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 9.3

Title:	**Auditing**
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:	**02/26/03**
Applies:	**All UCD campuses**

Introduction

Purpose

The HIPAA regulations require that computer systems containing electronic Protected Health Information (ePHI) possess technical mechanisms and administrative processes that protect the confidentiality, integrity, and availability of the software and data they maintain.

Reference

45 C.F.R. § 164.308(a)(1)(ii)(D)

45 C.F.R. § 164.308(a)(5)(ii)(C)

45 C.F.R. § 164.312(b)

Applicability

This policy covers the hardware, software and/or procedural mechanisms implemented by UCD units to record and examine activity in information systems that contain or use ePHI.

Computers covered by this policy include desktop systems, laptops, handheld devices, database servers, application servers, data management systems, and infrastructure devices.

Policy

UCD shall assess potential risks and vulnerabilities by reviewing information system activity, and developing, implementing, and maintaining appropriate administrative, physical, and technical security measures in order to detect and minimize security violations involving ePHI. These protective measures give UCD the ability to identify unauthorized data access activities, assess security safeguards, and respond to potential weaknesses.

Procedures

A. General

UCD maintains a comprehensive internal security control program, which is coordinated by the Information Technology Services Department ("ITS"). Procedures, policies and record keeping activities have been established to ensure proper legal, ethical and business practices.

This program complements the user authentication process and may act as a deterrent to internal abuse by making users aware that audit trails, file access reports, and security incident tracking reports are produced, reviewed and investigated. Violations are subject to applicable sanctions.

The internal security control program may take various forms including regular information system activity review. These reviews incorporate login monitoring, automated reports of audit trails or logs, file access reports, and manually produced security incident tracking reports.

B. Audit Controls

ITS will centrally monitor audit records from firewall and other network protection layer logs, domain logs including login and data access activity, and event logs from host operating systems.

1. Audit Control and Review Plan

An Audit Control and Review Plan must be developed by each unit that hosts ePHI and must be approved by the HIPAA Security Officer. If the unit's ePHI inventory changes, causing its Audit Control and Review Plan to change, the Plan must be re-evaluated and re-submitted to the HIPAA Security Officer. The plan must include:

a. Systems and applications to be logged;

b. Information to be logged for each system;

c. Login reports for each system; and,

d. Procedures to review all audit logs and activity reports, including workforce member responsible for performing the audit, the frequency

the audit is to be performed, and escalation procedures if suspicious activity is detected.

2. Audit Trail

The audit trail provides a means to monitor user activity and detect suspicious activity and/or breaches. It also provides the ability to reconstruct events where data integrity may be questioned and functions as a deterrent to misuse by workforce members. The audit trail process includes the implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

3. Audit Trail Mechanisms

The mechanisms used to capture audit trail information may include use of automated tools designed to report suspicious activity or use of automated warning messages that appear prior to access of sensitive information.

Each unit with systems containing medium and/or high risk ePHI (determined during the regular risk assessment) must log activity. The system hardware, software, and applications must have the capability of creating log files. These logs must include, but are not limited to:

a. user ID;

b. login date/time; and,

c. activity time.

Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.

Audit control mechanisms for systems containing low risk ePHI (determined during the regular risk assessment) are not required.

4. Workforce Accountability

Units must educate their workforce members on the unit's specific audit procedures and requirements as necessary. This includes incorporating the concept of audit trail and individual user accountability.

C. Information System Activity Review

Units that host ePHI must regularly review records of information system activity, such as audit logs, file access reports, and security incident reports. Routine review of information systems activity provides an automatic trail of user actions whenever ePHI is accessed or modified. This review promotes individual user accountability and gives UCD the ability to reconstruct significant events or examine suspicious activities as necessary.

1. Conducting the Review

Units must designate an individual responsible for conducting the review of information systems activity and determine the frequency with which the review will be conducted, based on the unit's Audit Control and Review Plan.

To support an effective review, the following information should be examined: audit trails or logs; file access reports; and, security incident tracking reports. If suspicious activity is detected, the reviewer should collect: type of event; date and time of occurrence; user ID; and, program used.

2. If misuse or suspicious activity is discovered, the unit administrator and HIPAA Security Officer must be contacted.

D. Log-in Monitoring

As part of the unit Audit Control and Review Plan, units must monitor login success and failure to systems that host ePHI. To ensure that unauthorized login attempts are discovered, discrepancies or unusual login patterns must be reported to the department administrator and HIPAA Security Officer.

1. Monitoring of audit trails should be performed with the help of an automated alerting tool or periodic manual review of the logs.

2. Units must educate members of their workforce on their specific procedures and reporting requirements for log-in monitoring.

E. Retention

Audit trails, file access reports, and automated security incident reports in exact and retrievable copy form must be retained in a secure manner, taking into consideration system capability, space issues, and modality. The method of retention and length of time these reports are to be retained is to be determined at the unit level and included in the Audit Control and Review Plan.

All unit procedures, documentation of decisions made, information system activity reviews, and investigations conducted pursuant to this policy must be retained for a period of no less than six (6) years from the date the policy was last in effect or from the date the decision or investigation was made.