AHIMA's Long-Term Care Health Information Practice and Documentation Guidelines

Practice Guidelines for LTC Health Information and Record Systems

---

Destruction

HIM STANDARD:

- The healthcare organization's and health information management department's health record and data destruction systems, policies, and procedures comply with federal and state regulations and accepted standards of practice.
- Policies and procedures exist to facilitate the destruction of health records and protected health information stored in paper or electronic format using an acceptable method of destruction after the appropriate retention period.
- Destruction of any record involved in an open investigation, audit or litigation is not permitted
- The destruction system is designed and implemented to ensure the security and confidentiality of the health records and protected health information being destroyed.

Every long term care facility should have a policy and procedure established to destroy records or confidential documents, whether in paper or electronic format, that are beyond their retention period. Destruction should be done at least annually based on a proper written retention schedule that encompasses federal and state regulations. The policies and procedures and the destruction schedule should demonstrate that records are destroyed in the normal course of business, as consistency and documentation are key components of record management. A destruction program that documents both appropriate retention and destruction of documents protects the facility/organization from legal liability. At least annually, every facility should review the documents on the retention guideline and destroy records as appropriate. It is recommended that the Executive Director/Administrator be notified and approve of records/documents to be destroyed. (See Retention section)

Acceptable Methods of Destruction - Paper-based Records

Paper-based records containing resident-identifiable data must be destroyed in a manner that makes it impossible to reconstruct and read the information. Records and protected health information cannot be disposed of in the garbage containers without some type of shredding or obliteration. Documents awaiting destruction should be housed in secure collection containers, with specific attention to location of the container and the locking capabilities. Acceptable methods used today include shredding, incineration pulping and pulverization.

In addition to the records maintained for a specific retention period, there are other documents that should be destroyed after their usefulness has ended. These secondary or

incidental documents include duplicates, carbon copies, misprints, worksheets and documents containing billing statements.
On-Site: The health information management staff should oversee any shredding of documents at the facility. Cross cut shredders have a higher degree of security than strip-shred. Destruction companies do offer on-site services where trucks with industrial shredders come to the facility to perform the service. A business associate agreement with the destruction company should detail the location of the destruction, method of destruction and require proof of destruction.
Off-Site: If the records are destroyed off-site through a destruction company, a business associate agreement should detail the safeguarding practices while the PHI is in transit, time that will elapse between acquisition and destruction, method of destruction and require proof of destruction.
Note: Some states might require notification prior to destruction of health records and also might require the use of only approved destruction companies. Check specific state laws prior to setting up destruction program.

Acceptable Methods of Destruction - Electronic Records and Information:

Like paper-based records, electronically stored resident-identifiable data, such as MDS/RAI, MPI, Dietary, or other documents, must be destroyed in a manner that makes it impossible to reconstruct and read the information. Acceptable methods used today include digital sanitation and physical destruction.

Digital sanitation or overwriting is the most common, cost-effective process for destruction of data without rendering the hard drive useless. Overwriting replaces existing data on a hard drive with meaningless data in such a way that the original data cannot be recovered. (Keating, Angie Singer. “Destroying Data the DoD Way: Military Standards Help Ensure compliance for Electronic Data Security.” *Journal of AHIMA* 76, no.7 (July-August 2005): 54-55.62.)

Degaussing is another destruction method and this uses a process that erases the data by changing the magnetic alignment to random patterns that renders the previous data unrecoverable.

Physical destruction requires damaging the medium so that it is unusable in a computer and the data is no longer retrievable.

Methods of destruction and disposal should be reassessed periodically based on current technology, accepted practices, and the availability of timely and cost-effective destruction/disposal services.

If a service is used for disposal, the vendor should provide a Certificate of Destruction indicating the following:

- Computers and media that were decommissioned have been disposed of in accordance with environmental regulations, as computers and media may contain hazardous materials.
- Data stored on the decommissioned computer or media was destroyed per the previously stated method(s) prior to disposal. (AHIMA Workgroup on Electronic Health Records Management. “The Strategic Importance of Electronic Health Records Management. Appendix A: Issues in Electronic Health Records Management” *Journal of AHIMA* 75, no.9 (October 2004): web extra.)

Computer Data and Media 2

Workstations, laptops, and servers use hard drives to store a wide variety of information. PHI may be stored on a number of areas on a computer hard drive. Simply deleting these files or folders containing this information does not necessarily erase the data.

