Data Security Policy – Monitoring and Effectiveness

PURPOSE

To provide principles and guidelines for performing regular security assessments and monitoring of Organization's data security program. To provide detailed instructions for conducting regular security assessments and monitoring of Organization's data security program.

SCOPE

The Monitoring and Effectiveness Policy and Procedures will cover Organization's:

- Security assessments and process, including
- Technical and non-technical assessments
- Remediation
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization conducts regular security assessments to evaluate the effectiveness of our data security program. These security assessments will also be performed in the event of a major change.

Assessments can be performed by both internal and external parties.

Assessment reports are communicated to company leadership and the Board of Directors.

Technical and Non-Technical Assessments

Organization uses a mix of technical and non-technical assessments to monitor the effectiveness of our data security program. Assessments may include penetration testing, risk assessments and audits and can include use of the Guard's Data Security Program.

Remediation

Any findings resulting from security assessments will be documented and tracked in a risk register. The Guard's data security program can be used to accomplish this. We develop action plans to address these issues, and track remediation to completion.

PROCEDURES

Organization conducts security assessments **annually** and uses a mix of technical and non-technical measures to evaluate the effectiveness of our data security program. Additional assessments are performed when major changes occur that call for a formal security assessment.

Organization works with its internal teams and third parties to conduct security assessments. Any third parties that are contracted to perform security assessments must meet our due diligence and third-party risk requirements. We may use the Data Security and Physical Safeguards Programs in The Guard to accomplish this.

The results from security assessments are documents and communicated to company leadership, including the Board of Directors when appropriate.

Technical and Non-Technical Assessments

Organization performs penetration testing or an equivalent technical assessment on an annual basis to evaluate our data security program. Technical assessments should cover:

- ePHI and other sensitive information security and controls
- Key information systems
- Security configurations
- Infrastructure security
- Network security
- Application security
- Workstation/Endpoint security
- Identification of new or emerging technology risks

Non-technical assessments should evaluate:

- The overall information security program and controls, including:
    - Access controls
    - Audit controls
    - Integrity controls
    - Identity and authentication controls
    - Incident response controls
    - Contingency planning controls
- The effectiveness of controls to mitigate risks
- Identification of new or emerging business risks
- Facility and physical security controls

All assessments are documented. New risks are logged in our risk register. The Guard's program module can be used to accomplish this for the non-technical assessments and as an evidence collection tool for the technical assessments.

Remediation

Any findings, observations, or issues discovered over the course of a security assessment should be logged in our risk register. Organization will update its security measures to remediate issues identified during an assessment. These updates will be reflected in updated policies and procedures. Remediation efforts should reduce the likelihood or impact of an identified risk to an acceptable level.

Remediation will be tracked to completion. This can be accomplished by adding, tracking and completing tasks attached to the relevant controls in the Guard's Data Security and Physical Safeguard Programs.

ROLES AND RESPONSIBILITIES

Security Assessor(s): Conducts technical and non-technical security assessments. Records risks, observations, and findings and reports them to management. Provides remediation recommendations.

FORMS/PLANS/DOCUMENTS

- Security Assessment Report(s)
- Risk Register

RELEVANT HIPAA REGULATIONS

- § 164.308(a)(8) *Perform a periodic technical and non-technical evaluation.*

RELEVANT SOC 2 CRITERIA

- CC 2.3.3 *Communicates With the Board of Directors*
- CC 3.4.4 *Assess Changes in Systems and Technology*
- CC 4.1.1 *Considers a Mix of Ongoing and Separate Evaluations*
- CC 4.1.2 *Considers Rate of Change*
- CC 4.1.3 *Establishes Baseline Understanding*
- CC 4.1.4 *Uses Knowledgeable Personnel*
- CC 4.1.5 *Integrates With Business Processes*
- CC 4.1.6 *Adjusts Scope and Frequency*
- CC 4.1.7 *Objectively Evaluates*
- CC 4.1.8 *Considers Different Types of Ongoing and Separate Evaluations*
- CC 4.2.1 *Assesses Results*
- CC 4.2.2 *Communicates Deficiencies*
- CC 4.2.3 *Monitors Corrective Action*