Data Security Policy - Workforce Security

PURPOSE

To provide principles and guidelines for managing the workforce and workforce security.

SCOPE

The Workforce Security Policy and Procedure will cover Organization's**:**

- Workforce security
- Job descriptions
- Workforce background checks or screenings
- Confidentiality agreements
- Development and performance reviews
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has adopted and follows processes to enforce workforce security and workforce management controls. The company restricts access to sensitive and protected information, including ePHI, to appropriate and authorized members of the workforce only. When necessary, Organization sets up controls to separate incompatible duties and responsibilities.

The company has set up workflows to supervise the approval of access to sensitive and protected information and assets.

Organization aims to foster a security-conscious workforce and culture and seeks to hire, develop, and maintain skilled workforce members.

Job or Role Descriptions

To attract and hire skilled talent, Organization requires written and defined job or role descriptions for each position at the company, and for recruitment. Job descriptions should be periodically reviewed and updated when necessary.

Workforce Background Checks and Security Screenings

As part of the recruitment process, the company has adopted and follows a defined screening process, incorporating interviews, case studies, or technical examinations when appropriate for the job or role.

Organization requires a background check to be performed when possible prior to hiring an employee. If a background check is not possible due to privacy laws, the company will use a different screening method.

Development and Performance Reviews

Developing the workforce is key to Organization's success. Organization provides basic security training for all employees and provides role- or job-specific training as needed.

The company provides resources for employees' development and completes a regular performance review for all employees. Performance reviews should be documented and follow a defined process.

Confidentiality Agreements

Prior to beginning work, workforce members must sign Organization's Confidentiality Agreement. While not required for HIPAA compliance, it is a best practice.

PROCEDURES

Job Or Role Descriptions

Whenever a new role or job is opened, a formal job description is created and maintained. Job descriptions should be reviewed at least annually and updated if necessary.

Workforce Background Checks and Security Screenings

Organization uses various screening mechanisms, such as interviews, case studies, or technical examinations to evaluate applicants for a job function or role. All new hires must have a background check completed prior to onboarding. If a background check is not permitted due to regional laws or mandates, the company will use a combination of background screening methods, such as references and work experience.

Screening records and background check documentation is retained for compliance purposes. The company may redact information on screening records and background check documentation when appropriate.

Development and Performance Reviews

To attract, retain, and develop workforce members, Organization requires all employees to undergo basic security training that covers proper handling and protection of PHI and *ePHI*. The company provides role- and job-specific training to employees and workforce members as needed.

At least annually, Organization completes a performance review for all employees. Performance reviews should be documented and retained, including information about the individuals involved in the review, the date the review was performed, and any action items or outcomes resulting from the review. These performance reviews will be kept as part of workforce records.

Confidentiality Agreements

Organization requires all workforce members, including contractors, to sign a Confidentiality Agreement. These Confidentiality Agreements are retained as part of workforce records. This can be accomplished using the Guard's Vendor module or by other similar means.

ROLES AND RESPONSIBILITIES

Security Official: Accountable for workforce security and workforce access to sensitive and protected information, including *ePHI.* Delegates responsibilities and authority as needed. Informs workforce members of changes to access levels or clearance or delegates these communications.

Access Approval: Delegates with appropriate levels of knowledge and experience may have access approval authority for certain roles, information, assets, and/or systems. Access requests that require approval may be routed to one or more supervisory approvers.

VIOLATIONS

Access to information or assets may be revoked or suspended if a workforce member has accessed sensitive or protected information without the right level of authorization and approval.

FORMS/PLANS/DOCUMENTS

- Confidentiality Agreement (Samples available in the Guard Document Module)
- Offboarding Checklist

RELATED POLICY

- Data Security Policy - Access Control

RELEVANT HIPAA REGULATIONS

- §164.308(a)(3)(i) *Workforce security*
- §164.308(a)(3)(ii)(A) *Authorization and/or supervision*
- §164.308(a)(3)(ii)(B) *Workforce clearance procedure*
- §164.308(a)(3)(ii)(C) *Termination procedures*

RELEVANT SOC 2 CRITERIA

- CC5.2.3 *Establishes relevant technology infrastructure control activities*
- CC6.1.2 *Restricts logical access*
- CC6.1.6 *Restricts access to information assets*
- CC6.2.1 *Controls access credentials to protected assets*
- CC6.2.3 *Reviews appropriateness of access credentials*
- CC6.3.3 *Uses role-based access controls*
- CC6.1.8 *Manages credentials for infrastructure and software*