**POLICY & PROCEDURES**

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

### **Assigned Security Official §164.308(a)(2)**

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

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

**Policy:** Our assigned HIPAA Security Official, [add name here], is operationally responsible for assuring that the organization complies with the HIPAA Security Rule. This rule requires the responsibility for security be assigned to a specific individual or group to provide an organizational focus and importance to security.

**Procedures:** Our security official is responsible for the development and implementation of all policies and procedures necessary to appropriately protect the confidentiality, integrity and availability of our information systems and ePHI. Responsibilities include the management and supervision of the security measures we use to protect data, and the conduct of personnel in relation to the protection of data.

**Details:** Responsibilities of the assigned security official include but are not limited to:

* Ensure that information systems comply with all applicable federal, state, and local laws and regulations.
* Ensure that no information system compromises the confidentiality, integrity, or availability of any other information system.
* Develop, document, and ensure dissemination of appropriate security policies, procedures, and standards for the users and administrators of information systems.
* Ensure that newly acquired information systems have features that support required and/or addressable security Implementation Specifications.
* Coordinate the selection, implementation, and administration of significant security controls.
* Ensure workforce members receive regular security awareness and training.
* Conduct periodic risk analysis of information systems and security processes.
* Develop and implementing an effective risk management program.
* Regularly monitoring and evaluating threats and risks to information systems.
* Monitor auditing records to identify inappropriate activity.
* Maintain an inventory of all information systems that contain ePHI.
* Create an effective security incident response policy and related procedures.
* Ensure adequate physical security controls exist to protect ePHI.
* Coordinate with the Privacy Official to ensure that security policies, procedures and controls support compliance with the HIPAA Privacy Rule.
* Evaluate new security technologies that may be appropriate for protecting information systems.
* Review the HIPAA Security policies and procedures documentation and update on an annual basis.
* Ensure that the access control, disaster recovery, business continuity, incident response, and risk management needs of the organization are properly addressed.
* Work with vendors, outside consultants, and other third parties, to reduce security risks and vulnerabilities within the organization.
* Communicate the Security Official's role and responsibility throughout the organization.
* Retain documentation (e.g. training materials, job description) 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 |  |  |  |