Data Security Policy – Policy and Procedure Management

PURPOSE

To provide principles and guidelines for managing policies, procedures, and other documentation at Organization.

SCOPE

The Policy and Procedure Management document will cover Organization's:

- Policy and procedure review
- Compliance documentation, access, and retention
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY/PROCEDURES

Organization's Security Officer is responsible for implementing policies and procedures that meet the requirements of the HIPAA Security Rule.

All policies and procedures related to the HIPAA Security Rule and other regulatory and compliance standards followed by the company are written and retained, usually in electronic form. Related documentation is also created and retained for security measures and control activities.

Documentation is retained for a minimum of six (6) years from the time of its creation or the date it was last in effect, whichever is later.

Access to security and compliance documentation other than policies and procedures is limited only to those people who require access for their job functions and/or roles.

Policies and procedures, as well as other key documents, are reviewed at least annually and updated as needed. Reviews of policies and procedures must include the date of review, and the signoff of the reviewer.

ROLES AND RESPONSIBILITIES

Security Official: Responsible for adopting policies and procedures that meet the requirements of the HIPAA Security Rule for the company.

Policy Owner or Reviewer: Responsible for reviewing and updating policies and/or procedures that fall under their jurisdiction.

RELEVANT HIPAA REGULATIONS

- §164.316(a) Policies *and procedures*
- §164.316(b)(1) *Documentation*
- §164.316(b)(2)(i)*Time limit*
- §164.316(b)(2)(ii) *Availability*
- §164.316(b)(2)(iii) *Updates*

RELEVANT SOC 2 CRITERIA

- CC5.3.2 *Establishes responsibility and accountability for executing policies and procedures*