



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

Introduction

All UCSC entities subject to the HIPAA Security Rule must implement the *UCSC Practices for HIPAA Security Rule Compliance* and document their implementation¹. The UCSC HIPAA Security Rule Compliance Workbook has been developed to facilitate this documentation. This Workbook contains all HIPAA Security Rule Standards and Implementation Specifications² along with associated UCSC Practices for Compliance and a format for documenting implementation of these Practices. The HIPAA Security Rule Compliance Team is responsible for reviewing compliance documentation and identifying potential gaps. For information about the development of the *UCSC Practices for HIPAA Security Rule Compliance*, please see the 1-page introduction available at http://its.ucsc.edu/security/docs/hipaa_cover.pdf.

Instructions for Completing this Workbook

The individual responsible for HIPAA Security Rule compliance, or his/her designee, should complete the unit/department information below and all “Implementation for Compliance / Supporting Documentation” boxes in the Workbook. Required Standards and implementation specifications must be implemented as stated for compliance. 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, or otherwise indicate how the intent of the standard can still be met. If a Standard or Implementation Specification does not apply, indicate “N/A” along with an explanation in that item’s “Implementation for Compliance” box.

While each entity is ultimately responsible for their compliance with the HIPAA Security Rule, in situations where a service provider is responsible for services that fulfill one or more requirement(s) on behalf of a unit or department, the unit or department can request verification of implementation from the service provider where this documentation is not otherwise readily available. A sample form for this purpose is included in Appendix A of this Workbook. The HIPAA requirements for which a service provider is responsible must be clearly indicated in this Workbook and in any verification documentation.

Note: Page breaks in this Workbook can be modified to maintain document continuity.

Unit/Department Information

Unit/Department Name:	
Individual responsible for HIPAA Security Rule compliance:	Name & Title: Designee, if applicable:
Nature of electronic protected health information (ePHI) necessitating HIPAA Security Rule compliance:	
List of systems, portable devices and electronic media that contain, access or transmit ePHI: <i>Note: For services maintained or supported by a service provider, including ITS, consult with the service provider to develop this list.</i>	
Last update:	Date:

¹ http://its.ucsc.edu/security/policies/hipaa_practices.php - See *UCSC HIPAA Security Rule Compliance Policy* for additional information:
<http://www.ucsc.edu/ppmanual/pdf/it0001.pdf>

² An “implementation specification” is an additional detailed instruction for implementing a particular Standard.



Table of Contents

This document is arranged by HIPAA Security Rule requirement. Each implementation specification (or Standard in the absence of specific implementation specifications) is followed by practices for compliance, along with space to document implementation of the practices and list other supporting documentation.

Introduction	1
Instructions for Completing this Workbook	1
HIPAA Security Rule: ADMINISTRATIVE STANDARDS	3
§164.308(a)(1)(i) - Security Management Process	3
§164.308(a)(2) - Assigned security responsibility	5
§164.308(a)(3)(i) - Workforce security	5
§164.308(a)(4)(i) - Information access management	7
§164.308(a)(5)(i) - Security awareness and training	8
§164.308(a)(6)(i) - Security incident procedures	10
§164.308(a)(7)(i) - Contingency plan	11
§164.308(a)(8) - Evaluation	13
§164.308(b)(1) - Business associate contracts and other arrangements	13
HIPAA Security Rule: PHYSICAL STANDARDS	15
§164.310(a)(1) - Facility access controls	15
§164.310(b) - Workstation use	17
§164.310(c) - Workstation security	17
§164.310(d)(1) - Device and media controls	18
HIPAA Security Rule: TECHNICAL STANDARDS	21
§164.312(a)(1) - Access Control	21
§164.312(b) - Audit controls	23
§164.312(c)(1) - Integrity	23
§164.312(d) - Person or entity authentication	24
§164.312(e)(1) - Transmission security	25
APPENDIX A	26



HIPAA Security Rule: ADMINISTRATIVE STANDARDS

STANDARD

§164.308(a)(1)(i) - Security Management Process

Implement policies and procedures to prevent, detect, contain, and correct security violations.

§164.308(a)(1)(ii)(A) - Risk Analysis (Required)

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Practices for Compliance

- Identify relevant information systems and electronic information resources that require protection.
- Conduct risk assessments to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. Risk assessments should take into account the potential adverse impact on the University's reputation, operations, and assets.
 - Evaluate backups and non-original sources of ePHI to determine whether additional protections are required.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(1)(ii)(B) - Risk Management (Required)

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.308(a).

