WORKFORCE SECURITY POLICY

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

HIPAA Security Rule Language:

"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information." Standard 45 CFR 164.308(a)(3)(i)

"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed." Addressable Implementation Specification for Workforce Security Standard 45 CFR 164.308(a)(3)(ii)(A)

"Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate." Addressable Implementation Specification for Workforce Security Standard 45 CFR 164.308(a)(3)(ii)(B)

"Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section." Addressable Implementation Specification for Workforce Security Standard 45 CFR 164.308(a)(3)(ii)(C)

Purpose:

This policy reflects CU Medicine's commitment to allow access to information systems containing electronic protected health information (ePHI) only to individuals who have been appropriately authorized and to ensure that individuals who can access CU Medicine information systems containing ePHI are appropriately authorized or supervised.

Policy:

1. As defined in CU Medicine's **Information Access Management Policy**, CU Medicine must protect the confidentiality, integrity, and availability of its information systems containing ePHI by preventing unauthorized access

while ensuring that properly authorized workforce member access is allowed.

2. All individuals who access CU Medicine information systems containing ePHI must sign a User Account Security Acknowledgement Form that affirms their responsibility for the protection of the confidentiality, integrity, and availability of CU Medicine information systems and processes. The form must include the sanctions that may be applied if an individual does not meet their responsibilities.

3. CU Medicine managers must ensure that all workforce members who are authorized to access information systems containing ePHI access the information appropriately and in accordance with their respective job duties.

4. The background of all CU Medicine workforce members must be adequately reviewed during the hiring process. Verification checks must be made, as appropriate. Verification checks include, but are not limited to:

    - Business and character references,
    - Confirmation of claimed academic and professional qualifications, and
    - Professional license validation.

5. The type and number of verification checks conducted must be based on the employee's probable access to CU Medicine information systems containing ePHI and their expected ability to modify or change such ePHI.

6. All individuals granted access to CU Medicine's information systems must agree not to provide ePHI or any other confidential information to which they have access to unauthorized persons.

7. It is the responsibility of each CU Medicine department that retains the services of a third party to ensure that the party or person(s) adheres to all appropriate CU Medicine policies.

8. CU Medicine must create and implement a process for terminating access to ePHI when the employment of a workforce member ends.

9. When the employment of CU Medicine workforce members ends, their information systems privileges, both internal and remote, must be disabled or removed within one-half business day of receipt of notification by the Help Desk. CU Medicine information system privileges include, but are not limited to:

    - Workstation and server access,
    - Data and network access,

- Email accounts, and
- Inclusion on email distribution lists.

10. As appropriate, all physical security access codes used to protect CU Medicine information systems that are known by a departing workforce member must be deactivated or changed.

11. When workforce members depart from CU Medicine, they must return all CU Medicine supplied equipment by the time of departure. The return of this equipment must be tracked and logged. Equipment includes, but is not limited to:

    - Portable computers,
    - Building, desk, or office keys,
    - Access cards, and
    - Security tokens.

12. When CU Medicine workforce members' employment ends, their personal electronic files must be destroyed or must be reviewed by their immediate supervisors to determine the appropriate transfer or disposal of any confidential information.

Procedures:
User Account Security Forms
User Account Security Form Instructions
User Account Procedure
Authorization Processes and Procedures
Access Identification Procedures
CU Medicine Information Systems Termination Options
Account Review Termination

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: 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: Information Access Management Policy
Person or Entity Authentication Policy
Security Management Process 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**