Data Security Policy - Access Control

PURPOSE

To provide principles and guidelines for access control activities at Organization**.**

SCOPE

The Access Control Policy will cover Organization's**:**

- User Identification and Unique IDs
- Access Management, including provisioning, modification, and termination
- Emergency Access
- Access Reviews
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has adopted and follows processes for managing access to data and systems. Only authorized and appropriate workforce members have access to sensitive or protected information (including *ePHI*) and systems. The company aims to protect the confidentiality, integrity, and availability of sensitive and protected data, and has set up safeguards to restrict access to systems and assets.

Organization has set up role-based access control (RBAC) to limit access to only those workforce members who need it to complete their job function(s). Wherever possible, the company has employed the principle of "least privilege," reducing access to the minimum necessary.

Access to *ePHI* and other protected information is approved and granted only to those workforce members who require access to complete their job function(s) or role(s). Users who do not need access to *ePHI* are not given access.

Organization separates incompatible duties between one or more different workforce members.

User Identification and Unique IDs

Organization ties users' identities to their unique IDs at the company. Workforce members must use their unique IDs or user accounts to conduct their daily job functions. Unique IDs are used to tie user activities and access logs back to individuals and are important for maintaining quality audit trails.

Access Management

Organization has set up processes to facilitate access requests, access grants or provisioning, access modification, and access termination. Access to sensitive or protected information and assets must be approved by an appropriate supervisor.

Organization has set up a mechanism for users to request additional access rights. These requests are formally documented through a ticketing system or similar repository.

Access Provisioning

Organization has set up a process to grant or provision access only when access is approved and appropriate. Users should only be given access to information or systems that they need to complete their job function(s).

Access provisioning activities are documented and captured through a ticketing system or similar repository.

Access Modification

Organization has set up a process to request and complete modifications to a user's access, either due to a role change, or other business reasons.

Access modification activities are documented and captured through a ticketing system or similar repository.

Access Termination

Organization has set up a process to remove, revoke, or terminate user access to information and systems upon the workforce member's termination, or other business reasons. Access termination is performed timely to prevent unauthorized access to sensitive and protected information.

Access termination activities are documented and captured through a ticketing system or similar repository.

Emergency Access

In the event that emergency access is required, and an appropriate approver is not immediately available, emergency access and subsequent activities performed with that access may be approved after the fact.

Cases of emergency access must be formally requested and documented through a ticketing system or similar repository.

Any emergency access activities will be reviewed by an appropriate workforce member.

Access Reviews

Organization performs periodic access reviews over users' access to information and systems. If any actions, such are modifying or terminating access, are necessary following the review, they are carried out in a timely manner. User access reviewers must have the appropriate credentials and knowledge to complete the review.

Documentation of user access reviews and reviewer signoff is retained.

PROCEDURES

Organization has set up various processes for managing users' access, identifies, and authentication. Prior to receiving access to sensitive or protected information or systems, workforce members undergo a thorough screening process to verify their identities and skills.

Organization provides access to workforce members on the basis of their job function(s) or roles, and restricts access to sensitive or protected information through the access controls and processes described below.

User Identification and Unique IDs

Organization keeps an up-to-date, complete, and accurate listing of all users, accounts, and identities of workforce members at the company. As needed, each system owner should be able to generate a complete list of users with access to systems in their jurisdiction and their roles or access permissions. These listings will be used to manage and review user access across the organization.

The company uses a Single-Sign On solution that enables users to access multiple applications or systems using one set of secure credentials when feasible.

Password or Passkey Management

Whenever users are required to make a new password as part of their job duties or role, they must meet the following standards:

- Use a minimum of eight (8) characters, with longer passwords being more secure
- Disallow or do not use sequences or repetitive characters, such as “12345” or “aaaaa”
- Disallow or do not use context-specific passwords, like the name of the site or company
- Disallow or do not use commonly used passwords, such as “password123” and “12345678”
- Disallow or do not use single dictionary words
- Disallow or do not use passwords that have been compromised previously

The company provides workforce members with annual security training that provides instruction and guidelines for creating strong passwords.

Multi-Factor Authentication (MFA)

When possible, Organization enforces multi-factor authentication requirements for users and systems. Multi-factor authentication or MFA requires a user to have a second factor, like a phone or security token, to log in to their account(s). Adding another factor to authentication and log in makes it more difficult for accounts to be compromised through password attacks alone.

Any systems that house sensitive or protected information, including *ePHI*, must have MFA enforced for all users. If MFA cannot be enforced due to technical limitations or other business reasons, these exceptions should be documented and added to the company’s *Risk Register.*

Remote users must use MFA when accessing sensitive or protected information or assets.

Access Management

All systems that contain or process sensitive or protected information, including *ePHI*, must incorporate access controls that govern the provisioning, modification, and termination of user access.

Any systems that have built-in or default accounts must have those accounts either disabled or credentials and passwords changed to restrict and monitor access. Workforce members are discouraged from using group accounts or system accounts whenever possible and should only perform work activities through their own accounts. Workforce members are not permitted to share accounts or credentials.

All access control activities are captured and documented in Organization’s ticketing system or similar repository.

When possible, Organization has automated access control workflows to route tasks and requests to appropriate workforce members, such as approvers and system owners.

