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 9.5

Title:	**Facility and Device 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:	**04/08/05**
Applies:	**All UCD campuses**

Introduction

Purpose

This policy outlines the procedures for granting, modifying, and terminating physical access to electronic information systems and the facilities in which they are housed. UCD has adopted this policy to ensure that physical access to ePHI is appropriately limited.

Reference

45 C.F.R. § 164.310(a)

45 C.F.R. § 164.530(c)

Applicability

This policy applies to all supervisors in any physical site that house information systems that contain ePHI. All members of the workforce who have access to ePHI and physical sites housing ePHI must also follow this policy.

Policy

It is the responsibility of UCD Directors of Electronic Security, Information Systems, Facility Operations, Human Resources, and all affected unit managers and supervisors to limit physical access to their electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is not delayed.

Procedures

A. Facility Access Controls

UCD maintains ePHI in various forms throughout the University and its facilities. Facility access controls protect the devices or locations that hold ePHI using a variety of methods, while ensuring that properly authorized access is allowed.

Facility security consists of:

1. Facility Security Plan

   a. Units that house ePHI or systems that may be used to access ePHI must create a unit facility security plan to safeguard the facility, systems, and the equipment used to store or access ePHI against unauthorized physical access, tampering, and theft.

   b. Unit-level plans must be submitted to the Electronic Security Department for review and approval. Unit-level plans must be reviewed by the unit and amended as needed.

   c. UCD must create and amend as needed a campus level facility security plan. The Electronic Security Department will work with Campus Police, the Office of University Counsel, and the HIPAA Security Officer to create and amend the campus-level plan.

   d. Plans may include various control mechanisms as outlined below in section six.

2. Access Control

   a. Each unit manager or supervisor must determine what access is appropriate for each member of the unit workforce who needs physical access to ePHI or areas that house ePHI.

   b. Access determinations must be based on the workforce member's role or function within the unit. Determinations of access should take into account at what time(s) access will occur and under what conditions.

   c. Unit managers or supervisors will work with the Electronic Security Department to request and recommend access for each member of the unit workforce. For specific access forms, contact the Badging Office at (303) 724-0399.

   d. If a workforce member's access needs change or end, the unit manager or supervisor must work with the Electronic Security Department to modify or terminate the member's access.

   e. The Electronic Security Department is responsible for maintaining documentation of all workforce members who are granted physical

access to areas that house ePHI or information systems with ePHI, including documentation on how the decision was made.

f. The unit manager or supervisor must ensure that access is limited to what is appropriate for the workforce member's job function.

g. Visitor Control

i. All visitors to UCD areas in which ePHI is stored or may be accessed are subject to the provisions of the Visitor Policy and its procedures.

ii. Visitors to areas of the facility where ePHI is stored or may be accessed must be accompanied or escorted by a member of the UCD workforce who has legitimate access to the location.

iii. Visitors' access may be subject to authorizations, business associate agreements, confidentiality agreements, etc.

3. Validation Procedures

a. Once an individual's facility access has been determined and recommended by the individual's supervisor, validation of identity is performed by the Badging Office.
b. All members of the UCD workforce are reminded to wear their badges while on University property.

4. Maintenance Records

a. Unit managers and supervisors must retain records documenting physical repairs and modifications to facilities housing ePHI. Documentation may include repairs and modifications to the physical components of a facility such as hardware, walls, doors and locks, and other such components.
b. The Electronic Security Department is responsible for maintaining records on all installations, repairs, or replacements of access control devices at a building or campus-level.

5. Contingency Operations

Each unit that maintains ePHI must create procedures that allow facility access to support the restoration of lost data in the event of an emergency In situations when UCD is seeking to restore lost data under its disaster recovery plan(s), access to critical information systems' sites will be governed by the plan(s) and emergency access controls, as outlined in the Contingency Planning policy.

6. Control Mechanisms

Each unit that houses ePHI must adopt appropriate access control mechanisms to control physical access to all facilities containing ePHI

based systems. Units may control facility access by implementing various controls, such as:

a. Electronic security systems or physical intrusion detection systems;
b. Monitoring systems;
c. Visitor policies;
d. Alarms and various other locking systems;
e. Physical keys, swipe cards, keypads, and biometric devices;
f. Placement of security guards;
g. Restricted area registers (including name, date, time of entry and departure, purpose of visit, and who was visited) or other sign in sheets;
h. Name badges and badge readers;
i. Equipment enclosures, equipment identification, and fasteners;
j. Physical building construction reinforcements for secure areas (including wall, ceiling, and door materials);
k. Proper lighting of secure areas; and,
l. Fire prevention, detection and suppression.

7. Documentation and Records Retention

All documentation required by this policy must be maintained for a period no less than six (6) years from the date of creation or the date last in effect, whichever is later.