WORKSTATION USE POLICY

Latest Revision: September 20, 2013
Original Effective Date: April 18, 2005

HIPAA Security Rule Language: *"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information."* Standard 45 CFR 164.310(b)

Purpose: This policy reflects CU Medicine's commitment to appropriately use and protect its workstations.

Policy:

1. CU Medicine workstations are intended for CU Medicine business use. Such use shall demonstrate respect for intellectual property, ownership of data, and security controls.

2. All workforce members who use CU Medicine workstations must take all reasonable precautions to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).

3. ePHI should not be stored on the hard drive of CU Medicine workstations, laptops, or mobile devices.

4. Workforce members must not use CU Medicine workstations to engage in any activity that is either illegal under local, state, federal, or international law or is in violation of CU Medicine policy. Commercial ventures, religious or political causes, outside organizations, or other non-job related solicitations are prohibited.

5. Access to all CU Medicine workstations must be controlled with a username and password or an access device such as a token.

6. Access to all CU Medicine workstations must be authenticated via a process that includes unique user IDs that enables users to be identified and tracked. Access privileges for workforce members whose employment or contracted service with CU Medicine has ended will be removed.

7. Where possible, the initial password(s) issued to a new CU Medicine workforce member must be valid only for the new user's first logon to a workstation. At initial logon, the user must be required to choose another password. Where possible, this same process must be used when a workforce member's workstation password is reset.

8. Workforce members should log off a workstation before logging into another workstation.

9. CU Medicine IS Department approved anti-virus/anti-malware software must be installed on workstations to prevent transmission of malicious software. Such software must be regularly updated.

10. Workforce members must not:

    - Violate the right to privacy of protected healthcare information of CU Medicine's patients,
    - Install or distribute "pirated" or other inappropriately licensed software products,
    - Deliberately introduce malicious software onto a workstation or network (e.g., viruses, worms, Trojan horses),
    - Engage in procuring or transmitting material that is in violation of CU Medicine sexual harassment or hostile workplace policies,
    - Purposefully cause security breaches. Security breaches include, but are not limited to, accessing electronic data that the workforce member is not authorized to access or logging into an account that he or she is not authorized to access. CU Medicine employees that perform this activity as part of their defined job are exempt from this prohibition,
    - Perform any form of network monitoring that will intercept electronic data not intended for the workforce member. CU Medicine employees that perform this activity as part of their defined job are exempt from this prohibition,
    - Circumvent or attempt to avoid the user authentication or security of any CU Medicine workstation or account. Employees that perform this activity as part of their defined job are exempt from this prohibition, and
    - Place magnets or magnetic material near or on computer equipment, including computer disks such as floppies.

11. CU Medicine workforce members must enable screen savers with password protection so that screen displays are masked after no more than fifteen minutes of inactivity and to ensure that a password is required before the display can be reactivated.

12. CU Medicine workforce members must activate their workstation locking software whenever they leave their workstation unattended. CU Medicine workforce members must lock, log off from or shut down their workstation(s) when their shifts are complete.

13. Computer equipment including, but not limited to, mobile devices or workstations used off-site must be protected with security controls equivalent to those for on-site workstations. These security controls include, but are not limited to:

    - CU Medicine management approval for moving the equipment off-site,
    - CU Medicine IS Department approved encryption used to protect ePHI,
    - Activated locking software (including screen savers) for unattended equipment,
    - Current firewall, anti-virus/anti-malware protection, and
    - Equipment placed and maintained in a secure location.

Procedures: Computer Orientation

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: Device and Media Controls Policy
Computer Hardware Installation and Support
Computer Security Audit Policy
Computer Hardware and Software Acquisition Policy
Security Awareness and Training Policy
Person or Entity Authentication Policy
Computer Security Password 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
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:	**09/20/13**	**Chief Operating Officer:**	**09/20/13**
Signature on file.	**Date**	**Signature on file.**	**Date**