

1.0 Purpose

The purpose of these procedures is to establish hardware, software, and/or procedural mechanisms that record and examine activity in electronic information systems. System audit controls should utilize appropriate audit technologies and include practices to help identify and report actual or potential breaches in security.

These procedures are governed by HIPAA Security 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.

2.0 Definitions

2.1 Workforce: All faculty, staff, students, trainees, volunteers, and business associates who access restricted or confidential information during the course of their duties.

3.0 Procedures

3.1 System Audit Controls: Implement the following procedures when developing system audit controls:

3.1.1 Define Audit Control Requirements: List the audit controls required to ensure the security, reliability, and integrity of restricted or confidential information identified from the risk analysis process. Refer to the System Management Procedures 60.001 for instructions on completing the risk analysis.

- All access to ePHI should be logged including the ID of the person accessing ePHI, patient and any changes to the data.

3.1.2 Perform Audit Control Inventory: List the existing audit controls that are in place to determine if those audit control requirements are satisfactory.

- Information systems written by UCSF permit user access to ePHI only through application software that records the identity of the user and patient as well as the date and time of the access, and includes tools to search and review these audit records.
- All software purchased from and/or installed by external vendors is expected to provide appropriate audit controls.

3.2 System Audit Trails: Implement the following guidelines when establishing system audit trails:

3.2.1 Define Audit Trail Content: Define the content of the audit trail. At a minimum, the audit trails should contain the following information:

- Type of event
- Date and time of occurrence
- User ID associated with event
- Program, command, or method used to initiate event
- Patient and data elements whose information was changed

3.2.2 Define Audit Trail Security: Design and implement sufficient security controls to protect audit trails from unauthorized access. Separate the duties of those who administer the access control functions from those who administer the audit trails, if possible.

3.2.3 Define Audit Trails Review Guidelines: Determine review methods and the frequency of audit trails, based upon the identified risks level.

3.2.4 Define Appropriate Versus Inappropriate Activity: Identify what is considered to be appropriate activity and inform the individuals responsible for reviewing audit trails to ensure that they can distinguish between appropriate and inappropriate activity.

4.0 Initiation and Control Reporting

4.0 Records & Documentation Control

6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rules: Audit Controls	164.312(b) http://www.ucsf.edu/hipaa/dept_compliance/
Special Publication: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule – National Institute of Standards and Technology (NIST)	SP 800-66 http://www.ucsf.edu/hipaa/dept_compliance/
University of California Business and Finance Bulletin IS-3 Electronic Information Security	IS-3 http://www.ucsf.edu/hipaa/dept_compliance/ or http://www.ucop.edu/ucophone/policies/bfb/is3.pdf
Information Security and Confidentiality Policy (UCSF)	650-16 http://www.ucsf.edu/hipaa/dept_compliance/
Information Security and Confidentiality Policy (UCSF Medical Center)	5.01.04 http://www.ucsf.edu/hipaa/dept_compliance/
Security Management Procedures	60.001 http://www.ucsf.edu/hipaa/dept_compliance/

REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	03/04/05	Ken Jakobs	Initial Release
B	03/18/05	Ken Jakobs, Dan Yee and Barbara Heredia	Version 1.5 section 3.0 Procedures
C	01/02/2007	Rob Slaughter	Adapted for School of Nursing

If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.
 Contains Proprietary Information and is for the use of UCSF only.

Does not include changes after 01/02/2007