services Clinic, Gevirtz Graduate School of Education
4. Benefits, Human Resources
5. Intercollegiate Athletics Training
6. Police Rescue Office
7. Student Health Service

B. UCSB Ancillary Components

1. Audit and Advisory Services
2. Billing – Accounts Receivable Office (BARC)[1]
3. Information Technology Group, Gevirtz Graduate School of Education
4. Office of Information Systems & Technology / Information Systems & Computing
5. Risk Management & Insurance, Business Services
6. Student Information Systems & Technology

C. UCSB Confidentiality Agreement for HIPAA

D. UCSB Security Agreement for HIPAA

[1] To the extent BARC acts as a clearinghouse for claims processing or provides other services for departments that may result in incidental contact with PHI in the form of detailed billing or payment records, the activities and workforce that provide those services are covered under HIPAA.

To the extent BARC provides billing, accounts receivable, statement and collection services for students in which the only health information is the name of the covered component it is acting as a financial service provider, not as a healthcare provider, payer or employer, and the activities and workforce that provide those services are not covered under HIPAA.