Practices for Compliance

- Select appropriate mechanisms to safeguard data relative to the sensitivity or criticality determined by the risk assessment, and document the party(ies) responsible for implementation of each recommended practice.
- Where possible, incorporate these Standards and practices when evaluating and selecting new hardware and software.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

§164.308(a)(1)(ii)(C) - Sanction Policy

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

Practices for Compliance

- Take disciplinary or other action in accordance with University personnel policies, bargaining agreements, and guidelines on workforce members who, in the course of their employment, fail to comply with University policy and procedures, including information security policy and procedures. (See Personnel Policies for UC Staff Members (PPSM 62, 65, 67), UC BFB IS-3, applicable bargaining agreements, UC Academic Personnel Manual (APM 015, 016 & 150), and UCSC Campus Academic Personnel/Procedures Manual (CAPM 002.015 & 003.150).)
- Ensure that documentation of violations and application of sanctions is maintained appropriately.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(1)(ii)(D) - Information system activity review (Required)

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Practices for Compliance

- Develop a procedure for the review of information system activity, including the report of discrepancies. The procedure must:
 - Document steps for reviewing logs
 - Identify logs for review, including logs of activities performed by system administrator and third-party/vendor accounts
 - Unexpected access by system administrator and third-party/vendor logins should be confirmed
 - Identify criteria for review
 - Define “regular review” for each category of logs
- Maintain documentation of periodic log reviews.
- Logs relevant to security incidents should be retained for six years and the remainder of the data should only be retained for up to 90 days in accordance with usual and customary practice.
- Potential findings will trigger incident response procedures, as appropriate.
- Define responsibility for information system activity review in relevant job descriptions and in role-based matrix, as applicable.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

STANDARD

§164.308(a)(2) - Assigned security responsibility

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

Practices for Compliance

UC Guidelines for HIPAA Security Rule Compliance, Sec 3. HIPAA Security Rule. “HIPAA requires that a security official be assigned responsibility for HIPAA security implementation. ... Sr. Vice President Mullinix requested that campuses, laboratories, and hospitals appoint a HIPAA Security Officer. This individual should work closely with the systemwide taskforce under the direction of the designated University's HIPAA Privacy and Security Officer to ensure consistent compliance for the University.”

Implemented Policy and Procedures for Compliance

Campus-Level Implementation

The campus Vice Chancellor of Information Technology has been designated the campus HIPAA Security Official for UCSC. Each UCSC HIPAA entity must designate a position with responsibility for HIPAA Security Rule compliance.

STANDARD

§164.308(a)(3)(i) - Workforce security

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.

§164.308(a)(3)(ii)(A) - Authorization and/or supervision (Addressable)

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Practices for Compliance

Determine which individuals are authorized to work with ePHI in accordance with a role-based access approach.

Implementation for Compliance

Supporting Documentation (list by title and include as attachments)



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

§164.308(a)(3)(ii)(B) - Workforce clearance procedure (Addressable)

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Practices for Compliance

- Implement procedures to review role definitions and assignments for appropriateness at least annually.
- Implement procedures to review access management procedures for appropriateness at least annually.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(3)(ii)(C) - Termination procedures (Addressable)

Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section.

Practices for Compliance

Establish account maintenance procedures that ensure termination of accounts or change in access privileges for individuals or entities who have terminated or no longer are authorized to access ePHI.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

STANDARD

§164.308(a)(4)(i) - Information access management

Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

§164.308(a)(4)(ii)(A) - Isolating health care clearinghouse functions (Required)

If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

N/A for UCSC

§164.308(a)(4)(ii)(B) - Access authorization (Addressable)

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

Practices for Compliance

- There must be a formal system for authorizing user access to ePHI. This may take the form of an account request form requiring management approval.
- Maintain documentation of all authorized users of ePHI and their access levels.
- Employees must receive HIPAA and security awareness training prior to obtaining access to ePHI.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(4)(ii)(C) - Access establishment and modification (Addressable)

Implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.

Practices for Compliance

Develop and implement procedures to establish, document, review and modify a user’s access to ePHI.

- Procedures must ensure regular review of those with access to ePHI, including the appropriateness of access levels.
- Procedures must require prompt initiation of account modifications or changes.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

STANDARD

§164.308(a)(5)(i) - Security awareness and training

Implement a security awareness and training program for all members of its workforce (including management).

