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 9.9

Title:	**Person or Entity Authentication**
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:	**04/08/2005**
Applies:	**All UCD campuses**

Introduction

Purpose

Identification and authentication procedures provide the foundation for safeguarding systems. Authentication, or the ability to confirm that a person or entity is the one claimed, is the primary access control for validating the identity of users and monitoring their access to electronic Protected Health Information (ePHI).

Reference

45 C.F.R. § 164.312(a)(2)(i)

45 C.F.R. § 164.312(d)

Applicability

This policy applies to all members of the UCD workforce who have access to ePHI or provide access to ePHI.

Policy

All UCD workforce personnel shall authenticate the entity or person receiving PHI.

Procedures

A. Unique User Identification (Login)

1. Each person who accesses ePHI held by UCD must perform that access using unique user identification (login). The login may be a unique name and/or number used to identify and track user identity.

2. No member of the UCD workforce may use another member's login. Workforce members may not allow others to use their login and/or password.

3. The use of shared logins is prohibited when accessing ePHI.

4. Administrators of systems housing ePHI (or that may be used to access ePHI) are required to cancel or disable a user's account upon termination of the user's relationship with UCD or when the user no longer needs access to ePHI.

5. Any violations of this policy must be reported to the HIPAA Security Officer immediately.

B. Person or Entity Authentication

1. Each unit that houses ePHI must implement procedures to verify that a person seeking access to ePHI is the one claimed.

2. ePHI housed by UCD must be protected by authentication controls on all IT resources.

3. Valid authentication shall consist of at least a unique user login and password combination to verify user authenticity. Other authentication measures, such as cryptographic keys, tokens, smart cards, etc, may be implemented if feasible.

4. Entity authentication may be a shared password or public key, requiring a second form of authentication. It may also be a technical mechanism built into the software itself.