Data Security Policy - Information Access Management

PURPOSE

To provide principles and guidelines for information access management at Organization, including access to ePHI.

SCOPE

The Information Access Management Policy will cover Organization's**:**

- Information access management, including sensitive and protected information, such as ePHI
- Identity, roles, and authorization of user access to sensitive and protected information, such as ePHI
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY/PROCEDURES

Organization has and follows policies and procedures for managing access to information, including sensitive and protected information, like ePHI*.* Physical access to sensitive or protected information is also considered. The company considers access in the context of regulatory and compliance obligations, such as the HIPAA Security Rule.

Organization applies principles of "least privilege" and role-based access control throughout its operations and restricts access to sensitive and protected information and systems on a need-to-access basis. Access to systems and data is tied to users' identities.

Organization has set up systems and processes to record access requests, approvals, provisioning, modification, and termination. These Access Controls are captured in our *Access Control Policy.*

Access Reviews

Organization reviews access on a regular basis, including access to ePHI and other sensitive data. If changes are required based on the access review, they are carried out in a timely manner.

ROLES AND RESPONSIBILITIES

Security Official: Accountable for user access to ePHI and other protected data*.*

VIOLATIONS

Inappropriately accessing sensitive or protected data may result in disciplinary action, in compliance with the HIPAA Security Rule.

FORMS/PLANS/DOCUMENTS

- Onboarding Checklist
- Offboarding Checklist
- Access Reviews
- User Access Listing or Population

RELATED POLICIES AND PROCEDURES

- Data Security – Access Control Policy

RELEVANT HIPAA REGULATIONS

- §164.308(a)(4)(i) *Information Access management*
- §164.308(a)(4)(ii)(B) *Access authorization*
- §164.308(a)(4)(ii)(C) *Access establishment and modification*

RELEVANT SOC 2 CRITERIA

- CC5.2.3 *Establishes relevant technology infrastructure control activities*
- CC6.2.1 *Controls access credentials to protected assets*
- CC6.2.2 *Removes access to protected assets when appropriate*
- CC6.2.3 *Reviews appropriateness of access credentials*
- CC6.3.1*Creates or modifies access to protected information assets*
- CC6.3.2 *Removes access to protected information assets*
- CC6.3.3 *Uses role-based access controls*