WEBER HUMAN SERVICES	**Policy & Procedure** HIPAA / PRIVACY **DESTRUCTION OF PHI**	**NUMBER** 25 **APPROVED** 2/21/2014 **REVIEWED** 5/11/2017 **REVISED**

PURPOSE

To ensure that any medium containing Protected Health Information ("PHI") is properly destroyed.

POLICY

PHI stored in paper, electronic or other format will be destroyed utilizing an acceptable method of destruction after the appropriate retention period has been met.

Access to PHI stored on computer equipment and media will be limited by taking the appropriate measures to destroy electronically stored PHI.

PROCEDURE

Paper Documents

1. Documentation that is not part of the Medical Record and will not become part of the Medical Record (e.g., report sheets, copies of documents already in the Medical Record, etc.) shall be destroyed promptly when it is no longer needed by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.
2. PHI maintained in paper format will be destroyed at the end of the retention period. (See the Policy "Retention of Protected Health Information.")
3. All paper documents that contain PHI will be destroyed using an acceptable method of destruction.
4. Acceptable methods of destruction include shredding, incineration, pulverization and use of a bonded recycling company.
5. An *Inactive Medical Record Filing/Destruction Log ("Destruction Log")* must be maintained to identify the destroyed records. At a minimum, the *Destruction Log* must capture the information listed below.
    a. Date of destruction (date/s records are destroyed),
    b. Destroyed by (name/s of the individuals responsible for destroying the records),
    c. Witness (name/s of the person witnessing the destruction),
    d. Method of destruction (method used to destroy records), and
    e. Resident information (full name, Medical Record number, date of admission, date of discharge).

(See sample *Destruction Log* following this Policy.)

6. Prior to destruction of boxed items, the Facility will verify the retention period has expired.

7. If the records are destroyed off-site through a destruction company, a Certificate of Destruction should be obtained attesting to destruction of the records.

8. The Facility will maintain destruction documents permanently.

Computer Data Storage Media

1. Personal Computers: Workstations, laptops and servers use hard drives to store a wide variety of information. Clients' health information may be stored in a number of areas on a computer hard drive. For example, health information may be stored in "Folders" specifically designated for storage of this type of information, in temporary storage areas and in cache. Simply deleting the files or folders containing this information does not necessarily erase the data.

    a. To ensure that any clients' health information has been removed, a utility that overwrites the entire disk drive with "1"s and "0"s must be used.
    b. If the computer is being re-deployed internally or disposed of due to obsolescence, the aforementioned utility must be run against the computer's hard drive, after which the hard drive may be reformatted and a standard software image loaded on the reformatted drive.
    c. If the computer is being disposed of due to damage and it is not possible to run the utility to overwrite the data, then the hard drive must be removed from the computer and physically destroyed. Alternatively, the drive can be erased by use of magnetic bulk eraser. This applies to PC workstations, laptops and servers.

2. Backup or Data Tapes:

    a. Tapes are typically re-used many times but generally only by the data processing groups within the Facility, which routinely must handle client health information. However, there may be situations where tapes are sent to external recipients for specific processing. Tapes used for this purpose should be segregated from the general pool used for backups. These tapes should be degaussed prior to use in creating the files being sent to ensure that no prior client health information remains on that portion of the tape beyond the end of the current file.
    b. Tapes or diskettes that are being decommissioned must be degaussed before disposal. This can be accomplished using a bulk tape eraser. Alternatively, the media may be pulverized or shredded.

3. Compact Disks (CDs) and Diskettes: CDs containing resident health information must be cut into pieces or pulverized before disposal.

4. Fax/Copy Machines: Digital copiers use hard drives to store images of documents that have been copied, printed or faxed. Before these machines are returned to their leasing company or sold, the hard drive must be erased or destroyed.

a. To ensure that any clients' health information has been removed, a utility that overwrites the entire disk drive with "1"s and "0"s must be used.
b. If the computer is being re-deployed internally or disposed of due to obsolescence, the aforementioned utility must be run against the hard drive, after which the hard drive may be reformatted and a standard software image loaded on the reformatted drive.
c. If the computer is being disposed of due to damage and it is not possible to run the utility to overwrite the data, then the hard drive must be removed from the computer and physically destroyed. Alternatively, the drive can be erased by use of magnetic bulk eraser.

5. If a service is used for disposal, the vendor should provide a certificate indicating the following:

a. Computers and media that were decommissioned have been disposed of in accordance with environmental regulations as computers and media may contain hazardous materials.
b. Data stored on the decommissioned computer and/or media was erased or destroyed per the previously stated method(s) prior to disposal.

SAMPLE

INACTIVE MEDICAL RECORD FILING/DESTRUCTION LOG

Year of Discharge: _____ Year to Destroy: _____

Client Name (First and Last)	Medical Record Number	Admission Date	Discharge Date	Box Number

Date of Destruction: _____ Witness: _____

Destroyed By: _____ Method of Destruction: _____

Center Name / Number: _____ HIM Representative: _____

The information described above was destroyed in the normal course of business pursuant to proper retention schedules as determined by Federal and State law and destruction policy and procedure.

Retain log permanently.