INTEGRITY POLICY

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

HIPAA Security Rule Language:

"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction." Standard 45 CFR 164.312(c)(1)

"Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner." Addressable Implementation Specification for Integrity Standard 45 CFR 164.312(c)(2)

Purpose:

This policy reflects CU Medicine's commitment to appropriately protect the integrity of all electronic protected health information (ePHI) contained on its information systems.

Policy:

1. CU Medicine must appropriately protect the integrity of all ePHI contained on its information systems. Such ePHI must be protected from improper alteration or destruction.

2. CU Medicine must implement appropriate electronic mechanisms, to confirm that ePHI contained on its information systems has not been altered or destroyed in an unauthorized manner.

3. Methods used to protect the integrity of ePHI contained on CU Medicine information systems must ensure that the value and state of the ePHI is maintained and is protected from unauthorized modification and destruction. Such controls include but are not limited to:

    - Checksums,
    - Digital signatures,
    - Hash values,
    - Encryption,
    - Anti-virus protection,
    - Intrusion detection, and
    - Backup procedures.

Procedures:
Data Integrity Controls
Contingency Plan Documentation Table of Contents
Computer Orientation
Encryption Guidelines

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
Transmission 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
05/01/2017	**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**