**POLICY & PROCEDURES**

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

### **Access Control and Validation Procedures §164.310(a)(2)(iii)**

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

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

**Policy:** Access rights to areas where ePHI is kept should be given only to workforce members who have a need for specific physical access in order to accomplish a legitimate task. Our workforce members must not attempt to gain physical access to sensitive areas containing information systems having ePHI or software programs that can access ePHI for which they have not been given proper authorization. All visitors to sensitive areas of our office must have a valid reason for access, and be met by the appropriate workforce member prior to gaining access.

**Procedures:** A workforce member’s access to information is specifically aligned with his or her role or function in the organization. These functional or role-based access control and validation procedures are closely aligned with the facility security plan. Our procedures are the means to actually determine the workforce members or persons that should have access to certain locations within the facility based on their role or function.

**Details:** The access control and validation procedures include but are not limited to:

* Physical access by a workforce member or other authorized personnel to the facility is gained by using a physical key or entering the building once the entry door has been unlocked during business hours.
* Visual recognition is used to distinguish authorized from unauthorized people. Keycards and employee badges may also be used to supplement visual recognition.
* All visitors must be check-in at the reception area. Visitors shall be escorted in areas containing access to ePHI if there is a reason for visitors to be in such areas. Visitor sign-in sheets and badges may also be used to control and validate access.
* Workforce members are trained to challenge any individual within our facilities who is not recognized, unsupervised or without proper authorization.
* Security access violations will be investigated by 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 |  |  |  |