SECURITY AWARENESS AND TRAINING POLICY

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

HIPAA Security Rule Language:

"Implement a security awareness and training program for all members of its workforce (including management)." Standard 45 CFR 164.308(a)(5)(i)

"Implement . . . Periodic security updates." Addressable Implementation Specification for Security Awareness and Training Standard 45 CFR 164.308(a)(5)(ii)(A)

"Implement . . . Procedures for guarding against, detecting, and reporting malicious software." Addressable Implementation Specification for Security Awareness and Training Standard 45 CFR 164.308(a)(5)(ii)(B)

"Implement . . . Procedures for monitoring log-in attempts and reporting discrepancies." Addressable Implementation Specification for Security Awareness and Training Standard 45 CFR 164.308(a)(5)(ii)(C)

"Implement . . . Procedures for creating, changing, and safeguarding passwords." Addressable Implementation Specification for Security Awareness and Training Standard 45 CFR 164.308(a)(5)(ii)(D)

Purpose:

This policy reflects CU Medicine's commitment to provide regular security awareness and training to its workforce members.

Policy:

1. As defined in CU Medicine's **Training Policy**, all workforce members must be trained to carry out their duties within the organization in compliance with HIPAA requirements.

2. After the training has been conducted, each CU Medicine workforce member must verify that he or she has received the training and training materials.

3. All CU Medicine information security policies and procedures must be readily available for reference and review by appropriate employees, affiliates, and business associates.

4. All CU Medicine Information Services workforce members responsible for implementing safeguards to protect information systems must receive

formal training that enables them to stay abreast of current security practices and technology.

5. CU Medicine's Information Services Department is responsible for ensuring that workforce members receive regular security information and awareness.

6. Methods for providing security information and awareness include, but are not limited to:

   - Newsletter articles,
   - Email reminders,
   - Memos, and
   - Workforce member meetings.

7. CU Medicine must develop and implement a process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems and data. All CU Medicine workforce members must be trained and reminded about this process.

8. Unless appropriately authorized, CU Medicine workforce members must not bypass or disable anti-virus/anti-malware software.

9. CU Medicine must develop, implement, and regularly review a process for limiting and monitoring login attempts and reporting discrepancies. Access to all CU Medicine information systems must be via a secure log-in process. All CU Medicine workforce members must be trained and reminded about this process.

10. CU Medicine must develop and implement a process for appropriately creating, changing and safeguarding passwords used to validate a user's identity and establish access to its information systems and data. All CU Medicine workforce members must be regularly trained and reminded about this process.

Procedures: Computer Orientation
Auditing Procedures – Integrity
Auditing Procedures – Windows Servers, Network, and Personal Computers
Computer Security Overview

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:
Training Policy
Security Incident Procedures Policy
Audit Controls Policy
Person or Entity Authentication 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**