**POLICY & PROCEDURES**

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

### **Workstation Security §164.310(c)**

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

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

**Policy:** Our workstations containing ePHI must be placed in locations that minimize the risk of unauthorized access to them. Workforce members must take reasonable measures to prevent viewing ePHI on workstations by unauthorized persons. Unauthorized workforce members must not attempt to gain physical access to workstations that can access ePHI. Workforce members must report loss or theft of any workstation or device containing ePHI.

**Procedures:** Workstation security procedures address how workstations are to be physically protected from unauthorized users. Our Security Official will coordinate the physical placement of our workstations in order to locate them where the risk of unauthorized access is minimal. Other strategies we use to restrict access to workstations with ePHI include using privacy screens; enabling password protected screen savers or logging off the workstation as well as positioning computer monitors away from patient view. Workforce members will need to take reasonable steps to prevent the viewing of ePHI on their workstations especially when outside the facility. Our Security Official will review and revise this procedure on an annual basis or when necessary.

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

* Workstations containing ePHI will be located in physically secure locations that minimize the risk of unauthorized access to them. A secure location would minimally be defined as one that is not routinely accessible to the public, particularly if authorized personnel are not always available to monitor security.
* Secure locations must have physical access controls (e.g. door locks) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security.
* Institutionally approved anti‐virus software must be installed on workstations to prevent transmission of malicious software.
* Workforce members will take reasonable measures to prevent unauthorized access to ePHI visible on their workstations. Such measures include but are not limited to:
* Locating workstations and peripheral devices (printer, modem, scanner, etc.) in secured areas not accessible to unauthorized persons.
* Positioning monitors or shielding workstations so that data shown on the screen is not visible to unauthorized persons.
* Unauthorized workforce members must not attempt to gain physical access to workstations that can access ePHI.
* All portable workstations will be securely maintained when in the possession of workforce members. Such workstations will be handled as carry-on (hand) baggage on public transport and concealed and/or locked when in private transport (e.g. locked in the trunk of an automobile).
* An accurate inventory of the types and locations of workstations (e.g. laptops, workstations, and other portable devices or media) will be conducted on a periodic, at least annual, basis. The date of and updates to the inventory will be documented and maintained.
* Workforce members will receive training of their role in protecting the physical security of workstations. The loss or theft of any workstation or device containing ePHI must be reported to the Security Official.
* 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 |  |  |  |