Data Security Policy – Audit Control

PURPOSE

To provide principles and guidelines for creating, managing, reviewing, and retaining audit trails and audit logs.

SCOPE

The Audit Control Policy will cover Organization's:

- Audit log management
- Audit log review(s)
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has set up auditing, logging, and monitoring mechanisms on assets that contain or process sensitive or protected information, such as ePHI. Audit logs provide date and time-stamped entries that capture details about the activities performed on that asset, and the users who accessed the asset.

Audit logs can be set up for many different types of assets, to monitor everything from system performance to user activity.

Audit Log Management

Organization decides which assets to collect audit logs from based on criticality to the company and whether the asset contains sensitive or protected information, such as ePHI. Any systems that contain sensitive or protected information or are critical to the operation of the company must have audit logging enabled.

Organization considers asset performance, user activity, and other factors when deciding what to log on which systems.

Audit logs are retained based on regulatory and operational requirements.

Access to audit logs is restricted to appropriate workforce members and audit logs cannot be altered without tracking and approval.

Audit Log Reviews

Organization has adopted and follows a process for reviewing audit logs for security incidents. If any incidents are detected or suspected as part of the review process, they are reported through the incident response and reporting process.

Audit logs may also be reviewed to investigate detected incidents and can provide valuable insight into the security of the company's information assets.

PROCEDURES

Organization has set up processes to log and review access and activities performed on information systems that contain sensitive or protected information, including ePHI. The company has set up audit logging over:

- The network, including any vulnerabilities and unauthorized access
- Systems or assets containing sensitive or protected information, including ePHI
- System performance
- Changes to sensitive or protected data, including ePHI
- Applications and software

Audit Log Management

Audit logs should be configured to include, at minimum:

- The data and time of access or activity
- The origin of access or activity
- The identity of the user performing the access to activity
- A description of the access or activity

Access to modify audit logs is restricted to appropriate workforce members only.

Audit logs are retained for compliance purposes, and to complete incident investigation and response. Logs should be retained for a minimum of six (6) years. Network device and systems logs can be retained for a minimum of one (1) year if retention costs are prohibitive.

Audit logs will be stored securely and encrypted where applicable.

Audit Log Reviews

Audit logs are reviewed at least quarterly for all systems that contain or process sensitive or protected information, including ePHI. Reviewers must be competent and capable of performing the review based on their job function(s) or role(s) and must document their reviews through the company's ticketing system or other similar tool. Reviews must be completed in a timely manner.

Any changes or further action resulting from audit log reviews should be recorded as part of the review and have a ticket submitted through the incident response and reporting process.

If criminal activity is detected as part of audit log reviews, appropriate action should be taken, including contacting law enforcement.

ROLES AND RESPONSIBILITIES

Audit Log Reviewer: Reviews audit logs and reports incidents. Generates audit logs for compliance and operational purposes as needed.

RELATED POLICIES & PROCEDURES

- *Data Security Policy – Incident Response and Reporting*

RELEVANT HIPAA REGULATIONS

- §164.312(b) *Audit controls*

RELEVANT SOC 2 CRITERIA

- CC7.1.2 *Monitors infrastructure and software*
- CC7.1.3 *Implements change-detection mechanism**s*
- CC7.1.4 *Detects unknown or unauthorized components*
- 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*
- CC7.4.7 *Obtains understanding of nature of incident and determines containment strategy*