Sequestering EHR Data in IT Systems

Save to myBoK

by **William Miaoulis**

There can be three situations under which healthcare organizations may need to sequester (or segregate) certain data within a medical record: placing a legal hold in connection with litigation, limiting disclosures of a record pursuant to a request by a patient, and restricting access to sensitive information.

Once an organization establishes its policies on medical record restriction, it must understand its computer systems' abilities to handle the various requests. Each situation is unique and requires different IT solutions to meet organizational privacy and security policies.

While most IT systems allow for some level of restriction or sequestering of data, exactly what can be sequestered and how that can be accomplished depend on the organization's computer systems.

Preparing for Litigation

Once an organization is party to litigation, it has a duty to preserve evidence. In the old days, when the media for patient health information was entirely paper, HIM professionals would simply lock the chart in a filing cabinet, controlling access and ensuring no alterations of the record occurred during the course of the litigation. Now in the age of the digital record, information is readily accessible and easily changed. However, the Federal Rules of Civil Procedure explicitly extend the duty to preserve evidence to electronically stored information, including electronic health records.[1]

Assuming that an organization has identified the appropriate electronic information subject to litigation, it is possible to create a segregated database to ensure proper retention, protection, categorization, and retrieval. However, it can be very difficult to manage.

Patient data may reside in many systems from e-mail to clinical systems to spreadsheets on thumb drives. Tools are available to search through data to find specific documents that might be relevant to a subpoena. However, organizations that do not do this properly may give the impression to the court that they should have had it or may have lost or destroyed information.

Organizations should assign an individual or department (typically the legal department) to search for and then store the necessary information. It is important to show how the information was obtained, its original file format, and its chain of custody.

Software tools can assist organizations with tagging appropriate documents, eliminating duplicates, and tagging privileged information. These tools can assist in the process; however, it is important that organizations seek legal advice early. Organizations may write their own e-discovery tools, but they must be able to show the court that the tool is able to do a thorough job. If an organization writes its own scripts to search e-mail, the script may miss documents that a reliable tool would find.

Another possible solution is to use an outside vendor to search, categorize, and store documents. These types of vendors are typically trained in the use of tools and e-discovery requirements. However, organizations that outsource duties to vendors are responsible for fully researching the vendors and their qualifications.

Handling Patient Requests

With the promulgation of the HIPAA privacy regulations, individuals have the right to request that a covered entity restrict uses or disclosures of their protected health information in order to carry out treatment, payment, or operations or those disclosures made to other individuals involved in a patient's care.[2] In a typical request, an individual may ask that a specific healthcare provider or other staff member of the covered entity not be allowed to see the individual's record or portion of a record.

The covered entity has the right to decline the individual's request for a restriction, but there are legitimate reasons for the entity to want to honor the request. For example, the entity may want to keep providers involved in a malpractice case from looking at a plaintiff patient's records. It can be difficult for IT systems to fully sequester the data or restrict access by a specific user.

Access control and identity management systems are important to authenticate user access to specific healthcare systems, but they offer only some degree of functionality in limiting an individual's access within a specific application system from viewing a specific patient record. Most healthcare vendor IT systems can be configured to limit access to patient information by location, patient, or by unit. For example, restrictions may prevent a nurse on one floor from viewing the medical records of patients on another floor.

Even though most vendor IT software allows some level of restriction, many functions such as pharmacy, radiology, and business office need access to a wide range of patients. In the future, systems may evolve to allow individual user-specific limits to be applied to a specific patient record, so that a user can look at all patients that enter into the ED except for one.

Within larger integrated delivery networks, organizations can minimally limit access to one hospital. Another major restriction allows physicians and their staffs to view only their own patients. When possible, this is typically accomplished by tying the physician's relationship to the patient record. This is very important when organizations give access to physician practices and their employees. Without this control, organizations can risk giving these users greater access with less control than organizations have over their internal work force.

In reality many hospitals do not want to put an absolute hold on accessing patient information by area because staff often move between areas. Since many functions such as billing and pharmacy require access to all patients, many organizations rely on a combination of front-end access control, training, audit log review, and sanction processes to ensure appropriate access.

Triggering Audit Controls

Many systems allow for the use of confidential flags that trigger audit trail control and review. Although audit controls do not prevent inappropriate access to information, they can detect it. The effective use of audit controls can prove important in documenting who may have accessed information. Audit trails play a key role in proving that sequestered data were not compromised.

Even when a covered entity establishes restricted access, it must make provisions for emergency access. Such access and disclosure for treatment purposes is permitted under HIPAA and is prudent from a malpractice liability standpoint.[3]

An example is a so-called "break the glass" provision that allows access to confidential patient information in an emergency. A physician who does not have a previous relationship with the patient can enter a record by "breaking the glass," which triggers an audit trail documenting the event. A review process can ensure that the access was appropriate.

Restricting Access to Sensitive Data

A lead physician researcher in the early days of HIV/AIDS diagnoses once noted that HIV/AIDS is a disease, just like cancer, and that *all* health information is sensitive and should be protected. Still, many organizations may want to sequester other data, such as records related to mental illness, substance abuse, genetics, or adoption. Indeed, HIPAA privacy regulations contemplate that in some circumstances state law may afford certain information additional protections.[4] In such cases, a system may need to segregate such specially protected information to ensure there is no inappropriate use or disclosure.

Much of an organization's ability to sequester this type of data depends on its clinical software that maintains the information and how the information can be restricted. Clearly an organization can create a special hospital or unit and limit who has access to that area using the access controls within the application system. Most systems also allow individual records to be marked confidential. Within an application system, the ability to restrict certain fields is not widely used with regard to individual patients. However, this ability is typically used to restrict specific diagnosis or identity information from being provided.

When using such a system it is often important to allow access when needed. This break-the-glass process allows a user to receive a warning prior to accessing the information. Once this seal is broken, the system logs what information is accessed and by whom, thus allowing the organization to audit the access to ensure it was appropriate.

Notes

1. Federal Rules of Civil Procedure. Rules 26(a)(1), 33, and 34. Each state has unique procedural rules governing lawsuits brought in state courts, which requires organizations to confirm which rules are applicable to any particular case.
2. HIPAA. Public law 104-191. 45 CFR § 164.522(a)(1)(i). Available online at http://aspe.hhs.gov/admnsimp/pl104191.htm.
3. HIPAA. 45 CFR § 164.522(a)(1)(iv).
4. HIPAA. 45 CFR § 160.203.

William Miaoulis (wmiaoulis@phoenixhealth.com) is a subject matter specialist for Phoenix Health Systems in Montgomery, AL.

Article citation:
Miaoulis, William M. "Sequestering EHR Data in IT Systems" *Journal of AHIMA* 80, no.5 (May 2009): 50-51.