**POLICY & PROCEDURES**

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

### **Risk Management §164.308(a)(1)(ii)(B)**

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

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

**Policy:** Upon completing a risk analysis, risk management is the process we use to implement security measures that reduce the identified risks to our information systems containing ePHI to a reasonable and appropriate level based on our circumstances.

**Procedures:** We select and implement security measures based on our risk analysis process in order to protect our information systems, equipment and data from any natural or other type of threat. This process involves developing a remediation plan, implementing corrective actions for any compliance gaps that were identified and tracking progress against those items year to year.

**Details:** The risk management procedures include but are not limited to:

* Determine a course of action to take for each identified gap.
* Involve key members, including senior management and other key decision makers, to make risk prioritization and mitigation decisions.
* Develop a risk management plan and begin the remediation process.
* Implement both technical and non-technical security measures as appropriate.
* Evaluate and monitor the risk mitigation measures implemented periodically to review the progress or lack thereof being made to remediate the security risk analysis report findings.
* Retain documentation (e.g. remediation project plans) of the practices in place 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 |  |  |  |