ASSIGNED SECURITY RESPONSIBILITY POLICY

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

HIPAA Security Rule Language: *"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate."* Standard 45 CFR 164.308(a)(2)(i)

Purpose: This policy reflects CU Medicine's commitment to assign a single employee with overall final responsibility for the confidentiality, integrity, and availability of its electronic protected health information (ePHI).

Policy:

1. The CU Medicine Information Security Officer is to provide for the development, implementation, and management of information technology security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all organizational information systems, while safeguarding ePHI as defined by the HIPAA Security Rule.

2. The CU Medicine Information Security Officer's responsibilities include, but are not limited to:

    - Develops, implements, and communicates information technology security policies and procedures,
    - Performs information technology security risk assessments, risk management, and on-going evaluation,
    - Serves as information technology security consultant to the organization. Ensures the integration of information technology security with business strategies and requirements,
    - Collaborates with the Compliance/Privacy Officer to ensure the alignment of security and privacy, as well as the analysis and resolution of joint security and privacy issues that arise, and
    - Addresses and ensures disaster recovery of information systems and data.

Procedures: CU Medicine Information Security Officer Job Description

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: None.

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**