AUDIT CONTROLS POLICY

Latest Revision: May 1, 2017
Original Effective Date: April 18, 2005

HIPAA Security Rule Language: *"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."* Standard 45 CFR 164.312(b)

Purpose: This policy reflects CU Medicine's commitment to use appropriate audit controls on its information systems that contain or use electronic protected health information (ePHI).

Policy:

1. CU Medicine must be able to record and examine significant activity on its information systems that contain or use ePHI.

2. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on CU Medicine information systems that contain or use ePHI. When possible, such mechanisms must provide the following information:

   - Date and time of significant activity,
   - Origin of significant activity,
   - Identification of user performing significant activity, and
   - Description of attempted or completed significant activity.

3. The level and type of auditing mechanisms that must be implemented on CU Medicine information systems that contain or use ePHI must be determined by CU Medicine's risk analysis process.

4. As defined in CU Medicine's **Security Management Process Policy**, logs created by audit mechanisms implemented on CU Medicine information systems must be reviewed regularly.

5. When possible, CU Medicine information systems' real-time clocks must be set to the official United States time as reflected by the National Institute of Standards and Technology at http://nist.time.gov, so that audit events are synchronized.

Procedures: Auditing Procedures – Integrity
Auditing Procedures – Windows Servers, Network, and Personal Computers

Scope/Applicability: This policy is applicable to all departments that use or disclose electronic protected health information for any purpose.

This policy's scope includes all electronic protected health information.

Regulatory Category: Technical Safeguards

Definitions: See glossary for key terms and acronyms used in this policy.
(On file with Security Officer)

Policy Authority/ Enforcement: Enforcement of this policy will reside with the Security Officer or appropriate Management.

Related Policies: Security Management Process Policy
Security Awareness and Training Policy
Computer Security Audit Policy

Renewal/Review: This policy is to be reviewed periodically to determine if the policy complies with current HIPAA Security regulations. In the event that significant related regulatory changes occur, the policy will be reviewed and updated as needed.

MM/DD/YYYY	COMMENT
05/01/2017	**Updated and reviewed for CU Medicine name change**
9/20/13	**Reviewed and updated for Omnibus Rules; Senior Security/Project Manager.**
7/24/12	**Reviewed; Senior Security/Project Manager.**

Governance: Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		**Executive Approval**	
Security Officer:	**05/10/17**	**Chief Financial Officer:**	**05/01/17**
Signature on file.	**Date**	**Signature on file.**	**Date**