Documenting Data Loss: Losses Must Be Documented Just Like Other Business Activities

Save to myBoK

by **Sandra Nunn** , MA, RHIA, CHP

Good faith information management practices are an important form of compliance with the Federal Rules of Civil Procedure, the regulations issued in December 2006 that in part govern e-discovery in federal courts. Organizations responding to the regulations are in the midst of creating policies, procedures, and employee training programs that demonstrate good faith practices regarding record creation, management, retrieval, and destruction.

E-discovery teams are rushing to establish duty to preserve lessons, retention schedules, and metadata management practices. Policies are growing around how to apply legal holds, how to decommission legacy information systems, when to allow electronic health records to expire, and what constitutes a record when it is generated from new technologies such as e-mail and instant messaging.

However, one of the most slippery good faith practices to implement revolves around documenting data losses as a routine part of business activities. Although the majority of data losses are no one's fault, there is a sense of guilt or finger-pointing around these losses that inhibits the practice of routinely documenting their occurrence and retaining that documentation as a part of good faith practice.

Documenting data losses can safeguard the organization against the perception in future litigation that files were deliberately destroyed during periods deemed to be sensitive to the case at hand.

Defining Data Loss

To begin, organizations must first define data loss and establish what distinguishes it from a record loss.

Data are the collection of elements on a given subject; the raw facts and figures expressed in text, numbers, symbols, and images; facts, ideas, or concepts that can be captured, communicated, and processed either manually or electronically.[1]

Data and information are not synonymous. **Information** is data that have been organized and processed into meaningful form either manually or by computer to make them valuable to the user. Information adds to the representation and tells the recipient something that was not known before.[2]

A **record** is recorded information, the content of which requires protection, retention, and control, regardless of medium or characteristic. A record must be kept in a form that can be retrieved on demand.[3]

How Lost Are They?

In this electronic era, lost data or a lost record may not really be lost; with enough effort they may be recoverable. Therefore, in addition to defining what is lost, an organization must define degrees of loss. Presbyterian Healthcare's enterprise records management e-discovery subcommittee developed the following definitions for the organization's use:

- A **lost record** is any record or data set that cannot be located in the expected or anticipated data source or location (written or electronic) using the usual and customary search methods currently available in the organization and without using any forensic retrieval.
- A **currently inaccessible record** is any record or data set that cannot be restored to a readable format that is substantially the same as the format in which the data was originally recorded or where the unique data within the

record cannot be extracted in any readable format using the usual and customary methods currently available in the organization and without using any forensic retrieval.

- An **irrecoverable record or data set** is a record that is believed to have existed but that cannot be located or restored to a format substantially similar to the format in which the record or data set was originally collected, or any record or data set where the unique data within the record cannot be extracted or located through any means, including through the use of forensic retrieval.

Forensic retrieval is the use of specialized resources, outside the usual and customary methods currently available, either internal or external, to retrieve or restore otherwise lost or currently inaccessible records or data for the purpose of locating, extracting, or recreating a record or data to a format that is either readable or substantially similar to the format in which the record or data was originally recorded.

Outlining Data Loss Policies

Organizations must then create a policy to reflect a good faith posture of documenting and retaining the documentation of data and record losses. An accompanying procedure must be created to carry out the intent of the policy.

The policy must list the accountable parties who will carry out the documentation of data and record losses and who will submit such documentation to an archive for future reference if the organization must explain data gaps or losses in EHRs or other data- and record-generating systems.

A policy statement might read, “It is the policy of Feel Better Healthcare to record any data and/or record losses and the efforts taken to recover such lost data and/or records as part of the normal course of doing business at FBH.”

Each organization must determine how it will identify data and record losses, who will initiate the effort and expense to recover data or records, and who will document these efforts.

Reporting Data Loss

When data loss is discovered it must be reported to the organization’s security officer no matter who in the organization discovers it. Clinical or HIM employees would be most likely to discover a data loss if all or part of a group of electronic health records disappeared from the system. Organizations must document the training involved to get organizational employees to report such losses correctly, just as they have been trained to do in the case of incident reports.

Organizations must create a template to report a data or record loss. Ideally each of these reports will be numbered, entered into a system not unlike an IT service or help desk, and flagged for attention to the identified IT custodian of the particular system from which the data or record loss occurred. If the data or record cannot be recovered at the technician level, the loss then needs to be reported up to IT security and legal services.

It is at this senior level that a determination must be made about the criticality of the lost data or records and the amount of effort or expense deemed appropriate to begin additional recovery efforts. If the loss is thought to be mission critical, external help, including forensic retrieval experts, may be enlisted to try to find the data or record. All of these efforts must be documented along the way in the template.

The organization must document the loss of irrecoverable data or records. These completed templates must then be authenticated by senior IT, clinical, business, and legal services leaders.

Organizational leadership then must determine where data loss documentation should be archived. If the organization is fortunate enough to have a content management system, taxonomical categories can be created to tag the data loss reports into groups that can be recalled through the attachment of metadata to each file. Metadata might indicate date of loss, application in which the loss occurred, and data owner. Otherwise, an archive could be developed in a legal services system, in a dedicated IT application, or on a general records management site.

The most critical aspects of data loss documentation are that all steps are followed consistently by all data owners and that reporting is encouraged by senior leadership and supported by the CIO, security officer, and the general records manager.

Notes

1. Abdelhak, Mervat, et al. *Health Information: Management of a Strategic Resource*, 3rd Edition. New York, NY: Saunders, 2007.
2. National Archives and Records Administration. The Federal Records Act of 1950. 44 USC Chapter 21.
3. Ibid.

Sandra Nunn (snunn@phs.org) is enterprise records manager at Presbyterian Healthcare Services in Albuquerque, NM.

Article citation:
Nunn, Sandra L.. "Documenting Data Loss: Losses Must Be Documented Just Like Other Business Activities" *Journal of AHIMA* 80, no.7 (July 2009): 54-55.