**POLICY & PROCEDURES**

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

### **Encryption and Decryption §164.312(a)(2)(iv)**

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

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

**Policy:** Appropriate encryption must be used to protect the confidentiality, integrity, and availability of ePHI contained on our information systems. Encryption is a method of converting an original message of regular text into encoded text. Our Security Official will determine when encryption is a reasonable and appropriate safeguard to implement with our information systems.

**Procedures:** We are responsible for identifying all workstations and devices that store ePHI. Portable workstations and devices workstations and devices that leave our facility will be encrypted unless the Security Official grants an exception. Non-portable workstations and devices will be encrypted or protected by alternative safeguards. No workforce member will implement encryption of data without the knowledge and approval of our Security Official. We will maintain documentation regarding the encryption methods utilized.

**Details:** The encryption and decryption procedures include but are not limited to:

* The Security Official is responsible for identifying all the types of workstations (e.g. a desktop, laptop, smart phone, tablet), or removable storage devices (e.g. USB flash drive, external hard drive) that are used to store ePHI.
* At a minimum, encryption will be used to protect ePHI stored on portable workstations and devices. In the event a portable workstation or device is not protected with an encryption mechanism, it may be:
* Prevented from storing ePHI
* Retired in a timely manner and replaced by a device that supports an encryption mechanism
* Approved by the Security Official as an exception.
* Non-portable workstation and devices storing ePHI will be protected by encryption or other alternative safeguards such as: physical facility controls, firewalls, system level access controls and software application user ID and password access controls that authenticate the identity of those individuals accessing the data.
* All encryption methods will be approved by the Security Official.
* Cryptographic keys will be protected against modification, destruction and unauthorized disclosure.
* 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 |  |  |  |