PERSON OR ENTITY AUTHENTICATION POLICY

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

HIPAA Security Rule Language: *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."* Standard 45 CFR 164.312(d)

Purpose: This policy reflects CU Medicine's commitment to ensure that all persons or entities seeking access to CU Medicine electronic protected health information (ePHI) are appropriately authenticated before access is granted.

Policy:

1. CU Medicine must create and implement a process for verifying the identity of a person or entity before granting them access to ePHI.

2. At a minimum, CU Medicine's authentication process must include the following:

   - Procedure(s) for both granting a person or entity an authentication method (e.g. password, biometrics, or token) and changing an existing authentication method,
   - All authentication identifiers used for access to CU Medicine ePHI must be uniquely identifiable so activities using the identifier can be traced to an individual person or entity, and
   - Procedure for detecting and responding to unusual or suspicious authentication activity.

3. CU Medicine must use an appropriate and reasonable system(s) to ensure that only properly authenticated persons and entities access its ePHI. Such systems can include but are not limited to:

   - Biometric identification systems,
   - Password systems,
   - Personal identification number (PIN) systems,
   - Telephone callback systems, and
   - Security token systems.

4. When applicable, such authentication system(s) must include, at a minimum:

    - Unique user identifiers (user IDs) that enable persons and entities to be uniquely identified. User IDs must not give any indication of the user's privilege level,
    - A secret identifier (password),
    - The prompt removal or disabling of authentication methods for persons and entities that no longer need access to CU Medicine ePHI, and
    - Verification that redundant user identifiers are not issued.

5. All authentication methods must meet the defined standard(s) of the CU Medicine Information Services Department.

6. All authentication data, such as passwords and PINs, must be protected with appropriate access controls to prevent unauthorized access.

7. All password and PIN based authentication systems on CU Medicine information systems must mask, suppress, or otherwise obscure the passwords and PINs so that unauthorized persons are not able to observe them.

8. Methods (e.g. password or PIN) for authentication to CU Medicine information systems should not be built into logon scripts. All exceptions must be reviewed and approved by appropriate management.

9. CU Medicine employees must not share or reveal their authentication methods to others. Sharing an authentication method means the authorized user assumes responsibility for actions that another party takes with the disclosed method. A CU Medicine employee who believes that their authentication method is being inappropriately used must immediately notify his or her manager.

10. As also reflected in CU Medicine's **Workstation Security Policy,** CU Medicine employees must immediately report the loss or theft of an access method to the CU Medicine Help Desk.

11. As defined in CU Medicine's **Workstation Use Policy,** CU Medicine employees activate workstation locking software.

12. Authentication attempts to all CU Medicine information systems must be limited. Authentication attempts that exceed the limit must result in the account being disabled. Assistance from the CU Medicine Help Desk is required to reinstate disabled accounts.

Procedures: User Account Security Forms
User Account Security Form Instructions

User Account Procedure
Authorization Processes and 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: 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 Awareness and Training Policy
Workforce Security Policy
Workstation Use Policy
Workstation Security Policy
Computer Security Password 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**