**POLICY & PROCEDURES**

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

### **Disaster Recovery Plan §164.308(a)(7)(ii)(B)**

**Contingency Operations §164.310(a)(2)(i)**

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

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

**Policy:** We must create and document a disaster recovery plan to recover our information systems if they are impacted by a disaster. The plan must be reviewed annually and revised as necessary. We must ensure that, in the event of a disaster or emergency, authorized personnel can enter our office to maintain physical security and appropriate access to ePHI while allowing for data restoration activities.

**Procedures:** Our Security Official along with authorized personnel (i.e. Contingency Team) are responsible for restoring any loss of ePHI due to natural or man-made disaster. The Contingency Team will coordinate the recovery efforts to restore business operations. The Security Official will notify the workforce members when our services resume.

**Details:** The disaster recovery plan and contingency operations procedures include but are not limited to:

* In the event of a disaster, the Security Official along with authorized personnel (i.e. Contingency Team) are responsible for the data recovery process.
* The Contingency Team will determine the extent of the disaster in collaboration with any applicable IT vendor(s) and collectively decide if a facility shutdown is necessary.
* The Contingency Team will determine if workforce members should temporarily relocate to an alternative location site to continue normal business functions or stay at home.
* The Security Official will authorize workspace, computers, and supplies and coordinate travel arrangements, food, and accommodations for individuals supporting the temporary backup effort, as necessary.
* In the event of lost ePHI data and programs the information will be restored from our most recent backup media (onsite or off-site). Our IT vendor(s) will coordinate the restoration process per our service agreement contract.
* The Contingency Team will determine when our facility is safe and ready to resume daily business operations. The Security Official will notify the workforce members.
* Appropriate workforce members will be trained in the disaster recovery plan and will be authorized to access the facility to restore business operations.
* Documentation (e.g. IT vendor service agreement contracts, 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 |  |  |  |