§164.308(a)(5)(ii)(A) - Security reminders (Addressable)

Periodic security updates.

Practices for Compliance

- Establish security awareness and HIPAA training for all members of the UC workforce who are involved in the creation, transmission, and storage of ePHI, including management. Training activities include:
 - Initial security awareness and HIPAA training for individuals with ePHI-related job duties
 - Review of changes to internal policies and procedures
 - Periodic reminders about HIPAA and security awareness
 - Security notices or updates regarding current threats
- Document training activities.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(5)(ii)(B) - Protection from malicious software (Addressable)

Procedures for guarding against, detecting, and reporting malicious software.

Practices for Compliance

To protect all devices against malicious software, such as computer viruses, Trojan horses, spyware, etc., implement the following. Also ensure the safeguards and configurations below are included in the standard set-up procedures for new systems and workstations that contain or access ePHI.

- Run versions of operating system and application software for which security patches are made available and installed in a timely manner.
- Harden systems. “Hardening” includes:
 - Install OS and third party application updates (patches) and keep them current
 - Change or remove default logins/passwords
 - Disable unnecessary services
 - Install Virus and Spyware Protection Software and update them at least weekly
 - Set proper file/directory ownership/permissions; NTFS should be used on Windows servers and shared workstations
- Periodically, and at least annually, review e-mail client settings for compliance with the technical specifications in this document.
- Periodically, and at least annually, review browser settings to ensure that they are set to prompt the user before running unsigned applets or code (such as ActiveX and Java).
- Implement centralized system(s) to scan network workstations and servers.
- Implement e-mail malicious code filtering.
- Install firewalls (hardware and/or software) to reduce threat of unauthorized remote access.



**UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook**

- Intrusion detection software may also be installed to detect threat of unauthorized remote access.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(5)(ii)(C) - Log-in monitoring (Addressable)

Procedures for monitoring log-in attempts and reporting discrepancies.

Practices for Compliance

- Implement procedures to ensure regular review of log-in attempts, including the report of discrepancies. The procedures must:
 - Document steps for reviewing logs
 - Identify logs for review, including logs of activities performed by system administrator and third-party/vendor accounts
 - Unexpected access by system administrator and third-party/vendor logins should be confirmed
 - Identify criteria for review
 - Define “regular review” for log-in monitoring
- Maintain documentation of periodic log reviews.
- Only logs relevant to security incidents should be retained for six years and the remainder of the data should only be retained for up to 90 days in accordance with usual and customary practice.
- Potential findings will trigger incident response procedures, as appropriate.
- Define responsibility for log-in monitoring in relevant job descriptions and in role-based matrix, as applicable.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(5)(ii)(D) - Password management (Addressable)

Procedures for creating, changing, and safeguarding passwords.

Practices for Compliance

Passwords for systems containing or accessing ePHI will comply with the *UCSC Password Strength and Security Guidelines*: <http://its.ucsc.edu/security/policies/password.php>.

- Enforce UCSC password complexity requirements for third-party access as possible.

Implementation for Compliance



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

Supporting Documentation (list by title and include as attachments)

STANDARD

§164.308(a)(6)(i) - Security incident procedures

Implement policies and procedures to address security incidents.

§164.308(a)(6)(ii) - Response and Reporting (Required)

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Practices for Compliance

- Develop and implement written procedures to address suspected or known security incidents involving ePHI.
 - Security incident procedures should include notification, triage, investigation, evidence collection and preservation, containment, eradication, recovery, and reporting steps.
 - Security incident procedures must describe how workforce members are to report and respond to an incident or suspected incident.
- Security incidents determined to involve ePHI must be documented, tracked and reported as defined in written procedures.
 - Note: The *UCSC Implementation Plan for Protection of Electronic Personal Identity Information*, http://its.ucsc.edu/security/policies/ucsc_breach_guideline.php, applies to security incidents involving ePHI, though notification requirements may differ.
- Unit, IT and Campus incident response must coordinate as defined in written procedures.
- Notification procedures and requirements must comply with UC BFB IS-3: <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

STANDARD

§164.308(a)(7)(i) - Contingency plan

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

§164.308(a)(7)(ii)(A) - Data backup plan (Required)

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Practices for Compliance

- Conduct back up of original sources of essential ePHI on an established schedule.
- Back up copies must be securely stored in a physically separate location from the data source.
- Backups containing ePHI will be transported via secure methods.
- Documentation must exist to verify the creation of backups and their secure storage.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(7)(ii)(B) - Disaster recovery plan (Required)

Establish (and implement as needed) procedures to restore any loss of data.

