Data Security Policy – Facility Access Controls

PURPOSE

To provide principles and guidelines for managing access to Organization's facilities, including those that house information systems. To provide detailed instructions for managing access to Organization's facilities, including those that house information systems containing ePHI or sensitive information.

SCOPE

The Facility Access Controls Policy and Procedures covers Organization's:

- Facility access controls, including *visitor access*
- Facility security plans
- Contingency operations
- Maintenance records
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization is dedicated to maintaining the *confidentiality, integrity, and availability of ePHI*. Organization adopts and follows a process for controlling access to facilities and physical locations that hold information systems. These controls are enforced through technical and physical methods. Only *authorized and appropriate* personnel are given access to Organization's facilities and physical sites.

Facility Access Controls

To control access to facilities and physical equipment, including information systems*,* Organization has procedures for provisioning access, modifying access, terminating access, and reviewing access, including visitor access.

Only appropriate personnel are given access to facilities or parts of facilities containing information systems that host sensitive information or ePHI. Facility access must be approved by someone who is authorized to do so.

Provisioning Facility Access

Organization has adopted a process for approving and granting access to facilities based on an individual's role or function.

Access provisioning is formally documented and retained.

Modifying Facility Access

Organization has adopted a process for changing access to facilities as needed, including requesting the change, approving the change and executing the change. Access modifications may be requested when someone in the company changes roles, needs access to another physical site, needs temporary access to a facility, and other circumstances with a valid business justification.

Access modification is formally documented and retained.

Terminating Facility Access

Organization has adopted a process for removing or disabling access to facilities as needed. Access to facilities is removed within 24 hours of receiving the notification.

Access termination is formally documented and retained.

Reviewing Facility Access

Organization has adopted a process for reviewing and validating access to facilities on a periodic basis. Facility access should be limited to individuals who need access to perform their job or role. As part of this facility access review, any changes to access that are needed should be made.

Facility access reviews are formally documented and retained.

Visitor Access

Organization has adopted a process for controlling and monitoring visitor access to facilities and physical sites containing sensitive information or ePHI.

Visitor access logs are formally documented and retained.

Facility Security Plans

Organization has put in place facility security plans and safeguards that protect the facility and equipment and physical assets held at the site from unauthorized physical access, tampering, and theft. Any information systems or electronic media that contain ePHI or sensitive information are stored in secure physical locations.

Facility Contingency Operations

Organization has adopted and follows a Data Security Policy – Contingency Plan that provides guidance for how to respond in the event of an emergency or disaster. As part of disaster response and recovery, Organization has set up a contingency operations plan to recover any loss of data resulting from an emergency.

Organization has put in place a process to access facilities and physical sites holding ePHI or sensitive information during an emergency in support of the Business Continuity Plan (Emergency Mode Operating Plan), including requesting, approving, granting, monitoring, and terminating emergency facility access. Only authorized personnel will be given emergency facility access.

Facility Maintenance

Organization tracks and manages any security-related repairs, modifications or maintenance performed at facilities or physical sites that contain ePHI or sensitive information.

Facility maintenance records will be formally documented and retained.

PROCEDURES

Organization maintains the following facility access control procedures for its facilities and physical sites that contain information systems that store or process ePHI and other sensitive information.

Facility Access Controls

Organization keeps all documentation related to facility access in its ticketing system or a related tool.

Requesting Facility Access

To request access or modification of access to a facility or physical site, an individual or their manager must submit a formal request through the ticketing system or other tool. This request should include:

- Name or ID of the user receiving access
- Facility, site or area the user will access
- Requestor ID
- Date of request
- Business justification for access request

These requests are routed to the appropriate approver.

Provisioning or Modifying Facility Access

Upon receiving a request to provision or modify facility access, the Facility Manager or their delegate(s) review the request details and determine if the request should be approved or denied. Only appropriate personnel are approved for access to facilities that store ePHI or other sensitive information.

If the request is approved, the user will have their access granted or modified according to the request details. Any further changes to access will need a new request form.

