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 9.4

Title:	**Workforce Security**
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:	**05/02/05**
Applies:	**All UCD campuses**

Introduction

Purpose

This policy outlines procedures to ensure that UCD workforce members have appropriate access to electronic Protected Health Information (ePHI) and to prevent those who should not have access from obtaining access. This policy includes information access management, workstation use and security, and access control mechanisms.

Reference

45 C.F.R. § 164.308(a)(3)(i) and (ii)

45 C.F.R. § 164.308(a)(4)(i) and (ii)(B) – (C)

45 C.F.R. § 164.308(a)(5)(ii)(B)

45 C.F.R. § 164.310(b) and (c)

45 C.F.R. § 164.312(a)(1)

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

Applicability

This policy applies to control access of ePHI at UCD by the UCD workforce. This includes access authorization, modification and termination procedures, use of and security of workstations containing ePHI, and access control mechanisms.

Policy

All members of the UCD workforce are responsible for managing and protecting the information technology resources under their jurisdiction. They are also responsible for creating and enforcing policies regarding the administration of information technology resources in their areas. The UCD Information Technology Services Department (ITS) offers central disk storage and backup services which many departments and units use for maintaining their data. While central ITS systems meet the HIPAA physical security and contingency planning requirements, departments and units must still take care to address controls for workstation security, account management, and controlling access to ePHI they create or house. It is the responsibility of all members of the UCD workforce who access ePHI from any device and in any capacity at UCD to follow this policy. This includes faculty, staff, students, interns, trainees, volunteers, contractors, vendors, business associates, etc.

Procedures

A. Access to Electronic Protected Health Information (ePHI)

1. The use and access of UCD's information systems is restricted to appropriately identified, validated and authorized individuals. Treatment, payment, and healthcare operations are the only approved reasons for accessing ePHI. All other access may only occur pursuant to a permission to access ePHI. Permission includes valid HIPAA authorization from a human subject, data use agreement, business associate agreement, or decedent research certification.

2. Each unit that maintains or provides access to ePHI is responsible for ensuring that any necessary workforce clearance procedures have been followed before authorizing access to ePHI. Members of the workforce shall only be granted access to the minimum necessary ePHI that they require to perform their duties.

3. To set up access to an ITS-managed resource, an account request form must be completed. This process provides the ability to document access granted, modified, or terminated. The completion of this access establishment, modification or termination will be communicated to the requestor via e-mail. The access authorization e-mail will include the initial password for the account; the password must be strong and must be changed at first login. Separate authorization requests are required for temporary employees, remote access, and any other special access of UCD systems.

4. Unit managers / supervisors must re-evaluate access rights when a workforce member's access requirements to ePHI change. Unit managers / supervisors or other approved individuals are responsible for submitting

the appropriate form to UCD ITS when a workforce member's access requirements have changed.

5. UCD ITS will maintain an audit trail of requests for creation, modification, or termination of access to ePHI.

6. Termination of Access

a. It is the responsibility of the unit manager or supervisor or his/her designee to submit the appropriate form to UCD ITS when a workforce member's employment or affiliation with UCD is terminated or the member's access needs have ended.

b. In coordination with UCD Human Resources and the Affiliates, UCD ITS will disable user accounts if it finds that there has been a separation of employment, even if the appropriate forms have not been submitted.

c. UCD ITS maintains the right to disable user access when it finds a breach that endangers the security of ePHI.

B. Workstation Use and Security

1. Each workforce member must use a unique user name and strong password to access ePHI.

2. Computer workstations accessing ePHI must maintain security configurations that restrict access to ePHI to only those workforce members that have been legitimately granted access. Recommended security configurations include, but are not limited to:

- enabling a password protected screen saver;
- setting computers or applications to automatically terminate a computing session after a set period of idle time;
- the use of campus standard anti-virus products; and,
- applying security patches to computer software applications and operating systems.

3. UCD workforce members must observe the UCD Information Systems' Appropriate Use Policy (AUP) which outlines expectations regarding the ethical and permissible use of UCD computing resources.

4. Use of shared user accounts to access ePHI must be granted in advance by ITS for special purposes only. Workforce members inappropriately sharing user names and passwords may be subject to revocation of accounts or other sanctions.

5. UCD ITS will disconnect workstations from the network that pose a threat to UCD information systems due to a suspected policy violation, workstation

intrusions, virus infestations, and other conditions which might jeopardize UCD information or work.

6. UCD ITS will periodically scan workstations and servers for vulnerable software.

7. UCD workforce members must follow the provisions of the UCD ITS Security Computing policy in regard to guarding against, detecting, and reporting malicious software.

8. UCD workforce members shall not attempt to alter audit records or avoid accounting for computing services. (See UCD Information Systems' Appropriate Use Policy.)

9. UCD workforce members shall not use UCD resources to develop or execute programs that could infiltrate the systems or alter the software components of the workstations.

10. Workstations storing ePHI or that may be used to access ePHI must be located in areas with controlled access. An electronic audit trail of access must be maintained. It is the responsibility of unit administrators to establish and enforce a facility security plan to ensure access to workstations under their jurisdiction is restricted to authorized users.

11. All suspected policy violations, workstation intrusions, virus infestations and other conditions which might jeopardize UCD information systems, data, or business must be immediately reported to the HIPAA Security Officer.

C. Documentation

All documentation required by this policy must be retained for a period of six (6) years from when it was created or was last in effect, whichever is later.