SECURITY INCIDENT PROCEDURES POLICY

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

HIPAA Security Rule Language:

"Implement policies and procedures to address security incidents." Standard 45 CFR 164.308(a)(6)(i)

"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes." Required Implementation Specification for Security Incident Procedures Standard 45 CFR 164.308(a)(6)(ii)

Purpose:

This policy reflects CU Medicine's commitment to implement policies and procedures for detecting and responding to security incidents.

Policy:

1. CU Medicine must have a process for detecting and responding to security incidents that may impact the confidentiality, integrity, or availability of CU Medicine information systems.

2. A security incident, accidental or intentional, caused by internal or external activities or events, is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with computer system operations.

3. Examples of security incidents include, but are not limited to:

    - Denials of service, such as Internet outages or email failures,
    - Infections by malicious code such as viruses and worms,
    - Evidence of hacker activity,
    - Password sharing,
    - CU Medicine premises break-in, and
    - Lost or stolen computer device or electronic material containing electronic protected health information (ePHI) or other restricted/confidential information.

4. CU Medicine workforce members must report any observed or suspected security incidents as quickly as possible to the CU Medicine Help Desk and provide the following information:

    - Name and contact information,
    - Incident description, and
    - Date and time of incident.

5. A CU Medicine workforce member must not prevent another member from reporting a security incident.

6. CU Medicine must organize and maintain a security incident response team (SIRT) that will be CU Medicine's primary coordinator of security incident reporting and response. Members of the SIRT are to include:

    - Information Security Officer,
    - Information Services Department Managers,
    - Information Services Security Manager, and
    - Compliance/Privacy Officer and Chief Operating Officer, as needed.

7. The responsibilities of the SIRT include, but are not limited to:

    - Collecting and preserving of security incident evidence,
    - Analyzing and identifying the cause(s) of a security incident,
    - Evaluating and implementing appropriate mitigations to prevent further recurrence,
    - Notifying appropriate government or law enforcement agencies, patients, employees, and/or Affiliates, and
    - Documenting all actions taken.

8. CU Medicine's Information Security Officer, in cooperation with the appropriate department manager, is authorized to investigate any and all alleged violations of CU Medicine security policies, and to take appropriate action to mitigate the infraction and apply sanctions as warranted.

Procedures: Security Incident Response Procedure

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: HIPAA 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: Security Awareness and Training 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.**
10/8/12	**Updated to include restricted/confidential data and notification of appropriate individuals, organizations and/or agencies. Updated Privacy Officer title to Compliance/Privacy Officer. 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**