University of Colorado
Denver | Anschutz Medical Campus

Office of Regulatory Compliance

13001 E. 17th Place, Suite W1124
Mail Stop F497
Aurora, CO 80045
Main Office: 303-724-1010
Main Fax: 303-724-1019

HIPAA Policy 9.8

Title:	**Data Integrity**
Source:	**Office of Regulatory Compliance**
Prepared by:	**Assistant Vice Chancellor for Regulatory Affairs**
Approved by:	**Vice Chancellor for Research**
Effective Date:	**July 1, 2013**
Replaces:	**04/11/2005**
Applies:	**All UCD campuses**

Introduction

Purpose

Data integrity is the ability to confirm that data has not been altered or destroyed in an unauthorized manner. The purpose of this policy is to outline policies and procedures for protecting electronic Protected Health Information (ePHI) from improper alteration or destruction relative to the HIPAA Security Regulations.

Reference

45 CFR § 164.312(c)(1) and (2).

Applicability

This policy applies to every member of the UCD workforce who has access to or who uses ePHI and every unit administering computer systems containing ePHI. This includes ePHI used in research and ePHI housed in databases physically located at UCD but owned by research sponsors.

Policy

UCD shall protect ePHI from improper alteration or destruction. This responsibility resides both with the administration of the University as well as the units directly handling or storing the data.

Procedures

A. Protecting Data Integrity

UCD must protect ePHI in its possession from improper alteration or destruction. In order to preserve the integrity of ePHI in its possession, UCD must implement a combination of policy and technical solutions. The combination includes:

1. Policies and procedures to protect ePHI from improper alteration or destruction and to keep ePHI consistent with its source.

2. Electronic mechanisms to confirm that ePHI has not been altered or destroyed in an unauthorized manner.

B. Integrity Controls

Integrity controls are technical safeguards to prevent or detect unauthorized alteration or deletion of ePHI and critical system and network files. Technical safeguards may include:

1. Firewalls;

2. Encryption;

3. Password protection and other authentication devices;

4. Anti-virus software; and

5. Standards for change control, testing, documentation, approval, and rollback.

C. Unit Responsibilities

1. Each unit directly handling or storing ePHI is responsible for maintaining internal controls to protect ePHI from improper alteration or destruction and to keep it consistent with its source.

2. Decisions regarding the preferred combination of technical solutions, processes, and procedures may be made at the unit level. However, UCD requires that collectively, the combination of solutions used by the unit suffice to reasonably safeguard ePHI and to protect it from improper alteration or destruction.

3. Units must document their decision-making processes on which solutions they use and all technical and administrative solutions put in place. This information must be submitted to the HIPAA Security Officer for approval. Documentation must be retained by the unit for a period of at least six (6) years from the date the decision was made or the solution was last used.

4. Units are responsible for educating all unit members with access to ePHI on their unit level policies, procedures, and technical solutions.

5. Units must perform routine monitoring of the solutions chosen and policies and procedures implemented to assess the unit's effectiveness of proving data integrity. Units must weigh the confidentiality of ePHI against its availability and integrity. Units must perform this review as needed, no less than every two (2) years.

D. Data Authentication Controls

Data authentication is the electronic process in which holders of ePHI validate data integrity, verify that the data sent is the same data that is received, and ensure the integrity of data stored and retrieved. Data authentication controls consist of the following:

1. Database integrity – integrity checking and data recovery features which must be built into the database application;

2. Message integrity – transmitting ePHI from one place to another uses data integrity features. To ensure the protection of data transmitted over the Internet, ePHI in e-mail must be sent via the UCD secure mail. Web applications used for transmitting ePHI must incorporate secure transmission methods; and,

3. Procedure integrity – based on the level of risk it may be necessary to provide additional reliability in the form of redundant systems, duplicate power supplies, appropriate power conditioning and cooling systems. Regular preventive maintenance must be performed.

E. Software Controls

Systems without adequate authorization mechanisms built into the software should never be used to store or transmit ePHI. The design of UCD database systems and software used for handling ePHI should be evaluated for its ability to:

1. Protect against alteration or modification;
2. Record missing or critical information; and
3. Control simultaneous updates.

After database systems and software have been evaluated, if it is determined that they cannot provide the above, they should not be used to store or transmit ePHI. These systems must be upgraded or replaced.