Destruction of Patient Health Information (2000 update)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Editor's note: The following information supplants information contained in the January 1996 "Destruction of Patient Health Information" practice brief.

Background

Due to storage and fiscal restraints, most healthcare facilities are unable to maintain individual patient health information indefinitely. Consequently, these organizations find it necessary to develop and implement retention schedules and destruction policies and procedures. (See also AHIMA's Practice Brief "Retention of Health Information (Updated)" in the June 1999 *Journal of AHIMA*.)

Recommendations

Destruction of patient health information by a healthcare facility shall be carried out in accordance with federal and state law and pursuant to a proper written retention schedule and destruction policy approved by the health information manager, chief executive officer, medical staff, malpractice insurer, and legal counsel. Records involved in any open investigation, audit, or litigation should not be destroyed. Some states require creation of an abstract, notification of patients, or specify the method of destruction. In the absence of any state law to the contrary, AHIMA recommends the following:

- Destroy the records so there is no possibility of reconstruction of information. - Appropriate methods for destroying paper records include burning, shredding, pulping, and pulverizing. - Methods for destroying microfilm or microfiche include recycling and pulverizing. - The laser disks used in write once-read many (WORM) document imaging applications cannot be altered or reused, making pulverization an appropriate means of destruction. - The preferred method for destroying computerized data is magnetic degaussing. (Data are stored in magnetic media by making very small areas called magnetic domains change their magnetic alignment to be in the direction of an applied magnetic field. Degaussing leaves the domains in random patterns with no preference to orientation, rendering previous data unrecoverable.) Proper degaussing ensures that there is insufficient magnetic remanence to reconstruct the data. Overwriting can also be used to destroy computerized data. (To overwrite, cover the data with a pattern, its complement, and then another pattern, e.g., 00110101, followed by 11001010, and then 10010111.) In theory, however, files that have been overwritten as many as six times can be recovered. Total data destruction does not occur until the original data and all backup information have been destroyed. - Although magnetic tapes can be overwritten, it's a time-consuming process and there can be areas on a tape that are unresponsive to overwriting. Degaussing is considered preferable.
- Document the destruction, including: - date and method of destruction - description of the disposed records - inclusive dates covered - a statement that the records were destroyed in the normal course of business - the signatures of the individuals supervising and witnessing the destruction
- Maintain destruction documents permanently. (Such certificates may be required as evidence to show records were destroyed in the regular course of business. If facilities fail to apply destruction policies uniformly or if destruction is contrary to policy, courts may allow a jury to infer in a negligence suit that were the records available, they would show the facility acted improperly in treating the patient. See "Sample Certificate of Destruction" [below]
- If destruction services are contracted, the contract must provide that the business partner will: - not use or further disclose the information in a manner that would violate federal or state law - not use or further disclose the information other than as permitted or required by the contract - use appropriate safeguards to prevent use or disclosure of the information other than as provided for in the contract - report to the covered entity any use or disclosure of the information of which it becomes aware that is not provided for in the contract - ensure that any subcontractors or

agents to whom it provides the health information agree to the same restrictions and conditions that apply to the business partner with respect to such information - make its internal practices, books, and records relating to the use and disclosure of the information available to the secretary of Health and Human Services - destroy all protected health information and retain no copies of such information - indemnify the healthcare facility from loss due to unauthorized disclosure - provide proof of destruction - authorize termination of the contract if the healthcare facility determines that the business partner has violated a material term of the contract In addition, the contract should: - specify the method of destruction - specify the time that will elapse between acquisition and destruction of data

- Reassess the method of destruction annually, based on current technology, accepted practices, and availability of timely and cost-effective destruction services.

Note: The Department of Defense has published "A Guide to Understanding Data Remanence in Automated Information Systems." This document, available on the Web, can serve as a valuable primer and reference when establishing computerized data destruction methodologies.

References

Department of Defense. "A Guide to Understanding Data Remanence in Automated Information Systems," September 1991, version 2. Available at www.radium.ncsc.mil/tpep/library/rainbow/index.html. Department of Health and Human Services. "45 CFR, Parts 160 through 164 Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, November 3, 1999." Available at www.access.gpo.gov/nara/cfr/index.html.

Prepared by

Gwen Hughes, RHIA
Professional Practice Division

Acknowledgments

Assistance from the following reviewers is gratefully acknowledged:
Jill Callahan Dennis, JD, RHIA
Kelly McLendon, RHIA

Sample Certificate of Destruction

Facility Name

The information described below was destroyed in the normal course of business pursuant to a proper retention schedule and destruction policies and procedures.

Date of destruction:_____ Description of records or record series disposed of: _____
_____
_____ Inclusive dates covered:_____ Method of destruction: ( ) Burning ( ) Shredding ( ) Pulping ( ) Demagnetizing ( ) Overwriting ( ) Pulverizing ( ) Other:_____ Records destroyed by:_____ Witness signature:_____ Department manager:_____

Note: This sample form is provided for discussion purposes only. It is not intended for use without advice of legal counsel.
