Title: Computer Workstation Use and Security Policy Number: A-ISN-0022 **Replaces (supersedes):** CHA Cambridge Health Alliance	**Policy Chronicle:** Effective Date:1/27/2025 Date the Original Version of Policy was Effective: (month/year): 4/20/2005 Most Recent Review (month/year): 11/2024 Owner: (Name/Title) Astrid Lambert Previous Review: Previous Reviews: 1/2022 Previous Reviews: 8/2018 Previous Reviews: 4/2017 Previous Reviews: 4/2014 Previous Reviews: 3/2011 Previous Reviews: 3/2008

Area of Operations:
Information Technology (IT)
	Regulatory /Accreditation Standard(s):
	HIPAA
	164.310(b)
	164.310 (c)

Keyword(s): HIPAA, Security, Workstation	

Purpose:

Physical Safeguards Standard: Implement policies, procedures and physical safeguards for all workstations that access EPHI to restrict access to authorized users and to 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 EPHI.

Personnel:

CHA Workforce

Policy:

Cambridge Health Alliance workstations (including laptops and personal digital assistant (PDAs) and other wireless devices) shall be physically protected from theft, damage, or other loss to the workstation or the EPHI contained therein by the use of locks, bolts, encryption and other physical deterrents when deemed necessary in addition to standard physical safeguards within CHA facilities.

All programmable workstations equipped with fixed storage devices (e.g., hard disks) shall not be used by individuals and programs to store EPHI in the workstation and associated peripherals unless specifically approved by CIO or CISO. Storage areas and facilities for sensitive media shall be secured and all filing cabinets provided with locking devices appropriate to their sensitivity and protective requirements.

Removable media containing EPHI must be stored in a Cambridge Health Alliance approved fireproof receptacle or off-site storage facility.

Workstations that handle EPHI must employ an approved access control mechanism (e.g., software or hardware) to restrict access to authorized users. Only Cambridge Health Alliance authorized applications and utilities may be loaded on user workstations. Unauthorized applications will be removed by the Cambridge Health Alliance IT and the individual who installed the unauthorized application subject to possible disciplinary actions.

All EPHI must be stored on network drives, and can only be stored on local PC or laptop devices with encryption, upon approval by the CISO or CIO. EPHI that is allowed to leave the facility, whether it is on a laptop, PDA, or other forms of portable device, must be properly protected with passwords and files encrypted in secure file structures. All relevant policies must be followed.

Procedures:

1. **Locking Down Public Access PCs in Offices:** Public access PCs restrict user access only to the application intended or permitted for use of such PC.
2. **Protection for Sensitive Workstations:** All workstations that have access to EPHI are configured with screensavers to blank the screen. A power-on password is also used on workstations that access EPHI. Whenever operationally feasible, electronic sessions should terminate after [10] minutes of inactivity.
3. **Access Key Control:** When access keys or combinations (such as room or cabinet keys or locks) are used, a specific, identified individual shall be designated as responsible for managing, distributing, and logging the issuance of keys and combinations to other authorized individuals.
4. **Portable Equipment Control:** An employee who receives permission to remove equipment or electronic media containing EPHI from a Cambridge Health Alliance site must provide a reasonable level of protection for that equipment and associated EPHI, software, data, and media from theft and damage. A record of portable equipment assigned to employees and business associates/subcontractors are to be maintained by the individual or group authorized to distribute such equipment.
5. **Hardware Changes/Configuration Management:**
    a. All computer and communications systems used for processing EPHI employ a formal change control procedure to ensure that only authorized changes are made. The change control procedure is used to document all significant changes to software, hardware, communications links, and operational procedures, including changes to the physical deterrents (such as a change of locks or combinations) protecting such items.
    b. Change management is accomplished organization-wide by Microsoft System Center Configuration Manager (SCCM) and is a Windows product that enables administrators to manage the deployment and security of devices and applications across an enterprise.
6. **Workstation and Terminal Control:** Devices outside of locked computer or communications rooms must be logged off or physically secure when unattended; housed in a facility that provides adequate protection from theft or provided with additional physical safeguards; and protected from environmental hazards (e.g., extreme temperature changes, electrical power surges, dust, dirt, and liquids).

7. **Removal of Sensitive Information:** Employees must receive authorization from the applicable Security Official prior to removing from Cambridge Health Alliance premises any computer, PDA or electronic media containing EPHI.
8. **Inventory:** The storing of EPHI on workstations is not authorized unless specifically approved by CIO or CISO and requires file encryption. All workstations shall be marked with an asset tag and any movement of such equipment is recorded by Facility Security; such records must be maintained in accordance with Cambridge Health Alliance's record retention policy.
9. **Storage:** Cambridge Health Alliance staff must not store sensitive information, including EPHI, on workstation hard-disk drives unless the Security Official has determined that adequate information security encryption measures will be employed on the workstation. Additionally, sensitive information shall not be stored on diskettes, CDs or other memory removable devices without the approval of the Security Official.
10. **Identification Markings:** All media shall contain external identification markings for easy identification as Cambridge Health Alliance property. The identification markings are affixed to all media output, e.g., hardcopy and video displays, to inform users that the data contained therein is the property of Cambridge Health Alliance. Whenever documents/media containing EPHI are reproduced in total or in part, the reproductions shall bear the same identification markings as the original. Reproductions of documents/media containing EPHI shall be kept to the minimum number of copies required.
11. **Rooms and Cabinets to Protect Equipment:** Rooms intended to provide hardware security must limit physical access and control equipment configuration; provide personnel access control, and protect from environmental hazards.

References:

Refer to the AACN Level of Evidence Table for more information

Reference	Level of Evidence	Review Date

Reviewed by:

Committee Name / Content Expert	Chair Person / Name	Date

This policy has been reviewed and approved electronically by:

Approver	Title	Initials	Date
Astrid Lambert	CISO	AL	12/26/2024
Jeannette Currie	Chief Information Officer	JFC	12/26/2024
Renée A. Kessler	EVP Chief Operating Officer	RAK	1/2/2025