Practices for Compliance

- Develop data restoration procedures to be implemented in order to resume access to original sources of essential ePHI following a disaster or during an emergency.
- Copies of the data restoration procedures must be readily accessible at more than one location and should not rely on the availability of power or network.
- Backup procedures must include steps to ensure that all protections (patches, configurations, permissions, firewalls, etc.) are re-applied and restored before ePHI is restored to the system.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(7)(ii)(C) - Emergency mode operation plan (Required)

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

Practices for Compliance

Ensure that unit emergency operations procedures maintain security protections for ePHI.

- Evaluate operations in emergency mode, e.g. a technical failure or power outage, to determine whether security processes to protect ePHI are maintained.
- Document assessment and conclusions.
- Document and implement additional authorities and procedures necessary to ensure the continuation of security protections for ePHI during emergency operations mode.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(7)(ii)(D) - Testing and revision procedures (Addressable)

Implement procedures for periodic testing and revision of contingency plans.

Practices for Compliance

- Document the contingency plan procedures.
- Ensure that those responsible for executing contingency plan procedures understand their responsibilities.
- Periodically, and at least annually, perform a test of the contingency plan procedures.
- Document test results, review and correct any problems with the test, and update procedures accordingly.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.308(a)(7)(ii)(E) - Applications and data criticality analysis (Addressable)

Assess the relative criticality of specific applications and data in support of other contingency plan components.

Practices for Compliance

Prioritize criticality of applications and data sets for data back-up, restoration, and application of emergency mode operation plan.

- Priorities can be included in data restoration procedures (*§164.308(a)(7)(ii)(B) - Disaster recovery plan (Required)*)

Implementation for Compliance



**UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook**

Supporting Documentation (list by title and include as attachments)

STANDARD

§164.308(a)(8) - Evaluation

Perform a periodic technical and non-technical evaluation, based initially upon the standards and implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.

Practices for Compliance

- Review and update HIPAA Security policies and procedures annually, or more frequently in response to environmental or operational changes that affect the security of ePHI.
 - Identify the individual(s) responsible for determining when evaluation is necessary due to environmental or operational changes.
- Document periodic reviews and updates.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

STANDARD

§164.308(b)(1) - Business associate contracts and other arrangements

A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

§164.308(b)(4) - Written contract or other arrangement (Required)

Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

Practices for Compliance

Ensure that agreements with business associates³ contain language stating that University ePHI receives appropriate safeguards in accordance with Federal HIPAA Security Standards.

³ A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or as a service to, a covered entity. This includes services where disclosure of ePHI



UNIVERSITY OF CALIFORNIA, SANTA CRUZ HIPAA Security Rule Compliance Workbook

- Ensure that BAAs are in place at either a Systemwide or local level for vendors and third-party service providers with access to UCSC ePHI or to systems that contain or access ePHI.
 - If a Systemwide BAA does not exist, one must be executed locally.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

is not limited in nature, such as destruction services or a software vendor that needs access to ePHI in order to provide its service. Common exclusions include health care providers that must comply with HIPAA requirements, conduits (physical or electronic) that transport but do not access protected health information, custodial services, destruction services when the work is performed under the direct control of the covered entity (in which case the service may be treated as part of the workforce). For additional clarification, inclusions and exclusions, see <http://www.hhs.gov/ocr/hipaa/guidelines/businessassociates.pdf> and http://www.hipaadvisory.com/regs/Regs_in_PDF/finalsecurity.pdf, page 8378, column 1, (b)(1).



