Destruction of Patient Health Information (2002 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 replaces information contained in earlier versions of the Practice Brief, last published in the November/December 2001 Journal of AHIMA.

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)" available at www.ahima.org.)

Federal Requirements

Under the HIPAA privacy rule (42 CFR, Parts 160 and164), when destruction services are outsourced, the contract must include certain elements. Those contract elements are summarized in AHIMA's Practice Brief, "Letters of Agreement/Contracts," which is available in the June 2001 *Journal of AHIMA* and on AHIMA's Web site at www.ahima.org.

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:

- 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 back-up information have been destroyed.[1]
    - Although magnetic tapes can be overwritten, it's time consuming and there can be areas on a tape that are unresponsive to overwriting. Degaussing is considered preferable.
- Document the destruction, including:
    - date of destruction

    - 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. When facilities fail to apply destruction policies uniformly or where destruction is contrary to policy, courts may allow a jury to infer in a negligence suit that if records were available, they would show the facility acted improperly in treating the patient.)
- If destruction services are contracted, the contract must meet the requirements of the HIPAA privacy rule.

In addition, the contract should

- indemnify the healthcare facility 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

It should also specify the:

- method of destruction
- 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.

Sample Certificate of Destruction

Note

[1]The National Computer Security Center has published *A Guide to Understanding Data Remanence in Automated Information Systems* (version 2, September 2001). This document is available at www.fas.org/irp/nsa/rainbow/tg025-2.htm and can serve as a valuable primer and reference when establishing computerized data destruction methodologies.

References

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 67, no. 157 (August 14, 2002). Available at http://aspe.hhs.gov/admnsimp/.

Prepared by

Gwen Hughes, RHIA, HIM practice manager

Acknowledgments

Jill Burrington-Brown, MS, RIA
Jill Callahan Dennis, JD, RIA
Kelly McLendon, RIA

Source: AHIMA Practice Brief, "Destruction of Patient Health Information" (Updated November 2002)