

TITLE: EPHI5. WORKSTATION USE AND SECURITY

POLICY:

CUMC workforce members understand purposes and functions that are authorized on their workstations to access Electronic Protected Health Information (EPHI), and do not use workstations for unauthorized purposes or to perform unauthorized functions. This policy is in addition to ***CU Desktop and Laptop Security policy***.

PURPOSE:

CUMC defines acceptable functions to be performed at workstations, the manner in which they are performed, and the physical surroundings of workstations that can access EPHI systems.

APPLICABILITY:

CUMC faculty, staff, students, owners, custodians, and users of EPHI systems

PROCEDURE:

1. The authorized purposes of each workstation are to support the clinical, research, education, administrative and other legitimate functions of the institution.
2. Workforce members may not perform the following activities, as they are considered examples of unauthorized uses of workstations:
 - A. Violating any of institutional policies and procedures.
 - B. Violating the privacy of patients and/or workforce members.
 - C. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations. (e.g., installation or distribution of 'pirated' or other inappropriately licensed software).
 - D. Unauthorized copying, distribution and transmission of copyrighted material (e.g., digitization and distribution of photographs from magazines, books, music, video, movies or other copyrighted sources).
 - E. Intentional introduction of malicious software onto a workstation or network.
 - F. Transmitting material that is in violation of institutional sexual harassment or hostile workplace policies.
 - G. Making offers of products, items or services that are fraudulent and/or not related to the organizational business.
 - H. Intentionally causing a security incident (e.g., accessing electronic data that the workforce member is not authorized to access, logging into an

account that the workforce member is not authorized to access, denying legitimate work to continue on the information systems, etc.).

- I. Performing monitoring (network, computer, device, or any other) that will intercept data not intended for the workforce member unless specifically permitted by the Information Security Office.
- J. Attempting to avoid the user authentication or security of workstations or accounts.
- K. Allow patients to use institutional computers for personal use.
- L. Any unlawful activities.

This list is not intended to be an all-inclusive list.

3. Workforce members are responsible for reporting suspected unauthorized access/use of a workstation as specified in **Information security incident procedures policy** (#EPHI10).
4. Access to workstations is controlled by requiring authentication using a UserID and a password or an access device (e.g., token), unless specifically exempted based on an institutional purpose.
5. Access to workstations are authenticated via a process that normally includes:
 1. Unique User IDs that enable users to be identified and tracked. The User IDs used should be institutional User ID (Center-Wide User ID or Universal Network Identifier at CUMC, consult Information Security Office for *Information security procedures list: Center-wide identifier creation procedure*). A generic Group ID may be used only to access workstations that do not themselves store EPHI.
 2. Removal of workstation access privileges for workforce members when employment or contracted services have ended in accordance with **Workforce security clearance, termination and authorization policy** (#EPHI6).
 3. Verification that no redundant user IDs are issued.
6. Workforce members understand and follow the authentication and password management requirements as defined in **General information security policy** (#EPHI3).
7. Workstations are protected by processes and methods defined in **General information security policy** (#EPHI3).
8. Workforce members, if they used their individual userID to sign on, should sign off when they leave their workstation. Alternately, they are instructed to activate their workstation locking when they leave their workstations temporarily. (On a Windows workstation, it is locked by pressing the *Ctrl+Alt+Delete* keys together and then select 'Lock Workstation' or equivalent

button.) In general, the workstation may be configured to lock itself automatically after 3 minutes of inactivity, unless there are mitigating factors such as physically locked rooms and offices. In all cases, the workstation should sign off the user after detecting 15 minutes (maximum) of inactivity.

9. Portable workstations that are removed from the organization (e.g., laptops) are protected with security controls equivalent to on-site workstations.
10. Additional precautions are implemented for portable workstations (e.g., laptops, PDAs, portable medical equipment that stores sensitive information). The following guidelines are followed for such workstations (see **Information security: Backup, media and device controls policy** (#EPI7)):
 - A. EPHI may not be stored on a portable workstation unless it is protected (e.g., using encryption or (preferably and) password protection).
 - B. Workforce members must take reasonable steps to ensure that portable workstations are physically protected (e.g., carried as carry-on baggage when using public transportation, concealed and locked when using private transportation, not shared with other people, etc.)
11. Every department that accesses electronic information on its workstations is responsible for conducting a risk analysis to determine the level of physical protection required commensurate with threats and risks to the workstations. Also see **Information security: Facilities access control and security policy** (#EPI8). Such measures include:
 - A. Locating workstations and peripheral devices in secured areas not accessible by unauthorized workforce members or other unauthorized personnel or other individuals.
 - B. Positioning or shielding workstations so that data shown on the screen is not visible by unauthorized persons.
 - C. Implementing additional measures including screen savers, inactivity timeout or requiring workforce members not to leave workstations unsupervised.
12. Workforce members are required to report the loss or theft of any device containing EPHI as specified in **Information Security Incident Procedure** (#EPI10).

POLICY MAINTENANCE:

Information Security Office

REFERENCES:

*All information security policies
CU Administrative policies in Computing & Technology*

Health Insurance Portability and Accounting Act of 1996, 45 CFR
164.310(b), 164.310(c)

REVIEW/REVISION DATE:

November 2007