

## 1.0 Purpose

The purpose of these procedures is to implement electronic mechanisms or other procedures, as needed to establish controls and corroborate that restricted or confidential information has not been altered or destroyed in an unauthorized manner.

The HIPAA Security Rule that governs these procedures is *164.312(c)(1) Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

## 2.0 Definitions

**2.1 Source:** In the context of this document, the term “source” refers to unprocessed data or information that is utilized for input to a computer system.

**2.2 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 Establish Data Integrity and Validation Controls:** Systems owners and managers are responsible for establishing controls that support the integrity, timeliness, availability, and confidentiality of data.

- Data backups should be created and archived.

**3.2 Maintain Integrity of Collected Data and Secure Storage:** Systems and business owners, managers and administrators are responsible for ensuring that the integrity and accuracy of electronic data that is collected is consistent with the original source, and each process (manual or computer process) through which data passes preserves its integrity. Implement controls for securing the storage of electronic data.

**3.3 Inform Data Users of Their Responsibilities:** Business owners and managers are responsible for informing all data users of their responsibility to maintain the confidentiality and integrity of the data. Refer to the UCSF HIPAA Handbook, Appendix 1 which is posted on the UCSF Medical Center Administrative Policies Manual <http://manuals.ucsfmedicalcenter.org/AdminManual/AdminManualHome.htm>

**3.4 Link Production Input to Source:** A unique sequence number or identifier assigned to each transaction will link it back to the source facilitating tracking and problem resolution. If not technically possible, application managers and developers may utilize other methods such as a transaction log file.

**3.5 Validate Input Data:** Application managers and developers are responsible for implementing validation checks and/or edit checks. Transactions that fail such checks, must either be (a) rejected with a notification of the rejection sent to the submitter (b) corrected and resubmitted or (c) suspended pending further investigation.

**3.6 Establish Data Modification Controls:** Application managers and developers must establish and maintain sufficient controls to mitigate the risk of undetected production data alterations.

**3.7 Establish Data Transmission Security Controls:** System owners and managers must implement appropriate measures to ensure that information (restricted and confidential) has not been altered in an unauthorized manner during transmission. Refer to the Transmission Security Controls Procedures 60.014 for further details.

**3.8 Define Audit Controls:** System owners and managers must establish appropriate system audit controls to validate that restricted or confidential information has not been altered in an unauthorized manner. Refer to System Audit Controls Procedures 60.012 for further details.

**4.0 Initiation and  
Control Reporting**

**5.0 Records &  
Documentation  
Control**

**6.0 Related  
Documents**

Document Name	Procedure No.
---------------	---------------

HIPAA Security Rules: Integrity	<b>164.312(c)(1)</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
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)	<b>SP 800-66</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
University of California Business and Finance Bulletin IS-3 Electronic Information Security	<b>BFB IS-3</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a> or <a href="http://www.ucop.edu/ucophome/policies/bfb/is3.pdf">http://www.ucop.edu/ucophome/policies/bfb/is3.pdf</a>
Information Security and Confidentiality Policy (UCSF Campus)	<b>650-16</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
Information Security and Confidentiality Policy (UCSF Medical Center)	<b>5.01.04</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
System Access Control Procedures System Audit Controls Procedures Information Access Management Procedures Transmission Security Controls Procedures	<b>60.011</b> <b>60.012</b> <b>60.003</b> <b>60.014</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>

**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 1.3 section 3.0 Procedures
C	11/8/2006	Rob Slaughter	Revised for School of Nursing