Data Security Policy – Workstation Use and Workstation Security

PURPOSE

To provide principles and guidelines for the secure use of workstations by **Organization's** workforce. To provide detailed instructions for the secure configuration and use of workstations by **Organization's** workforce.

SCOPE

The Workstation Use and Workstation Security Policy and Procedures cover Organization's requirements for**:**

- Workstation use
- Workstation security, including
    - Workstation access control
    - Workstation physical security
    - Secure workstation configurations
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization defines workstations as the endpoint devices, such as computers, tablets, or mobile phones, that employees use to conduct their job duties. For on-site workers, this includes their workspace, cubicle, and desk area.

Organization adopts and follows workstation use and security controls that support the confidentiality, availability, and integrity of ePHI and other sensitive information.

Organization catalogs all devices in our IT environment in our asset inventory.

Workstation Use

Employees should only use company-issued or approved assets for their job role and related responsibilities. Only appropriate personnel have access to ePHI or other sensitive information, as required by their role.

Organization requires employees to keep ePHI and other sensitive information secure and prevent unauthorized personnel from viewing or obtaining that information.

Physical Workstation Use

Organization adopts and follows processes that keep workstations, ePHI, and other sensitive information physically secure.

Remote Workstation Use

Temporary, hybrid, and fully remote workers must use secure channels, such as VPN, to access ePHI when they are not at a company facility.

Workstation Security

Organization adopts and follows processes that safeguard workstations with access to ePHI or other sensitive information.

We do not allow the use of removable media, such as USB drives, external hard drives, or SD cards.

Workstation Access Control

Organization adopts and follows processes for restricting access to workstations with access to ePHI or other sensitive information.

Secure Workstation Configurations

Organization has set up workstation configuration baselines in order to protect confidential information. All workstations must meet the workstation configuration baseline to be used for work. These workstation configurations include session timeout, password requirements, and regular anti-virus/anti-malware scans.

PROCEDURES

Organization adopts and follows processes for workstation use and workstation security that support the confidentiality, availability, and integrity of *ePHI* and other sensitive information.

All workstation devices are logged in our asset inventory with the following details:

- Asset tag (highly recommended)
- Unique ID or Serial Number
- Device Name
- Device Type
- Operating System and Version
- Assignee or Device Owner
- IP Address (most recent)
- MAC Address

Workstation Use

Organization's workforce members agree to use company assets and devices for appropriate purposes only. Workforce members should only access ePHI and sensitive information through authorized devices.

Organization does not allow the use of removable media for storing ePHI and other sensitive information.

Workforce Members have *no expectation of privacy* when using Organization's company assets and devices.

Physical Workstation Use

Employees must take measures to prevent unauthorized access to *ePHI* and other sensitive information, including making sure that screens are protected from view, such as through a privacy screen. When transporting endpoint devices, workforce members should keep them locked and out of sight in their vehicles. Passwords should never be written down in an accessible location or kept on a post-it note on your workstation.

Any PHI or sensitive information in physical form must be locked away when not in use. All PHI or sensitive information must be securely destroyed. Physical keys should also be secured and kept out of sight.

Mobile endpoint devices should be locked away in a cabinet or drawer when unattended.

Remote Workstation Use

Workforce members who work remotely must maintain a secure work environment and safeguard ePHI and other sensitive information from unauthorized access.

Workforce members must use VPN or an equivalent secure channel to access ePHI and other sensitive information when working remotely.

Workstation Security

Organization adopts and follows processes for configuring and securing workstations and restricting access to workstations with access to ePHI or other sensitive information.

Workstations are placed in secure locations and to prevent unauthorized individuals from viewing device screens or confidential data.

Workstation Access Control

Individuals receive unique IDs and credentials for logging into workstations. Users must create strong passwords that align with Organization's password requirements.

Users are not allowed to share their credentials with other users.

Secure Workstation Configurations

Organization has set up and defined workstation configuration baselines to protect confidential information and workstation security. All workstations issued by the company are required to meet the workstation configuration baselines. Employees should not tamper with secure workstation configurations.

Organization requires these secure configurations for all company-issued workstations and/or devices:

- **Password Protection:** Endpoint devices must be secured with strong passwords that enforce Organization's password requirements.
- **Anti-Virus and Anti-Malware:** AV/AM software must be installed on all endpoint devices and be scheduled to run and remove malicious software on a weekly basis at minimum.
- **Session Timeout:** Endpoint devices will lock out the session after a set time of inactivity (best practice is <15 minutes). Users must log back into devices using their credentials.
- **Deny Auto-Run:** Endpoint devices should be prohibited from auto-running removable media.
- **Encryption:** Endpoint devices should be encrypted by default.

Organization manages our endpoints and devices using a mobile device management (MDM) solution when appropriate or feasible.

ROLES AND RESPONSIBILITIES

IT Team or IT Manager: Securely configures workstations based on the workstation configuration baseline(s). Issues company devices and workstations. Troubleshoots workstations.

VIOLATIONS

Employees that knowingly disable security controls or circumvent workstation controls may face disciplinary action.

Allowing unauthorized access to ePHI and other sensitive information can lead to disciplinary action, up to and including termination.

FORMS/PLANS/DOCUMENTS

- Workstation Secure Configuration Baseline
- Asset Inventory
- Workstation Use Policy or Acceptable Use Policy

RELEVANT HIPAA REGULATIONS

- [§164.310(b)] https://www.law.cornell.edu/cfr/text/45/164.310 *Workstation use*
- [§164.310(c)] https://www.law.cornell.edu/cfr/text/45/164.310 *Workstation security*

RELEVANT SOC 2 CRITERIA

- CC 6.1.3 *Identifies and Authenticates Users*
- CC 6.1.5 *Manages Points of Access*
- CC 6.7.3 *Protects Removal Media*
- CC 6.7.4 *Protects Mobile Devices*
- CC 6.8.4 *Uses Anti-Virus and Anti-Malware Software*