ACCESS CONTROL POLICY

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

HIPAA Security Rule Language:

"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in [the Information Access Management Standard]." Standard 45 CFR 164.312(a)(1)

"Assign a unique name and/or number for identifying and tracking user identity." Required Implementation Specification for Access Control Standard 45 CFR 164.312(a)(2)(i)

"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency." Required Implementation Specification for Access Control Standard 45 CFR 164.312(a)(2)(ii)

"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity." Addressable Implementation Specification for Access Control Standard 45 CFR 164.312(a)(2)(iii)

"*Implement a mechanism to encrypt and decrypt electronic protected health information."* Addressable Implementation Specification for Access Control Standard 45 CFR 164.312(a)(2)(iv)

Purpose:

This policy reflects CU Medicine's commitment to provide information system access only to those entities that have been granted access rights in accordance with its **Information Access Management Policy**.

Policy:

1. As appropriate, CU Medicine information systems must support user, role, or context based types of access control to protect the confidentiality, integrity and availability of electronic protected health information (ePHI) contained on CU Medicine information systems.

2. As defined in CU Medicine's **Information Access Management Policy,** CU Medicine information systems must support a formal process for

granting appropriate access to CU Medicine information systems containing ePHI.

3. Access to CU Medicine information systems must be via user identifiers that uniquely identify workforce members and enable activities with each identifier to be traced to a specific person or entity.

4. CU Medicine must have an emergency access procedure enabling authorized workforce members to obtain required ePHI during an emergency.

5. CU Medicine must implement electronic processes that lock workstations and/or end electronic sessions after a predetermined time of inactivity. CU Medicine workforce members may not disable or alter their workstation locking process.

6. CU Medicine must implement mechanisms to encrypt and decrypt ePHI when deemed appropriate.

7. As specified in CU Medicine's **Transmission Security Policy**, workforce members must use encryption when transmitting ePHI over an open electronic communications network. The CU Medicine and Affiliate networks are considered to be private and secure. Data transmitted within these networks does not require encryption.

8. CU Medicine must ensure all encryption keys meet the minimum encryption key length standard as determined by HCFA.

9. The CU Medicine Information Services department must approve all encryption methods and tools prior to their use. No CU Medicine department will implement encryption of data without the knowledge and approval of the Information Services department.

Procedures:

Computer Orientation
Encryption Key Lengths used at CU Medicine
Encryption Guidelines
Data Integrity Controls
User Account Security Forms
User Account Security Form Instructions
User Account Procedure
Authorization Processes and Procedures
Emergency Application and Data Access Procedure

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: Information Access Management Policy
Transmission Security Policy
Workstation Use Policy
Person or Entity Authentication

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:	**05/01/17**	**Chief Financial Officer:**	**05/01/17**
Signature on file.	**Date**	**Signature on file.**	**Date**