HIPAA POLICIES AND PROCEDURES

|  |  |  |
| --- | --- | --- |
| **Policy Title:**  Workstation Security Policy **ID: WorkstationSecurityPolicy07042015**  **rev: 0.8** | | **Approval Date:**  00/00/0000  **Effective Date:** 00/00/0000  **Revisited date:** 00/00/0000 |
| **Subject:** Policy for the security of workstations that store, transmit, access or otherwise interact with electronic personal health information (EPHI). | | |
| **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 / IT | |

**Scope:**   
Workforce

**Purpose:**   
To comply with all applicable laws, regulations and our own policies for security, availability, confidentiality and privacy this policy provides the workstation security compliance framework.

**Authoritative Reference:**

45 CFR § 164.310(c)

**Policy Definitions:**

1. **Workstation Security**
2. Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information must be restricted to authorized users in an appropriately access controlled environment environment.
3. Workforce members using workstations must consider the sensitivity of the information, including PHI and EPHI that may be accessed to minimize the risk of data breach or loss.
4. We must Implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.
5. Appropriate measures must include where appropriate:
6. All administrative safeguards to workstations allowing only authorized personnel with a UUID for that system.
7. All physical safeguards to workstations allowing only authorized personnel with a UUID for that system.
8. Technical safeguards to workstations allowing only authorized personnel with a UUID for that system.

**Violations:**

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

**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