HIPAA POLICIES AND PROCEDURES

|  |  |  |
| --- | --- | --- |
| **Policy Title:**  Facility Access Controls **ID: FacilityAccessControls07022015**  **rev: 0.8** | | **Approval Date:**  00/00/0000  **Effective Date:** 00/00/0000  **Revisited date:** 00/00/0000 |
| **Subject:** Facility Access Control Policy | | |
| **Primary Responsible Departments and/or BAA:**   Security / Compliance | | **Review Frequency:**  **Last Review:** 00/00/0000  **Next Review:** 00/00/0000 |
| **Secondary Responsible Departments and/or BAA:**  Administration | |

**Scope:**

Workforce and Visitors

**Purpose:**  
In accordance with HIPAA compliance and these policies this policy details the specifics of our facility control plan, workforce access controls, and visitor access controls while ensuring that PHI and EPHI remains confidential, available and monitored.

**Authoritative Reference:**

45 C.F.R. § 164.310(a)(1) & (2)

**Policy Definitions:**

**1. Facility Security -** We must create and maintain facility security policies and procedures that outline and document safeguards for all facilities, systems, and equipment used to store EPHI against reasonably foreseeable physical risks, threats and vulnerabilities.   
  
The Facility Security must include the following components:

1. **Contingency Plan**  – Policies and procedures that allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan.
2. **Access Control and Validation** – Procedures to control and validate Workforce member's access to facilities based on their role or function.
3. **Physical Access Records** – Procedures to log physical access to any facility containing medium and high risk EPHI-based systems. Examples of facilities requiring physical access records are computer, telephone and system rooms.
4. **Maintenance Records** – Procedures to document and manage repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.

**2. Workforce Access Controls**

1. Establish and implement appropriate procedures to control and validate employees access to all facilities used to house PHI and EPHI based systems.
2. Adopt access control mechanisms to control physical access to all facilities containing PHI / EPHI based systems. (e.g. fireproof locked doors, biometric scanners, safes, card scanners are examples of physical access control mechanisms.)

**3. Visitor Access Controls**

1. We must create and implement procedures to control, validate, and document any visitor, that is, a non-workforce member (e.g. contractor, technician, auditor) accessing facilities used to house PHI/EPHI based systems.
2. Visitors who require access to facilities containing PHI or EPHI-based systems must sign in and provide information regarding their identity and the purpose of their visit.
3. Visitors must be escorted or otherwise appropriately monitored while in the facilities requiring access controls.

**Violations:**

Any individual found to have violated this policy may be subject to disciplinary action up to and including termination of employment or appropriate alternative actions in the case of visitors.

**Related Policies and Procedures:**

**Administrative:**

HIPAA Security Management Root Process

HIPAA Assigned Security Responsibility  
HIPAA Workforce Security

HIPAA Information Access Management

HIPAA Security Awareness and Training

HIPAA Security Incident Procedures

HIPAA Contingency Plan

HIPAA Evaluation

**Physical:**

HIPAA Device and Media Control Policy

HIPAA Facility Access Control Policy

**Technical:**

HIPAA Access Control Policy

HIPAA Audit Policy

HIPAA Authentication Policy

HIPAA Workstation Use Policy

HIPAA Workstation Security Policy

HIPAA Information Integrity Policy

HIPAA Transmission Security Policy

**BAA’s and Other Agreements:**

HIPAA Business Associate and Other Agreement Policy  
Google BAA