

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: Integrity and accuracy of electronic data backups is verified by the application used for backup. The backup application required verification of data integrity. Backup failures are emailed to systems administrators for review.

3.3 Inform Data Users of Their Responsibilities: Department and Unit 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.

3.4 As of 5/16/05, ISU is not responsible for any software or database applications that allow for field or record level updates, adds, or deletes for ePHI. Therefore, the following procedures do not apply at this time and will not be implemented:

3.4.1 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.

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.

3.4.2 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.

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

**4.0 Initiation and
Control Reporting**

**5.0 Records &
Documentation
Control**

**6.0 Related
Documents**

Comment [UU1]: Page: 3
Insert names and locations of forms and documents used to implement this procedure.

Comment [UU2]: Page: 3
Insert names and locations of forms and documents used to record the activities associated with this procedure (as it is invoked).

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

Data Integrity and Validation Procedures

HIPAA Security Rules: Integrity	164.312(c)(1) http://www.ucsf.edu/hipaa/dpt_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/dpt_compliance/
University of California Business and Finance Bulletin IS-3 Electronic Information Security	BFB IS-3 http://www.ucsf.edu/hipaa/dpt_compliance/ or http://www.ucop.edu/ucophone/policies/bfb/is3.pdf
Information Security and Confidentiality Policy (UCSF Campus)	650-16 http://www.ucsf.edu/hipaa/dpt_compliance/
Information Security and Confidentiality Policy (UCSF Medical Center)	5.01.04 http://www.ucsf.edu/hipaa/dpt_compliance/
System Access Control Procedures System Audit Controls Procedures Information Access Management Procedures Transmission Security Controls Procedures	60.011 60.012 60.003 60.014 http://www.ucsf.edu/hipaa/dpt_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 1.3 section 3.0 Procedures; modified to match SOM template
C	10/15/05	Judi Mozesson	Modified to match SOM template which was converted 5/16/05.

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.