INFORMATION ACCESS MANAGEMENT POLICY

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

HIPAA Security Rule Language:

"Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part." Standard 45 CFR 164.308(a)(4)(i)

"If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization." Required Implementation Specification for Information Access Management Standard 45 CFR 164.308(a)(4)(ii)(A)

"*Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.*" Addressable Implementation Specification for Information Access Management Standard 45 CFR 164.308(a)(4)(ii)(B)

"Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process." Addressable Implementation Specification for Information Access Management Standard 45 CFR 164.308(a)(4)(ii)(C)

Purpose:

Access to CU Medicine information systems containing electronic protected health information (ePHI) must be managed in order to protect the confidentiality, integrity and availability of ePHI. This policy reflects CU Medicine's commitment to have a process for authorizing appropriate access to CU Medicine information systems containing ePHI.

Policy:

1. CU Medicine must have a process for granting, establishing, modifying, and documenting access to CU Medicine information systems containing ePHI.

2. Appropriate CU Medicine information system owners or their chosen delegates must define, authorize, and regularly review all access to CU Medicine information systems containing ePHI.

3. Access to CU Medicine information systems containing ePHI must be authorized only for an individual having a need for specific information in

order to accomplish a legitimate task. All such access must be defined and documented.

4. All revisions to an individual's access rights must be tracked, logged, and securely maintained.

5. An individual must not attempt to gain access to CU Medicine information systems containing ePHI for which they have not been given proper authorization.

6. An individual must not provide access to CU Medicine information systems containing ePHI to unauthorized persons.

7. An individual must not be allowed access to information systems containing ePHI until properly authorized.

Procedures:
User Account Security Forms
User Account Security Form Instructions
User Account Procedure
Authorization Processes and 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 purposes.

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

Regulatory Category: Administrative 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:
Workforce Security Policy
Facility Access Controls 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:	**05/01/17**	**Chief FinancialOfficer:**	**05/01/17**
Signature on file.	**Date**	**Signature on file.**	**Date**