**POLICY & PROCEDURES**

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

### **Mechanism to Authenticate Electronic Protected Health Information §164.312(c)(2)**

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

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

**Policy:** We must implement appropriate electronic mechanisms to confirm that ePHI contained on our information systems has not been altered or destroyed in an unauthorized manner. Protecting the integrity of ePHI is a primary goal of the Security Rule.

**Procedures:** Electronic mechanisms used to protect the integrity of ePHI contained on our information systems ensure that the value and state of the ePHI is maintained and it is protected from unauthorized modification and destruction. These mechanisms are capable of detecting and reporting unauthorized alteration or be capable of detecting and reporting unauthorized alteration or destruction of ePHI.

**Details:** The mechanism to authenticate electronic protected health information procedures include but are not limited to:

* The Security Official is responsible for identifying risks to the integrity of the ePHI data and the security measures that will reduce those risks.
* Security risk assessments are conducted on a periodic basis to assess the risks to the integrity of the ePHI data.
* Risk management plans are developed and implemented to mitigate the risks identified in the security risk assessment report.
* Security measures put in place to reduce risks that may compromise the integrity of ePHI data include:
* Implementing software to protect against malicious software
* Using unique user identifications and password authentication
* Updating software with security patches
* Workforce awareness and security training
* Periodic security reminders
* Using workforce confidentiality agreements
* Using Business Associate contracts
* Physical facility access controls and security mechanisms
* Verifying backups complete successfully
* Maintaining a backup copy of ePHI data offsite.
* Using data in transit and data at rest encryption mechanisms
* Reviewing audit logs
* Implementing systems with built-in safeguards that protect the integrity of ePHI from being altered or destroyed in an unauthorized manner.
* Documentation (e.g. policies and procedures, training) 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 |  |  |  |