Access Provisioning

All access to sensitive or protected information or systems must be formally requested, documented, and approved prior to granting access. These access granting or provisioning activities are captured in a new hire *Onboarding Checklist* or *Access Request*.

Access requests include:

- Name and user ID of the user creating the access request
- Name and user ID of the user who access is being requested for
- Description of the access request, including systems, roles, or permissions
- Justification for the access request

The system owner receives and reviews the access requests for their system(s). If the access request is appropriate, the request is routed to the authorized approver, and the request is approved.

Access is granted or provisioned as described in the approved access request.

If the access request is not approved, access will not be granted.

Access Modification

If a user's access needs to be modified or changed for any reason, such as a role change or a reorganization, an access request must be submitted to document the modification.

The system owner receives and reviews the access modification requests for their system(s). If the access request is appropriate, the access request is routed to the authorized approver, and the request is approved.

Access is modified as described in the approved access request.

If the access request is not approved, access will not be modified.

Access Termination

Organization has set up a process to automatically terminate user access throughout the organization once notification or termination or access removal has been received. All access held by the terminated user to the company's systems and assets is promptly terminated, removed, revoked, or disabled, no later than 24 hours from notification.

Termination requests and control activities are captured in the company's *Offboarding Checklist* and ticketing system or similar repository. Documentation should include the reason for the access change, such as a termination of employment or role change.

Emergency Access

Organization has set up a process to grant emergency access permissions to workforce members during an emergency situation or major incident. Emergency access requests must be formally documented and submitted through the ticketing system. Emergency access may be granted without approval if the justification and severity of the incident is sufficient.

All activities performed with emergency access are logged and monitored. Emergency access logs are reviewed no later than 10 business days after the incident, and any unauthorized activities or actions are investigated and remediated as needed.

Emergency access requests must be approved by an appropriate workforce member within 48 hours.

Emergency access is removed or revoked once the access is no longer needed, or the situation has been resolved, and is automatically revoked unless extended.

Access Reviews

Organization has set up a process for conducting company-wide user access reviews on an at least bi-annual basis. During this review, the company's overall identity directory should be reviewed for any terminated employees, and any job changes. These changes should be carried out as a result of the review.

In addition, each system containing or processing sensitive or protected information, including ePHI, must have access listings reviewed for any inappropriate access, unauthorized access, or terminated access. Any findings resulting from the system access review should be documented and carried out through the standard access control procedure. Any anomalous activity detected should be reported through the incident response and reporting process.

Only qualified workforce members, such as Human Resources and system owners, should perform user access reviews. Reviewers must sign off on the review and reflect the date the review as performed, as well as any changes that need to be completed as a result of the review. Reviewer signoffs are documented in our ticketing system.

ROLES AND RESPONSIBILITIES

User Access Reviewer: Determines if user access is appropriate during periodic access reviews. May be the application or system owner.

System Owner: Accountable for the system, including user access. May be the approver for access requests to their system(s).

FORMS/PLANS/DOCUMENTS

- Access Request
- Onboarding Checklist
- Offboarding Checklist
- User Access Reviews and Reviewer Signoff
- Emergency Access Log
- User Listings or Populations
- Risk Register

RELATED POLICIES AND PROCEDURES

- Data Security Policy – Security Management
- Data Security Policy – Information Access Management
- Data Security Policy – Facility Access Control
- Data Security Policy – Workforce Security
- Data Security Policy – Security Awareness and Training
- Data Security Policy – Contingency Plan
- Data Security Policy – ePHI Safeguards

RELEVANT HIPAA REGULATIONS

- 164.312(a)(1) *Access control*
- 164.308(a)(5)(ii)(D) *Password management*
- 164.312(d) *Standard: Person or Entity Authentication*
- 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 CRTIERIA

- CC6.1.2 *Restricts logical access*
- CC6.1.3 *Identifies and authenticates users*
- CC6.1.5 *Manages points of access*
- CC6.1.6 *Restricts access to information assets*
- CC6.1.7 *Manages identification and authentication*
- CC6.1.8 *Manages credentials for infrastructure and software*
- 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*

APPENDIX A: CIRCUMSTANCES WARRANTING TERMINATION OF ACCESS TO EPHI

Workforce members' access to ePHI must be terminated:

1. If management has evidence or reason to believe that the user is using information systems or resources in a manner inconsistent with Organization's HIPAA Security Rule policies.
2. If the workforce member or management has evidence or reason to believe the user's password has been compromised.
3. If the user resigns, is terminated, is suspended, retires, or is away on unapproved leave.
4. If the user's job description changes and system Access is no longer justified by the new job description.

APPENDIX B: EXAMPLE TERMINATION ACTIVITIES

Specific termination procedures may include:

- Physical security measures, if any, including retrieving keys and pass cards, and changing locks
- Deactivation of computers and other electronic tools
- Deactivation of Access accounts
- Disabling of users and passwords
- Completion of an employee offboarding checklist. Organization will complete this checklist each time an employee leaves Organization. Checklist items should include at least the following:
    - Return of all Access devices
    - Deactivation of logon accounts, including remote Access
    - Return of any computers and other similar electronic tools, such as a tablet or cell phone
    - Delivery of any data/information in the workforce member’s possession or control.