Data Security Policy – Integrity Control

PURPOSE

To provide principles and guidelines for information and system integrity control.

SCOPE

The Integrity Control Policy will cover Organization's:

- Data, information, and system integrity controls
- Detection of unauthorized changes or destruction of data
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has adopted and follows processes to safeguard the integrity of sensitive and protected information, such as ePHI. These security measures are designed to protect information and systems from unauthorized modification, deletion, or access.

Organization has set up processes for detecting unauthorized changes or destruction of information and data. These processes may include mechanisms for validating the integrity of data. If an anomaly or event is detected, workforce members should report the event. Detection mechanisms are periodically reviewed and tuned to optimize operations.

PROCEDURES

Organization has set up processes to safeguard the integrity of sensitive and protected information, including ePHI.

Data, Information, and System Integrity Controls

In order to maintain the integrity of the company's production environment, Organization has set up separate production, development, and test environments. Only tested and approved components, infrastructure, and information is migrated or released into production. By separating environments, Organization can better ensure that only thoroughly validated systems, components, and data appear in production. To further safeguard sensitive and protected information, only "dummy data" or non-production data will be used in development and test environments.

Organization has set up strong encryption and cryptographic security on sensitive and protected information, including *ePHI*, at-rest and in-transit. The company uses modern, secure algorithms to encrypt sensitive or protected data.

Detection of Unauthorized Changes or Destruction of Data

Organization uses a combination of electronic authentication, procedural authentication, and data and system integrity checks to detect and protect *ePHI* from unauthorized changes, destruction, or disclosure.

Workforce members are trained and encouraged to report any suspected unauthorized access, changes, deletion, or disclosure of sensitive or protected information, including *ePHI*.

Organization has set up automated alerting mechanisms and filters to analyze anomalies and alert on potential threats to data or system integrity. These alerts are routed through the company's incident response and reporting procedure.

Definitions

Electronic Authentication - Mechanisms such as error-correcting memory, digital signatures, and checksum technology used to check data or system integrity.

Procedural Authentication - Mechanisms such as manual validation used to check data or system integrity.

Data and System Integrity Checks - Mechanisms and procedures (e.g., backup verification, hardware and software reviews) to perform periodic checks of data and system functionality to identify *integrity* issues (e.g., corrupted data, failing hardware, software errors).

RELEVANT HIPAA REGULATIONS

- 164.312(c) *Mechanism to Authenticate Electronic Protected Health Information*

RELEVANT SOC 2 CRITERIA

- CC6.8.2 *Detects unauthorized changes to software and configuration parameters*
- CC7.2.1 *Implements detection policies, procedures, and tools*
- CC7.2.2 *Designs detection measures*
- CC7.2.3 *Implements filters to analyze anomalies*
- CC7.2.4 *Monitors detection tools for effective operation*
- CC7.3.2 *Communicates and reviews detected security events*