**POLICY & PROCEDURES**

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

### **Evaluation §164.308(a)(8)**

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

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

**Policy:** We must conduct technical and non-technical evaluations of our security controls and processes. The purpose of the evaluation is to establish a process to review and maintain reasonable and appropriate security measures.

**Procedures:** Our Security Official will direct both the non-technical evaluation of policies and procedures documentation and the technical evaluation of our information systems on a periodic basis. Revisions to security measures will be made, as necessary, to address issues or gaps identified by the evaluation processes. We will ensure the results of such evaluations are documented.

**Details:** The evaluation procedures include but are not limited to:

* Conduct a non-technical review of existing policies and procedures documentation to:
* Determine whether the organization has written policies and procedures that demonstrate compliance for all the Security Rule standards and implementation specifications
* Assess whether the written procedures are being actively used, applied, and enforced.
* Determine whether the practices and enforcement of same, represent reasonable and appropriate safeguards to comply with the standards and implementation specifications.
* Conduct a technical review of information systems to ensure that hardware and software controls have been correctly implemented. This process may include conducting:
* External and internal vulnerability scans
* External and internal penetration tests
* Web application security scans
* Wireless security scans
* Social engineering testing
* ePHI data discovery scans.
* Revise security measures as necessary to remediate known gaps.
* Retain documentation (e.g. evaluation findings, remediation options, recommendations, and remediation decisions) 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 |  |  |  |