HIPAA POLICIES AND PROCEDURES

|  |  |  |
| --- | --- | --- |
| **Policy Title:**  Access Control Policy **ID: AccessControlPolicy06252015**  **rev:0.8** | | **Approval Date:**  00/00/0000  **Effective Date:** 00/00/0000  **Revisited date:** 00/00/0000 |
| **Subject:** Access control policy for personal health information (PHI) and electronic personal health information (EPHI) related systems and services. | | |
| **Primary Responsible Departments and/or BAA:**  Compliance and Security | | **Review Frequency:**  **Last Review:** 00/00/0000  **Next Review:** 00/00/0000 |
| **Secondary Responsible Departments and/or BAA:** Information Technology | |

**Purpose:**  To comply with all applicable laws, regulations and our own policies to this Policy covers the Audit controls required for HIPAA compliance in conjunction with a Google BAA.

**Authoritative Reference:**

45 C.F.R. § 164.312 (a)(1) & (2)

**Policy:** Control policy for Unique User ID (UUID), password, network and related tools for user and information control.

**Policy Definitions:**

**1. Unique User Identification**

a. To uniquely identify and track each user for the purpose of access control to all networks, systems, and services that interact with EPHI, and the monitoring of access to these systems in compliance with the measures outlined in this Policy and in accordance with the HIPAA.

b. Any user that requires access to any network, system, or application that accesses, transmits, receives, or stores EPHI must be provided with a unique user identification string.

c. When requesting access to any system that interacts with EPHI, a user must supply his or her previously assigned unique user identification in conjunction with a secure password to gain access.

**2. Passwords**

Passwords and passphrases are private key tied to an individual UUID and used in conjunction with other security policies to ensure the confidentiality and security of EPHI. Each user’s password must meet the requirements as outlined in the following password policy.

a. Each user's password must meet the following minimum requirements:

1. Passwords must be a minimum of eight characters in length
2. Passwords must not be only from words found in a dictionary, added dictionary words to other characters to create a unique passphrase is greatly encouraged as this creates a strong and easily remembered password.
3. Passwords must not include easily guessed information such as personal information (e.g. names, pets, birth dates, etc)
4. Passwords should include a mix of case, numbers and special characters where possible and that the user is not likely to resort to writing the password down).
5. Passwords should include some amount of randomness' to enhance the passphrase, by adding 2-8 unrelated but easy to remember additional characters to a passphrase it’s strength is greatly enhanced against all types of electronic attacks. (e.g. staplehorsebattery#24 is exceedingly secure and not so complex the user is likely to resort to writing it down.)

b. Users must never share their passwords or other unique verification credentials.

c. Users must protect their passwords and unique credentials at all times, never transmitting or storing them in an insecure manner and reporting all breaches immediately to their manager or if the manager is unavailable the responsible compliance agent or most closely associated personal.

d. Each user must ensure that their assigned UUID is appropriately protected and only used for legitimate business purposes and inside the company framework.

e. If a user believes their user identification has been compromised, they must report that security incident to their manager, who will contact the appropriate agent.

**3. Emergency Access**

a. To ensure that access to critical EPHI is maintained during an emergency situation, each Department must establish and implement procedures to ensure that access to a system that contains EPHI and is used to provide treatment to an individual is made available to any Policy caregiver in the case of an emergency, if the denial or strict access to that EPHI could inhibit or negatively affect an individual’s care. This information will always be available via the company to a company Internet administrator with access to the Google BAA tools.

b. EPHI repositories that do not affect an individual’s care are not subject to the foregoing emergency access requirement.

**4. Automatic Logoff**

a. Computers, devices, or other systems containing EPHI repositories that have been classified as high risk must employ inactivity timers or automatic logoff mechanisms.

b. The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity. These systems are usually easily protected using a screen-lock/screen saver to protect the device and having log-out timers built into the accounts controlling the data, in the case of a Google BAA all company devices should be registered and automatic logout timers employed via the Google Administration tools.

c. Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store EPHI must employ inactivity timers or automatic logoff mechanisms. (i.e., password protected screensaver that blacks out screen activity.) The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity. These machines should manually put into screenlock/screensaver mode and if EPHI is being utilized and it must be left unattended.

d. Applications and databases using EPHI, such as electronic claims records, must employ inactivity timers or automatic session logout mechanisms. The aforementioned application sessions must automatically terminate after a maximum of 30 minutes of inactivity

e. Servers, workstations, or other computer systems that access, transmit, receive, or store EPHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.

f. If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:

1. The system must be upgraded or moved to support the required inactivity timer or automatic logoff mechanism.
2. The system must be moved into a secure environment.

All EPHI must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism.

g. When leaving a server, workstation, or other computer system unattended, Users must lock or activate the systems automatic logoff mechanism or logout of all applications and systems containing EPHI.

**5. Encryption**

a. Networked devices that handle EPHI must do so inside a properly secured and encrypted environment to prevent tampering. Encryption of EPHI must take place during any network transmission, data used within the framework of Google gmail, Drive, Docs and Calendar on Google BAA accounts are encrypted in both storage and transmission using state of the art secure encryption methods (e.g. as of this writing TLS 1.2 or better on electronic traffic inside the applicable Google HIPAA compliant service).

**6. Secure Network Use**

a. All networks housing machines that connect to EPHI repositories such as those from our Google BAA must be appropriately secured. To ensure that all networks that contain EPHI-based systems and applications are appropriately secured, each connection to outside the network must follow the steps outlined below.

1. Connect to an associated Google BAA account or other EPHI repository only through proper clients, programs and workstations authorized to connect to EPHI repositories.

2. Only ever interact with or execute functions on EPHI for which you have been given explicit permission.

**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