TITLE: WORKSTATION USE AND SECURITY

POLICY:

Workforce members will use workstations in an appropriate and authorized manner. The authorized purposes of each workstation are to support the clinical, research, education, administrative and other legitimate functions of the institution.

PURPOSE:

Define acceptable functions performed at workstations, the manner in which these are performed, and the physical surroundings of workstations that can access electronic information systems.

APPLICABILITY:

Hospital staff, employees, owners, custodians, and users of information systems

PROCEDURE:

1. The following activities 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 the ability of legitimate work to continue on the information systems).

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. Allowing patients to use institutional computers for personal use unless clearly designated for such use.

L. Any unlawful activities.

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

2. Workforce members are responsible for reporting suspected unauthorized access/use of a workstation to the Service Desk or their manager. See Information security incident procedures policy (# 1255).

3. Access to workstations is controlled by requiring authentication using a User ID and a password or an access device (e.g., token), unless specifically exempted based on an institutional purpose. Unique User IDs enable users to be identified and tracked. The User IDs used should be institutional User ID (Center-Wide User ID, consult Information Security Office for Information security procedures list: Center-wide identifier creation procedure). A generic ID may be used only to access workstations that do not themselves store Electronic Protected Health Information.

4. Removal of workstation access privileges for workforce members when employment or contracted services have ended must be done in accordance with Workforce security clearance, termination and authorization policy (# 1235).

5. Workforce members shall follow the authentication and password management requirements. See General information security policy (# 1220).

6. Workforce members, if they used their individual User ID 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.
7. Portable workstations and devices that are used outside the organization are protected with security controls equivalent to on-site workstations.

8. Additional precautions are implemented for workstations and storage devices (e.g., laptops, USB storage devices, 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 (# I240)):

A. Sensitive data may not be stored on a workstation or device unless it is secured using encryption 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.)

9. 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 & security policy (# I245). 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.

10. Workforce members are required to report the loss or theft of any device as specified in Information security: Facilities access control & security policy (# I245).

RESPONSIBILITY:

Information Security Office

REFERENCES:

All information security policies
Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.310(b), 164.310(c)
REVIEW/REVISION DATE:

March 2005
June 2009
June 2011
Revised: June 2013