If the request is denied, the user will not receive access.

Terminating Facility Access

In the event that an individual's access to a facility or physical site must be removed, terminated or disabled, their access will be revoked upon notification.

Reviewing Facility Access

On a **quarterly** basis, Organization reviews the list of people with access to facilities that contain ePHI or other sensitive information and makes sure that the list is complete and up to date. As part of the facility access review, the assessor will ensure that people who have access are:

- Not terminated employees or contractors
- Appropriate to have access based on their role or job function
- Appropriate to have access due to another business reason

If any changes need to be made coming out of the access review, those changes are made in a timely manner and documented.

As part of the facility access review, physical keys are inventoried to ensure that they are being held securely and by the appropriate individuals.

The facility access reviewer documents their review and signs off on the results.

Visitor Access

Before visitors can access Organization's facilities or sites with ePHI or other sensitive information, they must present photo ID, sign in to the visitor's log, and include the following details:

- First name
- Last name
- Date and time of arrival
- Data and time of departure
- Reason for visiting
- Main contact
- Signature or Initials

Visitors are to be escorted through any common areas or any areas that contain ePHI or other sensitive information or systems.

Facility Security Plans

Organization secures its facilities and physical sites containing information systems hosting ePHI or other sensitive information using a combination of controls and mechanisms.

Facilities and offices are locked to entry unless you have a badge or key. When appropriate, authorized employees and contractors receive unique badges to enter sites. Employees should not share access badges or allow "piggy backing" when entering a facility.

Alarms and surveillance cameras (where appropriate) ensure that the premises are protected.

If a physical key is lost or stolen, we will change the affected locks.

If an individual loses their badge or access card, we will disable the old card immediately and issue a new badge.

Data Centers, Network Cabinets, and Server Rooms

Data centers, network cabinets, and server rooms are kept locked. Access is only provisioned to a limited number of privileged users. All access to these areas is logged.

Facility Contingency Operations

Organization keeps and updates a Data Security Policy – Contingency Plan that provides instructions for operating in the event of an emergency.

During an emergency, appropriate people will be given access to facilities in order to support the objectives of the Business Continuity (Emergency Mode Operation) Plan. These authorized individuals will work to restore any loss of data, protect the confidentiality, integrity, and availability of ePHI, and fulfill their obligations listed in the Business Continuity Plan. When possible, we will log the activities and actions taken during emergency facility access.

Facility Maintenance

In the event that facility maintenance, repairs, or modifications are required at sites that contain information systems housing ePHI or other sensitive information, the details of those maintenance activities will be documented and tracked by the Facility Manager. This log should include:

- Name(s) of the maintenance personnel on-site
- Maintenance company
- Date and time of arrival
- Date and time of departure
- Description of repairs
- Reason for repairs
- Outcome of repairs and maintenance

ROLES AND RESPONSIBILITIES

Facility or Site Manager: Reviews and approves facility access, provisioning requests, modification requests, and terminations. Accountable for tracking and managing facility maintenance.

VIOLATIONS

Access to facilities and physical sites that contain ePHI or other sensitive information is limited to authorized personnel only.

Organization may take disciplinary action if personnel access facilities, physical sites, devices or equipment when they are not authorized to do so.

FORMS/PLANS/DOCUMENTS

- Facility Security Plan(s)
- Facility Visitor Access Logs
- Facility Access Logs and Documentation
- Business Continuity Plan (Emergency Mode Operating Plan)
- Maintenance Records and Logs

RELATED POLICY

- Data Security Policy – Contingency Plan

RELEVANT HIPAA REGULATIONS

- §164.310(a)(1) *Facility access controls*
- §164.310(a)(2)(ii) *Facility security plan*
- §164.310(a)(2)(iii) *Access control and validation procedures*
- §164.310(a)(2)(iv) *Maintenance records*

RELEVANT SOC 2 CRITERIA

- CC 6.4.1 *Creates or Modifies Physical Access*
- CC 6.4.2 *Removes Physical Access*
- CC 6.4.3 *Reviews Physical Access*