**POLICY & PROCEDURES**

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

### **Automatic Logoff §164.312(a)(2)(iii)**

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

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

**Policy:** Our workforce members must end electronic sessions on information systems that contain or can access ePHI when such sessions are completed, unless the information system is secured by an appropriate locking method (e.g. by pressing the “Windows logo” key + “L” key). 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) when their workday ends.

**Procedures:** Our workforce members must activate their workstation locking software whenever they leave their workstation unattended for 10 minutes or more. Exceptions to our information system required inactivity timeout must be approved by our Security Official. Our workforce members must log off from or lock their workstation(s) when their workday ends.

**Details:** The automatic logoff procedures on information systems that contain or can access ePHI include but are not limited to:

* All workstations shall be configured to have a password-enabled screen saver.
* Workforce members will activate their workstation locking method (e.g. by pressing the “Windows logo”  key + “L” key) whenever they leave their workstation unattended for 10 minutes or more.
* After a predefined time period (e.g. 10 minutes) of inactivity, the password-enabled screen saver will lock the workstation and make information inaccessible. Workstations in high-traffic patient/visitor areas may have a timeout of 2 to 3 minutes while computers in protected areas with controlled, limited access, such as a lab or administrative office, could have longer timeout periods.
* Workforce members must log off or lock their workstation when their workday ends.
* Exceptions to our information system required inactivity timeout must be approved by our 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 |  |  |  |