**POLICY & PROCEDURES**

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

### **Person or Entity Authentication §164.312(d)**

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

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

**Policy:** We must create and implement a process for verifying the identity of a person or entity before granting them access to ePHI. All authentication data, such as passwords and PINs, must be protected with appropriate access controls to prevent unauthorized access. Our workforce members must not share or reveal their authentication methods to others. Any workforce member, who believes that their authentication method is being inappropriately used, must immediately notify our Security Official.

**Procedures:** Our Security Official will implement a process for the verifying of the identity of a person before they are able to gain access to ePHI. Each workforce member will have their own individual method for authenticating their identity. Our workforce member will not share or reveal their authentication method with others or ask another to share or reveal their authentication method. Unsuccessful authentication attempts to our information systems are limited.

**Details:** The person or entity authentication procedures include but are not limited to:

* All authentication methods will be approved by Security Official.
* Prior to being granted access to information systems containing or accessing ePHI, workforce members will complete the both Workforce Clearance and Access Authorization procedures.
* Workforce members are granted a unique user identification and a password that can be modified by the user.
* Information systems validate authentication attempts. Unsuccessful authentication attempts are limited.
* Information system review procedures are in place for detecting and responding to unusual or suspicious authentication activity.
* Workforce members must not share or reveal their authentication methods to others.
* A workforce member who believes that his/her authentication method is being used inappropriately or has lost a physical access method (e.g. key card or security token) must immediately notify his or her supervisor.
* 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 |  |  |  |