Current Status: *Active*	**PolicyStat ID:** *4806689*

Origination:	*09/2013*
Effective:	*09/2013*
Last Approved:	*09/2013*
Last Revised:	*09/2013*
Next Review:	*08/2016*
Owner:	*Colleen Ebel: HCS Dir Info Technology*
Policy Area:	*Information Services Division*
Policy Tag Groups:	
Applicability:	*UNC Medical Center*

Workstation Security

I. Description

Security procedures for UNC HCS workstations

II. Rationale

It is the policy of the UNC Healthcare System (UNC HCS) to protect electronic Protected Health Information (ePHI), Confidential Information and Internal Information stored or accessed through workstations or personal computers (PC) to prevent unauthorized access, disclosure and/or modification. This protection requires the implementation of physical, technical and procedural safeguards. (Refer to UNC HCS Information Security Policy for definitions, PHI, Confidential Information and Internal Information classification standards, and additional security requirements.)

III. Policy

A. Information Storage/Backup:

PHI, Confidential Information, and Internal Information should not be stored on end user computers. To ensure appropriate levels of controls for stored data, it is recommended that information be stored on UNC HCS IT approved file servers. Workstations containing the authoritative source of critical UNC HCS information must be backed up on a regular basis with the ability to retrieve an exact copy of the electronic information.

Should it be necessary to keep ePHI, Confidential and/or Internal Information on an end user computer, it is the responsibility of the owner/user to implement the following safeguards:

1. Store back up data on a secure UNC HCS IT approved server.
2. Test backup data to ensure reliability of backup/restore procedures.
3. PHI or Confidential Information stored on a mobile device or removable media must be protected by encryption.

B. Physical Access:

Workstations or PCs must be secured against use and/or viewing by unauthorized individuals. Physical safeguards must be implemented as determined by risk analysis.

The following physical safeguards must be implemented:

1. Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to ePHI.
2. Workstations must be positioned to minimize unauthorized viewing of ePHI.
3. Privacy screens should be installed on workstations where unauthorized viewing cannot be minimized.
4. Screen savers should be automated to protect unattended machines. If the applications to which workstations deliver access do not have an inactivity timeout with re-authentication, the screen saver should lock and require the user to re-authenticate to gain access.
5. Workstations containing ePHI, Confidential and/or Internal Information should be located in a secure area to prevent theft, destruction, or access by unauthorized individuals.

C. Equipment Controls:

The receipt and removal of hardware containing ePHI and/or Confidential Information and the movement of these items within the facility must be managed.

1. Inventory / Tracking:

   UNC HCS IT End User Services (EUS) is responsible for maintaining an inventory of all UNC HCS workstations. An electronic database is used to maintain a listing of all workstations. The inventory is updated during initial installation of workstations, when workstations are relocated, with an automated network inventory scanner, and when UNC HCS IT EUS visits departments for troubleshooting workstations. It is User Management's responsibility to notify UNC HCS ITEUS when workstations are moved within their departments to ensure the inventory of workstations is kept up-to-date. User Management must contact the UNC HCS IT Help Desk and request a ticket be entered that will be forwarded to UNC HCS IT EUS.

2. Reallocation (Re-use):

   UNC HCS IT EUS is responsible for removing ePHI and Confidential Information before reallocating workstations. User Management is responsible for notifying UNC HCS IT EUS when workstations need to be reallocated or removed from their department. User Management must contact the UNC HCS IT Help Desk and request a ticket be entered that will be forwarded to UNC HCS IT EUS.

3. Surplus (Disposal):

   UNC HCS IT EUS is responsible for the proper disposal of workstations to ensure the continued protection of ePHI and Confidential Information. User Management is responsible for notifying UNC HCS IT EUS to arrange for the disposal of workstations. User Management must contact the UNC HCS IT Help Desk and request a ticket be entered that will be forwarded to UNC HCS IT EUS.

D. Personally Owned End User Computers:

End user smart phones, tablets and laptops purchased by the user and used on the UNC HCS business networks are subject to the UNC HCS security policies and standards. The end user must configure his/

her device as follows:

- Strong PIN or Password – as strong as the UNC HCS standard for passwords if supported on the device. If UNC HCS password strength standards are not supported on the device, the password or pin should be as strong as the device allows.
- Inactivity timeout with re-authentication
- Automated OS security updates
- Encryption of content on the device if content encryption is supported by the device. Note: PHI and Confidential Information may not be stored on mobile devices that cannot encrypt content.
- Encryption of data in transmission.

Personally owned end user device owners may be required to sign an annual agreement in order to access business and clinical resources using their personally owned device.

The UNC HCS may deploy technical controls to enforce these security configurations on personally owned devices that are configured to access PHI or Confidential Information. Users of devices that do not offer the security controls options listed above should follow the exception process to ensure an optimal mitigation strategy is followed.

Attachments:

No Attachments

Applicability

UNC Medical Center