SECTION 2: HEALTH INFORMATION MANAGEMENT

2.4. Retention, Archiving, and Disposal

POLICY

1. **Retention:** The health record retention policies of the University of Florida (UF) are based on official schedules as well as on standards of professional practice and risk management guidelines. The subsequent death of a patient has no bearing on retention standards: Health records must be retained for the full period of time required by state laws and/or UF policies. Health records should not be retained beyond their official retention period.

   a. All primary medical records must be retained for at least ten (10) years from the date of the patient’s last episode of care, irrespective of the individual’s age or majority status at that time.

   b. Under Florida statutes, primary dental records must be retained for at least four (4) years, with certain exceptions, from the date of a patient’s last episode of care. (Refer to College of Dentistry policies for current specific retention requirements and procedures.)

   c. Other records containing PHI, including financial and research records, must be retained for the length of time prescribed in the General Records Schedule or by relevant state and federal laws.

   d. Records containing materials specifically required by HIPAA must be retained for at least six (6) years after the materials were last in effect.

2. **Archiving and Storage:** Primary health records and data, whether maintained in paper or electronic format, which are not being used for active provision of services, payment processes, or research may be archived until the retention requirements have been met.

   a. Only primary health, financial, and research records should be archived. The contents of true “Shadow” records should be destroyed after ascertaining that they contain only duplicates of records maintained elsewhere and do not contain any original materials.

   b. All inactive or back-up records containing PHI or other restricted data must be stored in approved storage facilities. Approved storage areas include:

      i. **On-Site:** An area inside the clinic, department, college, or other UF facility that meets the criteria listed below (C.3. Storage Areas). Record owners are responsible for making arrangements to inventory and move the records.

      ii. **Off-Site:** A private professional record storage company with which UF has an active contract for services. Off-site storage arrangements for back-up electronic records must be approved by the Privacy Office.

        NOTE: Moving and storage warehouses, mini-storage facilities, and off-campus personal or rental property, including garages, attics, homes, mobile homes, trailers, etc., are NOT acceptable for storage of inactive records containing restricted data.

3. **Disposal and Destruction:** Record owners are responsible for arranging for safe and secure disposal of records containing PHI and other restricted data, following UF policies and the processes outlined in this policy, and using established methods which do not permit recovery, reconstruction or future use of the information.
a. Whole primary health and financial records shall only be destroyed in the ordinary course of business; no entire record shall be destroyed on an individual basis.

b. Primary records of any type belonging to UF may only be destroyed when the retention periods established by UF have been met, and a Records Disposition Request has been approved by University Records Management.
   i. No records that are currently involved in open investigations, audits, or similar activities, or have litigation pending, shall be destroyed or otherwise discarded.

DEFINITIONS

1. “Scheduling” Records: Identifying types of records and then determining how long a particular type must be retained.

2. Archiving / Storage: The act of physically moving inactive or other records to a storage location until the record retention requirements are met or until the records are needed again.

3. Destruction of Records: The routine systematic disposal of primary records to permanently remove them from active use. Destruction methods should ensure that confidentiality of the information is maintained, and that there is no possibility of reconstructing the information contained in the records.

4. Disposal of Record Documents: The day-to-day discarding of duplicate or extra reports that are not now and/or historically never were pertinent to or required for inclusion in the primary record.

5. Inactive Records: Records of patients who have not received services, made payments for services, or been involved in research for a designated period of time. Clinics and departments determine the criteria for inactive status in their areas, based on need for the records and available storage space.

PRIVACY AND STATUTORY REQUIREMENTS

1. Chapter 257, Florida Statutes, establishes the State’s Records Management and Archives Program under the direction of the Division of Library and Information Services, Department of State, as well as specifically provides for a system for the scheduling and disposal of public records.

2. Obtaining Disposition Authorization: When records have met retention requirements, disposal of the records may be initiated by submitting a Records Disposition Request to the UF Records Management Office.
   a. Requests must be submitted and approved before actual disposition is carried out. Once approved, the request form authorizes the disposition of the listed records.
   b. Storage Areas for all records containing PHI or other restricted data must be physically secure and environmentally controlled, to protect the records from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.

3. Record Destruction: Primary records containing PHI or other restricted data shall only be destroyed by a bonded and insured professional document destruction company. Having a departmental or clinic representative witness the destruction is encouraged, but not required.

PROCEDURES

1. Archiving Inactive Paper Records: Preparing records for storage
   a. Storage Locations:
      i. Call the Privacy Office for information about currently contracted commercial storage facilities. Transport of records is included in the services.
ii. Inventorizing of records may also be arranged on the request of the record owner.

iii. Alternative arrangements for complying with security policies requiring off-site storage of back-up electronic media should be proposed in writing for approval by the Privacy Office.

b. Preparing Primary Health Records for Storage:

i. Create an inventory (see Forms), listing each individual record being sent to storage, so that they may be quickly retrieved, if needed. The list is also useful for documenting the destruction of the records after the retention requirement is met.

ii. The inventory list must be retained in the clinic or department that owns or is custodian for the records and should include:

