

University of Colorado at Denver and Health Sciences Center  
HIPAA Policy

---

Policy:	9.9	Latest Revision: 04/08/2005
	Person or Entity Authentication	Page: 1 of 2

---

I. Purpose, Reference, and Responsibility

A. 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).

B. Reference

45 C.F.R. § 164.312(a)(2)(i).  
45 C.F.R. § 164.312(d).

C. Responsibility

It is the responsibility of anyone who uses or provides access to ePHI to follow this policy.

II. Applicability and Definitions

A. Applicability

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

B. Definitions

Authentication  
Electronic Protected Health Information (ePHI)  
Login  
Security Officer  
Workforce

University of Colorado at Denver and Health Sciences Center  
HIPAA Policy

---

Policy:	9.9 Person or Entity Authentication	Latest Revision: 04/08/2005 Page: 2 of 2
---------	--	---

---

III. Policy

A. Unique User Identification (Login)

1. Each person who accesses ePHI held by UCDHSC 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 UCDHSC 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 UCDHSC 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 UCDHSC 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.

