TRANSMISSION SECURITY POLICY

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

HIPAA Security Rule Language:

"*Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*" Standard 45 CFR 164.312(e)(1)

"*Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."* Addressable Implementation Specification for Transmission Security Standard 45 CFR 164.312(e)(2)(i)

"*Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."* Addressable Implementation Specification for Transmission Security Standard 45 CFR 164.312(e)(2)(ii)

Purpose:

This policy reflects CU Medicine's commitment to appropriately protect the confidentiality, integrity, and availability of all data that it transmits over electronic communications networks.

Policy:

1. CU Medicine must appropriately protect the confidentiality, integrity and availability of all data it transmits over electronic communications networks.

2. CU Medicine workforce members must use encryption when transmitting electronic protected health information (ePHI) over an open electronic communications network. The CU Medicine and Affiliate networks are considered to be private and secure. Data transmitted within these networks does not require encryption.

3. CU Medicine must implement a process identifying how CU Medicine data requiring encryption and integrity controls will be transmitted over electronic communications networks.

4. As described in CU Medicine's **Access Control Policy**, the CU Medicine Information Services department must approve all encryption methods and tools prior to their use. No CU Medicine department will implement

encryption of data without the knowledge and approval of the Information Services department.

5. As described in CU Medicine's **Integrity Policy**, workforce members must use appropriate integrity controls when transmitting data across an open electronic communications network.

Procedures: Computer Orientation
Encryption Guidelines
Data Integrity Controls

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: Access Control Policy
Integrity 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**