Destruction of Patient Health Information (2001 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: An updated version of this practice brief, incorporating the final changes to the Privacy Rule published in the Federal Register *on 8/14/02, is available.*

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* or online in the AHIMA Library in the Communities of Practice at www.ahima.org.)

Federal Requirements

Under the HIPAA privacy rule, if destruction services are contracted, the contract must provide that the business associate will establish the permitted and required uses and disclosures of information by the business associate. The contract may not authorize the business associate to use or further disclose protected health information in a manner that would violate the requirements if done by the covered entity, except that:

- the contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, to carry out its legal responsibilities; and
- the contract may permit the business associate to provide data aggregation services relating to the healthcare operations of the covered entity

The contract must also provide that the business associate will:

- not use or further disclose the information other than as permitted or required by the contract, or as required by law
- use appropriate safeguards to prevent use or disclosure of information other than as provided for by its contract
- report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware
- ensure that any agents, including a subcontractor to whom it provides protected health information received from or created or received by the business associate on behalf of covered entity, agree to the same restrictions and conditions that apply to the business associate with respect to such information
- make available protected health information in accordance with section 164.526
- make available protected health information for amendment and incorporate any amendments to protected health information in accordance with 164.526
- make available the information required to provide an accounting of disclosures in accordance with 164.528
- make its internal practices, books, and records related to the use and disclosure of protected health information received from or created or received by the business associate on behalf of the covered entity available to the secretary for the purpose of determining the covered entity's compliance with this subpart
- at termination of the contract, if feasible, return or destroy all protected health information received from or created or received by the business associate on behalf of the covered entity that the business associate still maintains in any form and retain no copies of such information. Or if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible

The contract must authorize the covered entity to terminate the contract if the covered entity determines that the business associate has violated a material term of the contract.

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 is 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 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. If 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. See “Sample Certificate of Destruction,” below.)
    - 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 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

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.

References

National Computer Security Center. "A Guide to Understanding Data Remanence in Automated Information Systems." September 1991, version 2. Available at www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-025.2.pdf.

"Standards for the Privacy of Individually Identifiable Health Information." 45 CFR Parts 160 through 164. Federal Register 65, no. 250 (December 28, 2000). Available at http://aspe.hhs.gov/admnsimp/.

Prepared by

Gwen Hughes, RHIA

Acknowledgments

Jill Callahan Dennis, JD, RHIA

Kelly McLendon, RHIA