**Policy Title:** HIPAA Device and Media Control

**Number:** TD-QMP-7017

**Subject:** Guidelines for electronic equipment and storage media used in association of protected health information.

<table>
<thead>
<tr>
<th><strong>Primary Department:</strong></th>
<th><strong>Secondary Department:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>TennDent/Quality Monitoring/Improvement</td>
<td>TennDent/Administration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Effective Date of Policy:</strong></th>
<th><strong>Prior Policy or Cross Reference(s):</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>9/23/2011</td>
<td>10/1/2010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Last Reviewed by TennDent Quality Monitoring/Improvement Committee:</strong></th>
<th><strong>Date Policy Last Revised:</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Review Frequency:</strong></th>
<th><strong>Next Scheduled Review:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Annually</td>
<td>7/1/2012</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>TennDent Quality Monitoring/Improvement Committee Approval:</strong></th>
<th><strong>Approval Date:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>On File</td>
<td>9/23/2011</td>
</tr>
</tbody>
</table>

**Scope:**

TennDent staff, employees of Delta Dental of Tennessee (DDTN), TennDent/IT

**Purpose:**

Electronic equipment and Storage Media used in association with electronic protected health information (EEPHI) can be a potential source of disclosure when being moved, decommissioned or destroyed. The purpose of this policy is to establish guidelines for the following (the first two are required, the last two addressable):

1. Address the final disposition of EEPHI, and/or the hardware or electronic media on which it is stored.
2. Removal of EEPHI from electronic media before the media is made available for re-use
3. Creating a record of the movements of hardware and electronic media and any person responsible
4. Creating a retrievable, exact copy of EEPHI, when needed, before movement of equipment

**Authoritative Reference:**

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) HIPAA Security Rule [HIPAA Physical Safeguards] [see §164.310(d)(1) & (2)]
Policy:

DEFINITIONS:

Device: Including but not limited to personal computers, servers, laptops, copiers, fax machines, handheld units (i.e. PDA’s).

Storage Media: Including but not limited to disk drives, tapes, floppy disks, CD’s, zip disks, flash cards, USB memory sticks, optical disks, and hard copies.

1. Disposal: All EPHI on decommissioned devices and storage media must be irretrievably destroyed, in order to protect the confidentiality of the data contained. If the device or media 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. A typical reformat is not sufficient as it does not overwrite the data. If the device or media contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to disposal.

   a) Removable magnetic "disks" (floppies, ZIP disks, and the like) and magnetic tapes (reels, cartridges) can be "degauersed" by an appropriately-sized and -powered degasser or physically destroyed.

   b) Fixed internal magnetic storage (such as computer hard drives), as well as removable storage, can be cleansed by a re-writing process. Software is used to over-write all the usable storage locations of a medium. The simplest method is a single over-write; additional security is provided by multiple over-writes with variations of all 0s, all 1s, complements (opposite of recorded character), and/or random characters.

   c) A few kinds of "write-many" optical media (such as CD-RWs) can be processed via an over-write method. This is not the case for the vast majority of "write-once" optical media in use (notably the CD-R). Because such media are optical rather than magnetic, they can not be degaussued. For the write-once variety, only physical destruction will do.

   d) Removable "solid state" storage devices are also now available. These "flash memory" devices are solid state and are non-volatile (the memory maintains data even after all power sources have been disconnected). Examples include CompactFlash, Memory Stick, Secure Digital, SmartMedia and other types of plug-ins, and a range of "mini-" and "micro-drive" flash devices that use USB or FireWire ports. Secure overwrites (following manufacturer specifications) are possible for these media as well. Neither degaussing nor over-writing offers absolute guarantees. Unless, of course, one is willing to disintegrate, incinerate, pulverize, shred, or smelt. As with paper, the method of disposal depends on the perceived risks of discovery, and estimates of the type of threat.

   e) Paper containing sensitive information should be shredded. Strip cut shredders (also called straight cut or spaghetti cut) render paper into thin, long strips. Cross-cut shredders (also
called confetti cut) provide both length-wise and width-wise dismemberment -- generating from a few to many hundreds of pieces per shredded page.

2. **Media reuse**
   Any equipment or storage media that contains confidential, critical, internal use only, and/or private information will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee before the equipment/media is reused.

3. **Record of Movements**
   When using storage devices and removable media to transport EPHI a procedure will be implemented to track and maintain records of the movement of those devices and media and the parties responsible for the device and media during its movement.

4. **Retrieval of EPHI**
   All original EPHI must be backed up on a regular basis. Backup mechanisms will 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.

**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:**
- Document and Records Management Policy
- Document and Records Management Procedure
- HIPAA Access Control Policy
- HIPAA Data Backup and Contingency Planning Policy
- HIPAA Data Backup Procedures
- HIPAA Device and Media Control Procedure
- HIPAA Facility Access Controls Policy
- HIPAA Information Access Management Policy
- HIPAA Information Access Management Procedure
- HIPAA Password Policy
- HIPAA Personal Health Information Policy
- HIPAA Security Compliance Policy
- HIPAA Server, Desktop and Wireless Computer System Policy
- HIPAA System Security Procedure

**Related Documents:**