   • Heading: Clinic or Department name and type of record (use the current Records Schedule)
   • List: Patient’s name and record number, dates of service included in each record, box number or other location indicator for each record
   • Inventories may be in paper or electronic format.
   • Store electronic inventories and back-up copies on a secure server or on encrypted removable media only (disk, tape, or CD), not on a workstation hard drive. Back up electronic inventories and copies regularly.
   • Store paper inventories in a clearly labeled binder. Mark the binder: “Do Not Destroy.” Do not send the inventories to off-site storage.
   • Remove paper health records from the active file area (shelving, file cabinets) by year and place them in approved storage boxes in the order in which they were originally filed (alphabetical or numerical).
   • Use the storage facility’s guidelines, as appropriate, to place the boxes into storage.

c. Preparing Other Original/Primary Records for Storage:

i. Other types of records, even if they contain PHI, may, but are not required to be individually inventoried for storage. Follow above steps for these records.

ii. Shadow Records should not be archived. Purge shadow records often and file or otherwise place any original materials in the primary records. Follow the procedure below for record disposal to permanently destroy the duplicate parts of the record. (An inventory of duplicate records disposed of in this manner is not required.)

d. Retrieving records from storage: Track the location of stored records that have been brought back to UF from storage, whether active or inactive, and adjust the storage inventory list as needed if any records are not returned to storage.

e. Disposing of Non-Primary Record Documents Containing PHI (i.e., duplicate, extra, or obsolete individual reports or data that are not and, historically, never were pertinent to the patient’s care).

   i. Controlled Destruction: Paper records and records stored on electronic media must be immediately shredded or pulverized, electronically purged, or placed in locked or otherwise secure storage for contracted shredding/destruction. (See chart: Appropriate Record Destruction Methods at the end of this chapter.)

   ii. Contracted Recycling: Papers containing PHI may only be placed in locked bins provided under a department’s contract with a private, licensed and bonded document destruction company.
Papers containing PHI may NOT be placed in any UF recycling bins for pickup by UF Physical Plant, even if the bin is locked. Papers that have already been shredded may be placed in UF recycling bins for pick-up by Physical Plant Services.

f. Permanently Destroying Whole Health Records

i. Requesting Approval for Record Destruction

• Complete the UF Records Disposition Request (see Forms) prior to commencing record destruction procedures. Follow the instructions included on the form.
• Send the Request to the address on the form. Authorization to destroy records may take 6 to 8 weeks to process.

ii. Preparing Primary Health Records for Destruction

• Maintain Security: Maintain records that are scheduled for destruction in a secure location to guard against unauthorized or inappropriate access until the destruction is complete.
• Create an Inventory: Complete a Record Destruction Log (see Forms), individually listing each and every health record scheduled to be destroyed, or, if records are already archived, use the Storage Inventory, created when the records were put into storage, to avoid duplication of effort.
• Include the following information for each record (See Forms for a sample log).
  o Patient name and health record number
  o Dates of service included
  o Description of type of record (UF General Records Schedule type)
  o Date and Method of Destruction
  o The name of the company performing the destruction
  o Signature(s) of individuals witnessing the destruction, if any
  o Record Destruction Logs must be maintained for the life of the institution, and may only be maintained in paper formats.

g. How to Destroy Patient Records

i. Follow the record destruction company’s protocol for carrying out the actual destruction. Do not destroy whole records within a clinic, department or unit without using a bonded, licensed record destruction company that will provide an official certificate of destruction.

ii. After the destruction has been completed, sign the UF Records Disposition Request and the Record Destruction Log.

iii. Attach the Certificate of Destruction provided by the record destruction company to the Disposition Request form and the Record Destruction Log.

iv. Maintain all documentation of record destruction for the life of the institution.

REFERENCES

1. HIPAA: 45 CFR §164.501 (Definitions); §164.502 (Use and Disclosure)
2. Florida Statutes: 119 (Public Records – Health Records Excluded); 257 (Records Management and Archives Program)

EXHIBITS
2. UF Privacy Office forms at, http://privacy.ufl.edu/uf-health-privacy/forms/.
3. Appropriate Record Destruction Methods Table.

### Appropriate Record Destruction Methods

<table>
<thead>
<tr>
<th>Medium</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Records</td>
<td>Shred (cross-cut), pulp, burn, or pulverize</td>
</tr>
<tr>
<td>Audiotapes &amp; Videotapes</td>
<td>Recycle by recording over by the original user, cut up the tapes, or pulverize/crush the tape and cassette</td>
</tr>
<tr>
<td>Computerized Data / Hard Disk Drives / Magnetic Media / Memory Sticks, Keys and other USB memory devices</td>
<td>Professionally purge (degass) by a certified, licensed, and bonded vendor and pulverize</td>
</tr>
<tr>
<td>Computer Diskettes (old style: 3 and 6 inch)</td>
<td>Reformat and over-write all data, pulverize, remove from cover and cut up, or magnetically degauss</td>
</tr>
<tr>
<td>Laser Disks / Compact Disks</td>
<td>Shred or pulverize in appropriate equipment, OR break, using layers of newspaper and a hammer, OR thoroughly scratch both sides with knife or key</td>
</tr>
<tr>
<td>Microfilm / Microfiche</td>
<td>Shred or pulverize</td>
</tr>
<tr>
<td>PHI Labels on Devices, Containers, Equipment, Etc.</td>
<td>Obliterate all PHI on the label, remove and destroy the label, or incinerate the devices, container, etc., if removal or obliteration of the label is impossible.</td>
</tr>
</tbody>
</table>