

HIPAA Security Rule Compliance Policy

Vice Chancellor, Information Technology

(Policy IT-0001)

I. Purpose/Scope

UC Santa Cruz is subject to the federal Health Insurance Portability and Accountability Act (HIPAA) Security Rule¹, which identifies legal requirements for the protection of electronic health information for health care providers and related entities. The purpose of this policy is to establish the requirement that all UCSC entities subject to the HIPAA Security Rule must implement an identified set of practices in order to fulfill and demonstrate compliance with the requirements of this legislation.

II. Background

The HIPAA Security Rule, adopted in 2003, establishes safeguards to ensure the confidentiality of “electronic protected health information” (ePHI)² as well as the appropriate access and use of this information. Discussions with University Counsel and Internal Audit establish to whom the HIPAA Security Rule applies.³

The UCSC Vice Chancellor, Information Technology (VC IT), as campus HIPAA Security Official and in consultation with the UCSC IT Security Committee, empowered a cross-functional sub-group of the UCSC HIPAA Security Compliance Team to develop a common set of practices (the *UCSC Practices for HIPAA Security Rule Compliance*⁴) which, when fully implemented, would fulfill and demonstrate compliance with the HIPAA Security Rule. This sub-group includes representatives from all campus units subject to the HIPAA Security Rule, Internal Audit, and ITS Security and management.

The VC IT also recognized this sub-group as the appropriate body to review and update these Practices annually, or more frequently in response to environmental or operational changes that affect the security of ePHI, as well as to determine whether each UCSC HIPAA entity has fully and appropriately implemented them.

III. Detailed Policy Statement

All UCSC entities subject to HIPAA Security Rule requirements must implement the *UCSC Practices for HIPAA Security Rule Compliance* or, for addressable implementation specifications⁵, identify compensating controls where it is not practical or possible to fully address the Practices as stated. Implementation of these Practices must be documented utilizing

¹ See Sec VII. References

² Electronic Protected Health Information, or ePHI, is patient health information which is computer based, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media.

³ See Sec IV. B. Definitions - *UCSC Entity Subject to HIPAA Security Rule Requirements*

⁴ See Sec VIII, Attachment 1

⁵ See Sec IV. A. Definitions - *Implementation Specifications*

the *UCSC HIPAA Security Rule Compliance Workbook*⁶, or a similar documentation tool, and must be reviewed and updated at least annually.

IV. Definitions

A. Implementation Specifications⁷

An “implementation specification” is an additional detailed instruction for implementing a particular standard. Each set of [HIPAA Security Rule] safeguards is comprised of a number of standards, which, in turn, are generally comprised of a number of implementation specifications that are designated as either required or addressable.

- **Required:** Required Standards and implementation specifications must be implemented as stated for compliance.
- **Addressable:** For addressable implementation specifications, it must be determined whether each specification is reasonable and appropriate. If it is, it must be implemented as stated. If it is not, the entity must document the reasons for this determination and implement alternative compensating controls, where reasonable and appropriate, or otherwise indicate how the intent of the Standard can still be met.

B. UCSC Entity Subject to HIPAA Security Rule Requirements

For the University of California, 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.⁸ At UCSC, entities to which the HIPAA Security Rule applies are determined through discussion with University Counsel and Internal Audit⁹.

In general, covered entities relating to the University of California include:

- **Covered Health Care Providers:** Any provider of medical or other health care services or supplies who transmits health information in electronic form in connection with a transaction for which HHS (US Dept of Health and Human Services) has adopted a standard.
- **Health Plans:** Any individual or group plan that provides or pays the cost of health care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- **Health Care Clearinghouses:** A public or private entity that processes another entity’s health care transactions from a standard format to a non-standard format, or vice-versa.

V. Getting Help

For help with...	Contact...
------------------	------------

⁶ See Sec VIII, Attachment 2

⁷ See Section VII. References – *US Dept of Health and Human Services, Centers for Medicare and Medicaid Services (CMS)*

⁸ See Section VII. References – *UC HIPAA Website*

⁹ See Sec VIII, Attachment 3, for a current list of UCSC entities subject to HIPAA Security Rule requirements

For help with...	Contact...
...questions about this policy, including attachments	ITS Service Manager for Community and Compliance: itpolicy@ucsc.edu, (831) 459-2779
...technical questions about implementing the <i>UCSC Practices for HIPAA Security Rule Compliance</i>	The ITS Support Center: 459-HELP, help@ucsc.edu , http://its.ucsc.edu/support_center/ , or M-F 8AM-5PM, 54 Kerr Hall ITS Divisional Liaison or local computer support: http://its.ucsc.edu/divisional_liaisons/index.php

VI. Applicability and Authority

This policy applies to all UCSC entities subject to HIPAA Security Rule requirements. See **Detailed Policy Statement** and **Definitions** for details.

The campus Vice Chancellor, Information Technology on behalf of the Office of the Chancellor is the campus HIPAA Security Official and the campus authority for the *HIPAA Security Rule Compliance Policy*. This policy was originally reviewed and approved by the Campus Provost/Executive Vice Chancellor on 12/20/2006. It will be reviewed annually in conjunction with the annual review of campus HIPAA Security Rule compliance.

VII. References

Federal

The HIPAA Security Rule ([US] Department of Health and Human Services, Office of the Secretary, *45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule*): <http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>

US Department of Health and Human Services, Centers for Medicare and Medicaid Services (CMS): http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp and <http://www.cms.hhs.gov/SecurityStandard/>

University of California

UC HIPAA Website: <http://www.universityofcalifornia.edu/hipaa/>

UC Santa Cruz

UCSC HIPAA Security Rule Website: <http://its.ucsc.edu/security/policies/hipaa.php>

VIII. Attachments – all available online at <http://its.ucsc.edu/security/policies/hipaa.php>

Attachment 1: *UCSC Practices for HIPAA Security Rule Compliance*

Attachment 2: *UCSC HIPAA Security Rule Compliance Workbook*, to document implementation of the *UCSC Practices for HIPAA Security Rule Compliance*

Attachment 3: Current list of *UCSC entities subject to HIPAA Security Rule requirements*