**POLICY & PROCEDURES**

***Defining the Overall Approach toward Meeting a Requirement***

### **Workstation Use §164.310(b)**

### **Effective Date:** <Month Day, Year>

### **Policy Number:** <If applicable> **Rev.** 0

**Policy:** Our workforce members will take all reasonable precautions to protect the ePHI on our information systems. Workforce members will not engage in any activity at their workstation that is not work-related. Passwords will be used for access and will not be shared with anyone else. Workforce members will log off or lock their workstation whenever they leave their workstation for 10 minutes or more and at the end of their workday. Our Security Official will review and revise this plan on an annual basis or when necessary.

**Procedures:** Workforce members must not use our workstations to engage in any activity that is either illegal under local, state, federal of international law or is in violation of our policy. Access to all of our workstations containing ePHI must be controlled with a unique username and password. All password-based access control systems on our workstations must mask, suppress, or otherwise obscure the passwords so the unauthorized persons are not able to observe them. Our workforce members must not share passwords with others. If a workforce member believes that someone is inappropriately using their user-ID or password, they must immediately inform our Security Official. Our workstations containing ePHI must be physically located in such a manner as to minimize the risk that unauthorized individuals can gain access to them. The display screen of all of our workstations containing ePHI must be positioned such that information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in the reception area or other related areas. Our workforce members must activate their workstation locking software whenever they leave their workstation unattended for 10 minutes or more. Our workforce members must log off from or lock their workstation(s) at the end of their workday.

**Details:** The workstation use procedures include but are not limited to:

* Workstations will be used only for authorized purposes that support our organization’s mission. Such use demonstrates respect for intellectual property, ownership of data, security controls, and individuals' rights to privacy.
* Workforce members will not use workstations to engage in any activity that is either illegal under local, state, federal, or international law or is in violation of our policy.
* Access to workstations will be controlled and authenticated.
* Workstations will be located in physically secure areas and display screens will be positioned to prevent unauthorized viewing.
* Workforce members must activate workstation-locking software (press <Windows key> + <L> key) whenever their workstation is unattended for more than 10 minutes.
* Workforce members with access to ePHI are prohibited from storing/downloading ePHI data on any device (e.g. workstations, portable devices, home computer, etc.) unless authorized by the Security Official and only in the course of approved work-related functions or activities.
* Activities which workforce members must not perform while using workstations include, but are not limited to:
* Violations of the rights to privacy of protected healthcare information of our patients and clients.
* Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property or similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" or other inappropriately licensed software products.
* Unauthorized copying of copyrighted material, including but not limited to digitization and distribution of photographs from magazines, books, or other copyrighted sources and copyrighted music.
* Purposeful introduction of malicious software onto a workstation or network (e.g., viruses, worms, Trojan horses).
* Making fraudulent offers of products, items, or services.
* Purposefully causing security breaches. Security breaches include, but are not limited to, accessing electronic data that the workforce member is not authorized to access or logging into an account that he or she is not authorized to access. Workforce members that perform this activity as part of their defined job are exempt from this prohibition.
* Performing any form of network monitoring that will intercept electronic data not intended for the workforce member. Workforce members that perform this activity as part of their defined job are exempt from this prohibition.
* Circumventing or attempting to avoid the user authentication or security of any workstation or account. Workforce members that perform this activity as part of their defined job are exempt from this prohibition.
* Documentation (e.g. policies and procedures) of the practices in place will be retained as evidence of compliance.

**Location of supporting documentation:** If so, identify the document and location it is stored here.

## REVISION HISTORY

| Revision | Date | Initiator | Nature of Change |
| --- | --- | --- | --- |
| 0 |  |  | Initial draft |
| 1 |  |  |  |