HIPAA Security Rule: PHYSICAL STANDARDS

STANDARD

§164.310(a)(1) - Facility access controls

Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

§164.310(a)(1)(i) - Contingency Operations (Addressable)

Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

Practices for Compliance

Ensure that Contingency Plan procedures and authorization (See Administrative Standards) include facility access.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.310(a)(1)(ii) - Facility security plan (Addressable)

Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Practices for Compliance

- Systems and electronic media containing ePHI are to be located in physically secure locations. A secure location would minimally be defined as one that is not routinely accessible to the public, particularly if authorized personnel are not always available to monitor security.
- Secure locations must have physical access controls (Card Key, door locks, etc.) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security.
- Access control systems must be maintained in good working order.
- Facility security plans must document use of physical access controls.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



**UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook**

§164.310(a)(1)(iii) - Access control and validation procedures (Addressable)

Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Practices for Compliance

- The access plan for facilities containing ePHI utilizes role- or function-based access control, including for visitors and service providers.
- The functional or role-based access control and validation procedures are closely aligned with the facility security plan.
- The security plan for facilities containing ePHI includes key systems or Omnilocks.
 - Security plans utilizing key systems must adhere to the UCSC Key Control and Access policy: <http://www.ucsc.edu/ppmanual/abstract/sps0001.htm>
- Periodic (at least annual) review and implementation of termination procedures, which may include a review of key inventory or Omnilock access, to ensure currency of access authorization.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.310(a)(1)(iv) - Maintenance records (Addressable)

Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Practices for Compliance

- Develop policy and procedure for maintaining a record of any maintenance repairs and modifications to physical components of a facility containing ePHI related to security, such as hardware, walls, doors, and locks.
 - Documentation should contain appropriate detail for review, including date, repair and/or modification(s) made, and who the work was contracted through.
- Identify party(ies) responsible for recording and maintaining these records.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

STANDARD

§164.310(b) - Workstation use

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI

Practices for Compliance

- Functions to be performed on workstations containing or accessing ePHI are aligned with roles, such as through the use of a role-based matrix.
- Policies and procedures specify where to place and position workstations to only allow viewing by authorized individuals, as well as additional privacy measures, commensurate with the risk of exposure.
- Unencrypted ePHI will not be stored on portable electronic devices.
- Storage of ePHI on non-university equipment is forbidden, except in the case of storage by a third party with a HIPAA BAA.
- Remote access of ePHI will utilize secure channels.
- Additional UCSC practices for the protection of electronic restricted data are available online at <http://its.ucsc.edu/security/policies/rd.php>.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

STANDARD

§164.310(c) - Workstation security

Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Practices for Compliance

- All workstations, including laptops, containing ePHI are to be physically secured (locked down).
- All workstations and electronic devices that contain or access ePHI will be identified, such as laptops, desktop computers, personal digital assistants (PDAs).
- Unencrypted ePHI will not be stored on portable electronic devices.
- If ePHI is stored on removable media, additional physical controls must be implemented, such as ensuring that the device is physically secured or in the physical possession of the responsible party. Encryption is a compensating control for these additional measures.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



STANDARD

§164.310(d)(1) - Device and media controls

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

§164.310(d)(2)(i) - Disposal (Required)

Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

Practices for Compliance

Ensure that ePHI on hardware and electronic media is unusable and/or inaccessible prior to disposal, including disposal by a Business Associate⁴.

- When portable media is discarded, it should either be overwritten multiple times, in accordance with National Institute of Standards and Technology (NIST) guidelines (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf), or physically destroyed, eliminating all possibility that any ePHI contents could be read.
- When a System is recycled, transferred to another user not authorized for the data, or discarded, all storage devices or all ePHI records must be overwritten multiple times, in accordance with NIST standards (link above), or physically destroyed, rendering all ePHI records unreadable.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.310(d)(2)(ii) - Media re-use (Required)

Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

Practices for Compliance

Ensure that ePHI on hardware and electronic media is unusable and/or inaccessible prior to re-use.

- When a System is recycled or transferred to another user not authorized for the data, or otherwise re-used outside of a HIPAA-compliant environment, all storage devices or all ePHI records must be overwritten multiple times, in accordance with National Institute of Standards and Technology (NIST) guidelines (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf), rendering all ePHI records unreadable.

Implementation for Compliance

⁴ Also see §164.308(b)(1), Business associate contracts and other arrangements



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

Supporting Documentation (list by title and include as attachments)

§164.310(d)(2)(iii) - Accountability (Addressable)

Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Practices for Compliance

- The responsible unit must maintain a record of the movements of, and person(s) responsible for, hardware and electronic media containing ePHI.
 - Identify all types of hardware and electronic media that must be tracked.
 - Special attention must be paid to portable devices and removable media. These devices should not ordinarily contain ePHI and must be individually identified in the tracking system in order to contain ePHI. Their use must be consistent with the individual's identified role, such as according to a role-based matrix.
 - This inventory should be physically confirmed at least annually.
 - Tracking system must include a mechanism for documenting the initial assignment of responsibility for devices that contain ePHI, as well as the transfer of authority for these devices.
- Transport of archival media between the origination point and remote storage location must use a secure method to avoid unauthorized access to the archival media.
- Loss or theft of electronic equipment or media containing ePHI must immediately be reported according to campus incident response procedures: <http://its.ucsc.edu/security/report.php>

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.310(d)(2)(iv) - Data backup and storage (Addressable)

Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Practices for Compliance

Create a retrievable, exact copy of original sources of essential ePHI before moving equipment containing them.

