DEVICE AND MEDIA CONTROLS POLICY

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

HIPAA Security Rule Language:

"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility." Standard 45 CFR 164.310(d)(1)

"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored." Required Implementation Specification for Device and Media Controls Standard 45 CFR 64.310(d)(2)(i)

"Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use." Required Implementation Specification for Device and Media Controls Standard 45 CFR 164.310(d)(2)(ii)

"Maintain a record of the movements of hardware and electronic media and any person responsible therefore." Addressable Implementation Specification for Device and Media Controls Standard 45 CFR 164.310(d)(2)(iii)

"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment." Addressable Implementation Specification for Device and Media Controls Standard 45 CFR 164.310(d)(2)(iv)

Purpose:

This policy reflects CU Medicine's commitment to appropriately control and dispose of information systems and electronic media containing electronic protected health information (ePHI) moving into, out of, and within its facilities.

Policy:

1. ePHI located on CU Medicine information systems or electronic media must be protected against damage, theft, and unauthorized access. This includes both ePHI received by CU Medicine and created within CU Medicine. ePHI must be consistently protected and managed through its entire life cycle, from origination to destruction.

2. Information systems and electronic media for which this policy applies include, but are not limited to:

    - Computers - servers, desktops, laptops,
    - Hard drives of copiers or multi-function devices,
    - Floppy disks,
    - CD-ROMs,
    - Zip drives and portable hard drives, and
    - Backup tapes.

3. All CU Medicine information systems and electronic media containing ePHI must be disposed of properly when no longer needed.

4. Disposal of all CU Medicine electronic media and information systems containing ePHI must be tracked and logged.

5. All ePHI on CU Medicine information systems and electronic media must be removed before such media can be re-used. ePHI must be removed with erase tools that have been approved by CU Medicine's Information Services Department.

6. ePHI should not be stored on iPhones, Droids or the hard drive of desktop or laptop computers. It is strongly recommended that all ePHI be stored on CU Medicine's network drives.

7. All movement of CU Medicine information systems and electronic media containing ePHI into and out of its facilities must be tracked and logged. Those responsible for such movement must take all appropriate and reasonable actions to protect ePHI.

8. CU Medicine workforce members must immediately report to the CU Medicine Help Desk the loss or theft of any information system or electronic media.

9. Backup copies of all ePHI located on CU Medicine information systems or electronic media must be made and securely stored prior to the movement of the equipment, as defined in CU Medicine's **Contingency Plan Policy** and its associated procedures.

Procedures: Device and Media Controls 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: Physical 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: Computer Hardware Installation and Support Policy
Contingency Plan Policy
Workstation Use Policy
Workstation 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.**
06/29/2012	Modified for data storage on smart devices, copiers, printers and hard drives.

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**