HIPAA-33: Device, Media and Records Disposal or Re-Use Policy

Effective Date:	12-01-2015	Last Revised:	7-17-2017

Scope of Policy

This policy governs Media Disposal for **TCS**. All personnel of **TCS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Assumptions

- **TCS** must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- *Media subject to disposal* containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.
- *Media subject to reallocation* and reuse containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased, or sanitized ("wiped") before any re-use of such media may take place, or the data residing on such media is subject to corruption, compromise, or loss.

Policy Statement

- It is the Policy of **TCS** to dispose of all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in full compliance with all the requirements of HIPAA. This may include copiers, multi-function printers, and other devices in addition to computers, servers and other data storage systems.
- It is the Policy of **TCS** to properly erase and or sanitize ("wipe") all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before any media may be re-used.
- It is the Policy of **TCS** to fully document all media disposal-related or media re-use and disposition-related activities and efforts, in accordance with our Documentation Policy.
- Responsibility for proper media disposal and disposition shall reside with Executive Director who shall develop procedures to ensure the proper disposition of all such media before disposal or reuse.

Key Definitions

- Degauss: Using a magnetic field to erase (neutralize) the data bits stored on magnetic media.
- Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.
- Patient Health Information Media: Any record of patient health information, regardless of medium or characteristic that can be retrieved at any time. This includes all original patient records, documents, papers, letters, billing statements, x-rays, films, cards, photographs, sound and video recordings, microfilm, magnetic tape, electronic media, and other information recording media, regardless of physical form or characteristic, that are generated and/or received in connection with transacting patient care or business.
- Sanitization: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.

Procedures

- ❑ **TCS** has instituted an asset inventory management process to track the movement of hardware and electronic media into and out of the organization
- ❑ When devices are either transferred to another user, cycled out of use, or turned back in on lease, procedures will be employed to clear sensitive data by personnel appropriately qualified to do so and documented to provide adequate records of such action.
- ❑ All destruction/disposal of patient health information media will be done in accordance with federal and state laws and regulations and pursuant to the organization's written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- ❑ Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a custody release form will be executed which states the receiving party will be responsible for returning the records to TCS, or properly destroyed/disposed of by the requesting party.
- ❑ Before reuse of any recordable and erasable media, (for example hard disks, tapes, cartridges, USB drives, smart phones, SAN disks, SD and similar cards), all ePHI must be rendered inaccessible, cleaned, or scrubbed. Standard approaches include one or all of the following methods:
  - Overwrite the data (for example, through software utilities).
  - Degauss the media.
  - Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of PHI is complete.
- ❑ The business associate agreement must provide that, upon termination of the contract, the business associate will return or destroy/dispose of all patient health information. If such return or destruction/disposal is not feasible, the contract must limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
- ❑ A record of all PHI media sanitization should be made and retained by the organization. The organization has the responsibility to retain the burden of proof for any media destruction regardless of whether destruction is done by the organization or by a contractor. Retention is required because the records of destruction/disposal may become necessary to demonstrate that the patient information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal, such as a certificate of destruction, should include:
  - Date of destruction/disposal.
  - Method of destruction/disposal.
  - Description of the destroyed/disposed record series or medium.
  - Inclusive dates covered.
  - A statement that the patient information records were destroyed/disposed of in the normal course of business.
  - The signatures of the individuals supervising and witnessing the destruction/disposal.
  - Copies of documents and images that contain PHI and are not originals that do not require retention based on retention policies (e.g., provider copies, schedule print outs etc.) shall be destroyed/disposed of by shredding or other acceptable manner as outlined in this policy. Certification of destruction is not required.
- ❑ If destruction/disposal services are contracted, the contract must provide that the organization's business associate will establish the permitted and required uses and

disclosures of information by the business associate as set forth in the federal and state law (outlined in **TCS**'s HIPAA Business Associated Agreement/Contract). The BAA should also set minimum acceptable standards for the sanitization of media containing PHI. The BAA or contract should include but not be limited to the following:

- Specify the method of destruction/disposal.
- Specify the time that will elapse between acquisition and destruction/disposal of data/media.
- Establish safeguards against unauthorized disclosures of PHI.
- Indemnify the organization from loss due to unauthorized disclosure.
- Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect.

❑ Provide proof of destruction/disposal (e.g. certificate of destruction).

❑ Any media containing PHI should be destroyed/disposed of using a method that ensures the PHI could not be recovered or reconstructed. Some appropriate methods for destroying/disposing of media are outlined in the following table.

Medium	Recommendation
Audiotapes	Methods for destruction, disposal, or reuse of audiotapes include recycling (tape over), degaussing or pulverizing.
Electronic Data/ Hard Disk Drives including drives found in printers or copiers	Methods of destruction, disposal, or reuse should destroy data permanently and irreversibly. Methods of reuse may include overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten. See appendix A for links to some available software to completely remove data from hard drives.
Electronic Data/ Removable media or devices including USB drives or SD cards	Methods of destruction, disposal, or reuse may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until the data has been overwritten. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Shredding or pulverization should be the final disposition of any removable media when it is no longer usable.
Handheld devices including cell phones, smart phones, PDAs, tablets and similar devices.	Software is available to remotely wipe data from handheld devices. This should be standard practice. Any removable media that is used by these devices should be handled as specified in the previous paragraph. When a handheld device is no longer reusable it should be totally destroyed by recycling or by trash compacting
Optical Media	Optical disks cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.

Medium	Recommendation
Microfilm/ Microfiche	Methods for destruction, disposal, or reuse of microfilm or microfiche include recycling and pulverizing.
PHI Labeled Devices, Containers, Equipment, Etc.	Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Removing labels or incineration of the medium would be appropriate. Another option is to obliterate the information with a heavy permanent marker pen. Ribbons used to print labels may contain PHI and should be disposed of by shredding or incineration
Paper Records	Paper records should be destroyed/disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing. If shredded, use cross cut shredders which produce particles that are 1 x 5 millimeters or smaller in size.
Videotapes	Methods for destruction, disposal, or reuse of videotapes include recycling (tape over) or pulverizing.

- **Additional Information on Disposal of Discarded Paper Containing PHI:** Such paper copies may be disposed of in recycle bins or waste receptacles only as described below:
  1. Unsecured recycle bins/waste receptacles should be located in areas where the public will not be able to access them.
  2. When possible, dispose of paper waste containing PHI in receptacles that are secured by locking mechanisms or that are located behind locked doors after regular business hours. Locked containers must be used with copy machines located in insecure or unattended areas.
  3. Paper documents containing PHI may be placed in recycle bins/waste receptacles as described above only if the paper in such bins or receptacles will be disposed of in a manner that leaves no possibility for reconstruction of the information as described in the table above
- The methods of destruction, disposal, and reuse should be reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.
- Preservation or Destruction/Disposal of Patient Health Records Upon Closure of a Provider Office/Practice will be done in compliance with HIPAA specifications.

Note; See Certificate of Data Destruction in HIPAA Policy Addendum