- Establish a process for documenting or verifying its creation.
- Retrievable, exact copies of ePHI must be protected in accordance with these Standards.

Implementation for Compliance



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

Supporting Documentation (list by title and include as attachments)



HIPAA Security Rule: TECHNICAL STANDARDS

STANDARD

§164.312(a)(1) - Access Control

Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)

§164.312(a)(2)(i) - Unique user identification (Required)

Assign a unique name and/or number for identifying and tracking user identity.

Practices for Compliance

Ensure the verification of the individual or entity who is authorized to access ePHI and that the identity is correctly bound to a unique user identification (“sign-on”) for access to ePHI.

- Each User must be provided a unique account, with a unique User Name and Password.
- Generic or shared accounts are not permitted for access to ePHI.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.312(a)(2)(ii) - Emergency access procedure (Required)

Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Practices for Compliance

Establish procedures to ensure that necessary ePHI can be accessed during an emergency.

- Emergency access procedures may be included in Contingency Plan procedures (see §164.308(a)(7)(i) - *Contingency plan*).
- The emergency access protocol should be written and should be communicated in advance to multiple individuals within the organization.
- Emergency access procedure should not rely on the availability of a single individual. Access to emergency procedures should also not rely on the availability of power or network.
- Alternatively, if the data on the system is merely a copy of the data in the medical record and access to the system is not necessary for safe patient care, an acceptable protocol would be to access the medical record when the system is unavailable.
- Identify roles that may require special access during an emergency.
 - Individuals are to require proper ID or other official verification before granting access to unknown or not-normally-authorized individuals in emergency circumstances.

Implementation for Compliance



**UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook**

Supporting Documentation (list by title and include as attachments)
--

§164.312(a)(2)(iii) - Automatic logoff (Addressable)

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Practices for Compliance

Where possible, terminate electronic sessions after a period of inactivity.

- Where session termination is not possible, either technically or from a business process perspective, implement automatic workstation lockout as a compensating control.
- Maximum duration of inactivity prior to session termination or automatic workstation lockout is 10 minutes.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.312(a)(2)(iv) - Encryption and decryption (Addressable)

Implement a mechanism to encrypt and decrypt electronic protected health information.

Practices for Compliance

Note: The HIPAA Status Workgroup has determined the scope of this implementation specification to include stored ePHI. See §164.312(e)(2)(ii) – *Encryption (Addressable)*, below, for transmission of ePHI.

- Implement appropriate logical security measures, such as encryption, to protect ePHI from unauthorized access.
 - Unencrypted ePHI will not be stored on portable electronic devices (see §164.310(b) - *Workstation use* and §164.310(c) - *Workstation security*).
- In situations where encryption is problematic, the alternative compensating controls below must be implemented as appropriate, in consultation with UCSC ITS Security.
 - An explanation must be provided for why encryption is not being implemented.

Alternative, reasonable and appropriate compensating controls if encryption is not in place on servers and workstations (including laptops) for stored ePHI:

- Access controls, including unique user ID & password authentication, and user profiles (SHS only)
- Hardening of systems (see §164.308(a)(5)(ii)(B) - *Protection from malicious software (Addressable)* for details)
- Physical security for access to facilities and workstations that contain or access ePHI, including appropriate device and media controls
- Technically enforce complex passwords where possible
- Enable system security auditing/logging, including monitoring of audit reports/logs
- Correct configuration of applications to use secure protocols
- Implement automatic logoff (see §164.312(a)(2)(iii) - *Automatic logoff (Addressable)* for details)
- Ensure secure remote access



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

- Implement correctly configured firewalls (hardware and/or software)