To ensure that all PHI has been removed, utility software that overwrites (digital sanitation) the entire disks drive must be used. Remember, total data destruction does not occur until the backup tapes have been overwritten.

If the computer is being redeployed internally or disposed of due to obsolescence, the utility

software 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.

If the computer is being disposed of due to damage and is not possible to run the utility to overwrite the data, then the hard drive must be removed from the computer and physically destroyed.

Other Storage Devices 2

Compact disks, diskettes and backup tapes containing PHI must be shredded, pulverized or otherwise physically destroyed before disposal.

PDAs

Any PDA or other electronic device that does not have a hard drive must be reset to factory defaults prior to reuse

Abstracting Paper Documents and Electronic Data Prior to Discharge

Unless required by state law it is not necessary to abstract paper documents or electronic data out of the record to retain on a permanent basis. The master patient index and the destruction logs(manual or electronic) contain basic demographic information and are to be retained on a permanent basis.

Destruction Logs and Witnesses

Destruction Logs: In addition to written policies and procedures on retention and destruction, it is recommended that a facility maintain documentation of the records/documents that are destroyed and the date information was destroyed. Two types of destruction logs are recommended. These logs should be maintained permanently.

1. ***Clinical Record Destruction Log*** - When clinical records are destroyed, documentation of the destruction process and individual records destroyed must be in place. There are a number of methods that can be used to document records that have been destroyed. A log is a common process used to document the resident's name and the minimal demographic information for records that are destroyed. This log should contain the following information:

    - Resident Name
    - Medical Record Number
    - Admission Date
    - Discharge Date
    - Date of Destruction
    - Method of Destruction
    - Destroyed by
    - Witness

2. ***Destruction Log for All Other Types of Documents*** - A log should be used to reference when different types of documents were destroyed, when they were destroyed and who they were destroyed by. Some examples of the elements that might be recorded in this log include:

    - Document Name
    - Facility Retention Period
    - Dates Destroyed
    - Method of Destruction

Destroyed by

- Witnesses/Authorization
- Destruction Date

Certificate of Destruction - If an off-site record storage company or destruction company destroy records, they should supply a certificate of destruction that is signed and witnessed and includes a list of the items destroyed, the date of destruction and method of destruction. The LTC facility should have a written business associate agreement with the destruction company detailing their procedures, document insurance coverage and their security measures. If the specific items destroyed are not included on the certificate, then the certificate should be linked to this information to create an audit trail. (i.e. type of record destroyed, year, box numbers, etc.) This could be as simple as filing the certificate of destruction with the destruction logs. The certificate of destruction should be maintained permanently.

Sources:

AHIMA Practice Brief, "Destruction of Patient Health Information" (updated November 2002.

Johnson, Robert J. "Information Destruction Programs: How You Can Defend Them and They Can Defend You." *In Confidence* 10:6 (June 2002), pg 3.

Mead, Kevin. "Get Serious About Paper Record Destruction." *Journal of AHIMA* 73, no.5: 58, 60.

Johnson, Robert. "The Certificate of Destruction: What It Is, What It's Not." *Journal of AHIMA* 76, no. 6 (June 2005): 54-55, 59.

Inadvertent Destruction of Records

There are two types of situations in which records could be inadvertently destroyed. The first type is natural or man-made disasters, and would include flood, fire, hurricanes, tornadoes and explosions. The second type are provider induced disasters or disasters caused by negligence. Some examples of provider induced disasters are records destroyed by water due to storing the records on the floor, medical records lost or destroyed by computers or records inadvertently thrown away/destroyed.

If records are destroyed in either of the above situations, a risk assessment investigation should be conducted and documented as part of the Quality Assurance Committee which includes information about what caused the destruction and an action plan. See Section 4.8.2 (lost records)

If records requested by The Centers for Medicare & Medicaid Services (CMS) have been destroyed, then there is a procedure established to determine if the circumstances of the destruction was unforeseen and should not count as a "no documentation error". Refer to the CMS web site for additional information and instructions. (e.g. the *MLN Matters* article: The Comprehensive Error Rate Testing (CERT) Process for Handling a Provider's Allegation of Medical Record Destruction #SE0547)

Also check for state specific requirements for handling lost or destroyed records.
