**POLICY & PROCEDURES**

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

### **Risk Analysis §164.308(a)(1)(ii)(A)**

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

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

**Policy:** Risk Analysis is often regarded as the first step towards compliance with the HIPAA Security Rule. We must regularly identify, define, document and prioritize risks to the confidentiality, integrity and availability of our information systems containing ePHI.

**Procedures:** We conduct a risk analysis of our information systems as required by HIPAA (i.e. each year prior to Meaningful Use attestation, if applicable or every two years) or whenever there has been a significant change in our environment. The assessment process involves identifying and examining each information system in our office for threats and vulnerabilities that could cause harm to our equipment and data. The resulting analysis of these risks are prioritized and documented in a risk assessment report.

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

* Identify the systems that store, process, or transmit ePHI.
* Identify components of systems or applications that handle ePHI.
* Document the physical location (i.e. inventory) of IT assets that contain ePHI.
* Identify the criticality of the system and its data.
* Identify threats to the system.
* Identify vulnerabilities on the system.
* Analyze the controls that have been implemented, or are planned for implementation.
* Identify the probability that a vulnerability may be exploited.
* Identify the impact of a successful threat exercise.
* Assess the level of risk.
* Identify additional controls to mitigate identified risks.
* Document the results of the risk assessment.
* Retain documentation (e.g. risk assessment report) 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 |  |  |  |