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

STANDARD

§164.312(b) - Audit controls

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Practices for Compliance

- Establish criteria for system log creation, retention, and examination of activity. Audit logs should include sufficient detail to ensure that suspicious patterns of activity can be identified. At a minimum, record data that a) assists in investigations of unauthorized uses or disclosures, b) may detect unauthorized activity, c) indicates security design issues.
- Log security-related events and audit according to the established criteria.
- New systems should be selected with the ability to support audit requirements.
- See §164.308(a)(1)(ii)(D) - *Information system activity review (Required)* for additional administrative practices.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

STANDARD

§164.312(c)(1) – Integrity

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

§164.312(c)(2) - Mechanism to authenticate electronic protected health information (Addressable)

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Practices for Compliance

- Leverage application-specific mechanisms or functionality when available to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

- Regularly review access logs for unauthorized direct access or administrator/root access to table data containing ePHI.
- In addition, the following practices are in place as a means of protecting ePHI from being altered or destroyed in an unauthorized manner:
 - Ensure appropriate physical security is in place for devices that contain or access ePHI (see *Physical Security Standards*).
 - Protect all devices against malicious software (see §164.308(a)(5)(ii)(B) - *Protection from malicious software (Addressable)* for details).
 - Protect sensitive data with appropriate strategies, such as secure file transfer (§164.312(e)(1) - *Transmission security*) and use of web browser security standards (§164.308(a)(5)(ii)(B) - *Protection from malicious software*).
 - Implement processes to notify users and take other appropriate remedial action in the event of propagation of Intrusive Computer Software (see §164.308(a)(5)(ii)(A) - *Security reminders (Addressable)*).

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

STANDARD

§164.312(d) - Person or entity authentication

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Practices for Compliance

- Each User must be provided a unique account, with a unique User Name and Password, for access to ePHI.
 - Generic or shared accounts are not permitted.
 - Passwords will not be shared by UCSC Employees.
 - All passwords providing access to ePHI, including local administrator/root passwords, must comply with the password strength requirements in the *UCSC Password Strength and Security Guidelines*:
<http://its.ucsc.edu/security/policies/password.php>
 - Physically protect passwords (see *UCSC Password Strength and Security Guidelines*, link above)
- Log and review, as appropriate, workstation, OS and application access logs, as well as failed or successful changes to account permissions (also see §164.308(a)(1)(ii)(D) - *Information system activity review (Required)* and §164.308(a)(5)(ii)(C) - *Log-in monitoring (Addressable)*).
- Systems and applications will not be configured to save passwords.
- All of the above practices apply to vendors and third parties.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

STANDARD

§164.312(e)(1) - Transmission security

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

§164.312(e)(2)(i) - Integrity controls (Addressable)

Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Practices for Compliance

- Wired and wireless transmission of ePHI will utilize secure protocols (encryption), whenever possible.
 - All remote access into UC networks must be by secure methods only.
 - E-mail clients will be set to use secure protocols for both sending and receiving as well as for authentication.
 - Where secure protocols are not feasible for e-mail, compensating controls include utilizing password protected files and individual authorizations/waivers, security awareness education, and minimum use.
 - For SHS, email containing ePHI is only sent to @ucsc email addresses, and only with a waiver on file.
 - The Benefits Office will only send ePHI via email in password-protected attachments and only to known business partners, UCOP, and in response to legitimate email requests. Benefits staff will delete or redact ePHI from the body of email before replying to it.

Implementation for Compliance
Supporting Documentation (list by title and include as attachments)

§164.312(e)(2)(ii) – Encryption (Addressable)

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

See §164.312(e)(2)(i) - Integrity controls (Addressable), above, for recommended practices.

Note: Also see §164.312(a)(2)(iv) – Encryption and decryption (Addressable), above, for storage of ePHI.



UNIVERSITY OF CALIFORNIA, SANTA CRUZ
HIPAA Security Rule Compliance Workbook

APPENDIX A

Sample form for documenting service provider implementation of specified HIPAA Security Rule requirements

Date: _____

Contracting Unit/Department: _____

Responsible Individual: _____

Service Provider: _____

Responsible Individual: _____

HIPAA Security Rule Requirement (Standard or implementation specification) <i>To be completed by contracting Unit/Dept</i>	Practice(s) for Compliance Fulfilled by Service Provider (from this Workbook) <i>To be completed by contracting Unit/Dept</i>	Certification of Implementation (Service provider must provide implementation information here or must sign below and maintain implementation documentation sufficient to demonstrate compliance upon request.)