HIPAA POLICIES AND PROCEDURES

|  |  |  |
| --- | --- | --- |
| **Policy Title:**  HIPAA Device and Media Control Policy **Procedure ID: HIPAADeviceMediaControl06222015**  **Revision: 0.8** | | **Approval Date:** Pending  **Effective Date:** Pending  **Date Policy Last Revised:** |
| Subject: Guidelines for electronic device and storage mediums used in association of protected health information (PHI) and electronic Protected Health Information (EPHI). | | |
| **Primary Responsible Departments and/or BAA:**  Compliance and Security | | **Review Frequency:** Pending  **Last Review:** Pending **Last Reviewed by:**  Pending  **Next Review:** Pending |
| **Secondary Responsible Departments and/or BAA:** Information Technology / Records / Google BAA | |

**Scope:**

Employees/staff that handle PHI/EPHI and related media and devices

**Purpose:**Electronic equipment and Storage Media used for electronic protected health information (EPHI) has three primary risk vectors transmission, storage and decommissioning.   
  
**Authoritative Reference:**

45 C. F. R. §164.310(d)(1) & (2)

**Policy:** HIPAA Device and Media Control

**Policy Definitions:**

1. **Hardware Devices -** Including but not limited to personal computers(PC’s), servers, laptops, copiers, fax machines, scanners and handheld technology devices (i.e. smart-phones).
2. **Storage Media -** Including but not limited to disk drives, tapes, floppy disks, CD’s, zip disks, flash cards, USB memory sticks, optical disks, any other optical, magnetic or other long-term storage medium including hard copies.
3. **Disposal:** EPHI on decommissioned devices and storage media must be irretrievably destroyed. If the device contains EPHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. Simple deletion, ‘trashing’ and even formatting the media is not sufficient as it does not overwrite the data. If the device contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to disposal.
   1. Removable magnetic "disks" and sticks (floppies such as 3.5”) and magnetic tapes (cartridges) can be "degaussed" by an appropriately-sized and powered degasser, physically destroyed or undergo a “write-many” data shredding procedure where the files individual bits are overwritten several times randomly.
   2. Fixed internal magnetic storage (such as computer hard drives) and removable magnetic storage, can be cleansed by a rewriting or zeroing process. Software is used to overwrite all the usable storage locations of a medium. The simplest method, a single overwrite, is sometimes insufficient to completely destroy the EPHI so always use multiple over-writes with random overwrite variations to ensure the original EPHI data structure cannot be reconstituted.
   3. Write-many optical media (such as CD-RWs) can be processed with a single overwrite of the entire disc as this process stripes away the previous layer of data.
   4. Write-once optical media (e.g. CD-R disc). For the write-once media the physical destruction of the media is required to destroy the data.
   5. Removable solid state storage devices (SSD's, USB Sticks). These devices are solid state and are stable. Secure overwrites (following manufacturer specifications) are possible and in fact somewhat simpler for this type of media as once the storage bytes are zeroed the data no longer has anything to be reconstituted from unlike magnetic storage mediums.
   6. Paper containing sensitive information should be incinerated or pulped to guarantee the data cannot be reconstituted. Barring those options cross-cut shredders that provide both length and width dismemberment generating many hundreds of pieces per shredded page should be used.

**3. Media reuse**

Any equipment or storage media that contains confidential, critical, internal use only, and/or private information must be erased or destroyed using proper tools and techniques by the appropriate expert personnel before the equipment/media is reused or decommissioned.

**4. Record of Movement**

When using devices and media to transport EPHI a procedure must be implemented to monitor the movement of those devices and media and the parties responsible for the device and media during its movement. This is provided by our Google BAA for all EPHI on their network.

**5. Retrieval of EPHI**

All original EPHI must be backed up on a regular basis. Backup mechanisms must be tested regularly to verify that EPHI can be efficiently retrieved. This includes backup of portable devices such as laptops and PDA’s, when storing original EPHI. Backups of original EPHI must be stored off-site in a physically secure facility. This is provided by our Google BAA for all EPHI on their network.

**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