SECURITY MANAGEMENT PROCESS POLICY

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

HIPAA Security Rule Language:

"*Implement policies and procedures to prevent, detect, contain, and correct security violations."* Standard 45 CFR 164.308(a)(1)(i)

"*Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."* Required Implementation Specification for Security Management Standard 45 CFR 164.308(a)(1)(ii)(A)

"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec.164.306 (a)." Required Implementation Specification for Security Management Standard 45 CFR 164.308(a)(1)(ii)(B)

"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate." Required Implementation Specification for Security Management Standard 45 CFR 164.308(a)(1)(ii)(C)

"*Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports*." Required Implementation Specification for Security Management Standard 45 CFR 164.308(a)(1)(ii)(D)

Purpose:

This policy reflects CU Medicine's commitment to protect the confidentiality, integrity, and availability of its information systems containing electronic protected health information (ePHI) by implementing policies and procedures to prevent, detect, contain, and correct security violations.

Policy:

1. CU Medicine must implement appropriate and reasonable policies, procedures, and controls to prevent, detect, contain, and correct security violations.

2. The identification, definition, and prioritization of risks to CU Medicine information systems containing ePHI must be based on a risk analysis process. CU Medicine's risk analysis process must include the following:

   - Identification and prioritization of the threats to CU Medicine information systems containing ePHI,
   - Identification and prioritization of the vulnerabilities of CU Medicine information systems containing ePHI,
   - Identification and definition of security measures used to protect the confidentiality, integrity, and availability of CU Medicine information systems containing ePHI,
   - Identification of the likelihood that a given threat will exploit a specific vulnerability on a CU Medicine information system containing ePHI, and
   - Identification of the potential impacts to the confidentiality, integrity, and availability of CU Medicine information systems containing ePHI if a given threat exploits a specific vulnerability.

3. CU Medicine must conduct risk analysis on a regular basis. It must manage risk on a continuous basis and select and implement security measures to protect the confidentiality, integrity, and availability of CU Medicine information systems containing ePHI.

4. Strategies for managing risk should be commensurate with the risks to such systems and reduce the risks to its information systems containing ePHI to reasonable and appropriate levels.

5. All CU Medicine workforce members are responsible for appropriately protecting ePHI contained on CU Medicine information systems from unauthorized access, modification, destruction, and disclosure.

6. CU Medicine workforce members must understand and comply with all applicable CU Medicine security policies and procedures.

7. As defined in CU Medicine's **Sanctions Applicable to Workforce Policy,** CU Medicine must have a process for applying appropriate sanctions against workforce members who do not comply with its security policies and procedures.

8. As defined in CU Medicine's **Audit Controls Policy**, appropriate hardware, software, and/or procedural auditing mechanisms must be implemented on CU Medicine information systems that contain or use ePHI.

9. CU Medicine must regularly review records of activity on information systems containing ePHI. Records of activity may include but are not limited to:

   - Audit logs,
   - Access reports, and

- Security incident tracking reports.

10. Whenever possible, CU Medicine workforce members should not monitor or review activity related to their own user account.

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 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: Sanctions Applicable to Workforce Policy
Audit Controls Policy
Workforce Security 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
05/01/17	**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**