FACILITY ACCESS CONTROLS POLICY

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

HIPAA Security Rule Language:

"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed." Standard 45 CFR 164.310(a)(1)

"Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency." Addressable Implementation Specification for Facility Access Controls Standard 45 CFR 164.310(a)(2)(i)

"*Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.* Addressable Implementation Specification for Facility Access Controls Standard 45 CFR 164.310(a)(2)(ii)

"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision." Addressable Implementation Specification for Facility Access Controls Standard 45 CFR 164.310(a)(2)(iii)

"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)." Addressable Implementation Specification for Facility Access Controls Standard 45 CFR 164.310(a)(2)(iv)

Purpose:

This policy reflects CU Medicine's commitment to prevent unauthorized physical access to its facilities while ensuring that properly authorized access is allowed.

Policy:

1. CU Medicine must protect the confidentiality, integrity, and availability of its information systems by preventing unauthorized physical access, tampering, and theft to the systems and to the facilities in which they are located, while ensuring that properly authorized access is allowed.

2. CU Medicine must ensure that in the event of a disaster or emergency, appropriate persons can enter its facility to take necessary actions as required by the CU Medicine **Contingency Plan Policy**.

3. In the event of an emergency, only authorized individuals may administer or modify processes and controls, which protect electronic protected health information (ePHI) contained on information systems.

4. CU Medicine must develop and maintain a facility security plan that describes how its facilities and equipment within them are appropriately protected. CU Medicine's facility security plan must include appropriate safeguards for all equipment containing ePHI.

5. All appropriate CU Medicine workforce members must have a current copy of the facility security plan. An appropriate number of current copies of the plan must be maintained off-site.

6. Access to all areas of the CU Medicine facility must be controlled to prevent unauthorized access.

7. All visitors must sign in at CU Medicine's reception desk prior to gaining physical access to its facility office areas, as required by the CU Medicine **Visitor Policy.**

8. CU Medicine information systems containing ePHI must be physically located in areas where unauthorized access is minimized.

9. All physical access rights to CU Medicine areas where information systems containing ePHI are maintained must be clearly defined and documented. Such rights must be provided only to individuals having a need for specific access in order to accomplish the responsibilities of their positions.

10. All visitors to CU Medicine areas where information systems containing ePHI are maintained must show proper identification, state reason for need to access, and sign in prior to gaining access.

11. CU Medicine workforce members must not attempt to gain physical access to CU Medicine facility areas with information systems containing ePHI for which they have not been given proper authorization.

12. CU Medicine workforce members must immediately report to appropriate management the loss or theft of any device (e.g. key, card, or token) that enables them to gain physical access to CU Medicine facilities.

13. Access to software programs for either testing or revision requires an authorized account on the CU Medicine system. The account authorization and establishment process is defined in the **Information Access Management Policy** and associated procedures.

14. CU Medicine must document all repairs and modifications to the physical components of its facilities that are related to security of ePHI. Physical components include, but are not limited to, automated physical access systems, locks, doors, and walls.

Procedures: Accessing Information Services Secured Areas
On-Call Procedures

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: Physical 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: Contingency Plan Policy
Information Access Management Policy
Visitor 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 Financial Officer:**	**05/01/17**
Signature on file.	**Date**	**Signature on file.**	**Date**