EVALUATION POLICY

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

HIPAA Security Rule Language:

"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart." Standard 45 CFR 164.308(a)(8)(i)

Purpose:

This policy reflects CU Medicine's commitment to regularly conduct a technical and non-technical evaluation of its security controls and processes to document compliance with its security policies and the HIPAA Security Rule.

Policy:

1. CU Medicine must regularly conduct a technical and non-technical evaluation of its security controls and processes to document its compliance with its security policies and the HIPAA Security Rule.

2. CU Medicine must conduct a thorough technical and non-technical evaluation of its security controls and processes when environmental or operational changes occur which significantly impact the confidentiality, integrity, or availability of its electronic protected health information (ePHI).

3. The technical and non-technical evaluation of CU Medicine's security controls and processes must include:

    - A review of CU Medicine's security policies, procedures, and standards to determine whether they are effective and appropriate,
    - A gap analysis of the requirements of CU Medicine's security policies, procedures and standards, and actual practices, and
    - Testing of all significant CU Medicine security controls to ensure that hardware and software controls have been correctly implemented.

4. An appropriate CU Medicine business unit such as the information security officer, internal audit department, or an outside organization that has appropriate skills and experience may perform the evaluation.

5. The results of the evaluation must be documented and presented to appropriate CU Medicine management. The document must be securely maintained.

6. All appropriate areas and employees within CU Medicine must be included in the evaluation.

Procedures: All HIPAA Security 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: 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: All HIPAA Security Policies

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 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**