HIPAA POLICIES AND PROCEDURES

|  |  |  |
| --- | --- | --- |
| **Policy Title:**  Audit Controls Policy **ID: AuditControlsPolicy07052015**  **rev: 0.8** | | **Approval Date:**  00/00/0000  **Effective Date:** 00/00/0000  **Revisited date:** 00/00/0000 |
| **Subject:**  Policy for audit controls, reporting and logging. | | |
| **Primary Responsible Departments and/or BAA:**   Compliance / Security, Google BAA | | **Review Frequency:**  **Last Review:** 00/00/0000  **Next Review:** 00/00/0000 |
| **Secondary Responsible Departments and/or BAA:**  Administration / IT | |

**Scope:**

Workforce and BAA’s

**Purpose:**  
To comply with all applicable laws, regulations and our own policies this policy covers creating a framework for audit controls.

**Authoritative Reference:**

45 C.F.R. § 164.312 (b)

**Policy Definitions:**

**1. Audit Control Mechanisms**

1. EPHI and other materials with high risk must: reside on, be transmitted by, or otherwise interact with systems which logs, stores and otherwise monitors all access attempts, transmission attempts and other system interaction in a manner that makes tampering with the audit controls as difficult as administratively feasible.
2. Audit logs must be reviewed on a regular basis.
3. Risk assessment rests with the Chief Compliance Officer and is made in accordance with applicable laws, regulations and these policies.

Each audit log must include, but is not limited to:

1. Unique User Identification (UUID)
2. Login Date/Time,
3. Accessed EPHI or other High Risk material
   * 1. Date/Time and
     2. User UUID
     3. Workstation ID(s)
4. Transmitted EPHI or other High Risk material
   * 1. Date/Time and
     2. User UUID
5. Removed EPHI or other High Risk material
   * 1. Date/Time and
     2. User UUID
6. Materials otherwise interacted Date/Time and UUID
   * 1. Date/Time and
     2. User UUID

**2. Audit Controls and Review Plan**

1. Audit Control and Review Procedures will be developed for any system that handles EPHI determined to be a risk requiring audit controls. This must be approved by the Chief Compliance Agent. If the EPHI systems change outside of a BAA, the audit control and review procedures must be reevaluated by the Chief Compliance Agent. These procedures must include:
2. Procedures to log devices, applications and services with reports containing at a minimum the UUID and Date/Time and EPHI accessed, transmitted or otherwise interacted with
3. Procedures to review audit logs and reports

**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