Managing Audit Trails

Save to myBoK

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

Audit trails are records with retention requirements, and HIM professionals should include them in their management of electronic health record content. Legal and compliance needs drive audit trail management, but it is complicated by the challenges that IT departments face in storing these large volumes of data.

Audit Trails versus Audit Controls

Fundamentals of Law for Health Informatics and Information Management defines an audit trail as a "record that shows who has accessed a computer system, when it was accessed, and what operations were performed."[1] This definition spells out the most common audit trail function: access management.

Other audit trail uses include tracking employee behavior, pinpointing computer failure sites and times to allow for data reconstruction, reviewing the capability and capacity of a system or group of systems to carry out their functions (e.g., overload detection), and scanning for external intrusions of those unauthorized to enter organizational databases.

IS professionals have a somewhat different perspective and use the term *audit controls* in addition to audit trails. Audit controls are defined as "the mechanisms employed to record and examine system activity. The data collected and potentially used to facilitate a security audit is called the audit trail that in turn may consist of several audit files located on different entities of a network."[2]

This distinction is important because it may take several different systems' audit trails to detect inappropriate access or dangerous intrusions into clinical databases. It is assumed that the audit trail developed to monitor access to the primary EHR application may be the only one required to monitor inappropriate behavior. However, in reality it may require feedback from several systems.

Audit Trail Uses

HIM professionals are most familiar with audit trails that monitor appropriate role-based access to the EHR including use of the minimum necessary amount of protected health information (PHI) to get an employment-related task accomplished. Other common tasks include electronic oversight of the use of electronic documentation and electronic signature functionality in the EHR. HIM directors must consider carefully who can and cannot document and authenticate in the EHR, but they may need audit trails to ensure those restrictions are carried out.

In addition to the privileges granted to create and authenticate in the EHR, audit trails can also be used to monitor the import of PHI from external entities into an organization's EHR. These trails may make it possible to rely on the integrity of the records in health information exchanges and the data fed into personal health records.

Audit trails can also be built to monitor the modification, viewing, and deletion of information. For example, a healthcare entity's security officer could create policy, with organizational approval, to search access to:

- PHI by anyone not directly related to the patient's treatment, payment, or healthcare
- Information not corresponding to the role of the user
- PHI of VIPs or community figures
- Records that have not been accessed in a long time
- An employee's PHI
- PHI of a terminated employee
- Sensitive records such as psychiatric records[3]

In addition to auditing PHI access, trails can be used to ensure checks and balances for financial transactions and to inquire into the access of other types of sensitive information, including salary and credit card information. Human resources may choose to have audit trails attached to their HR staff to review their access to employee electronic records, including viewing employee drug testing information.

The Audit Trail as a Record

Without context, audit trails have little value. The name of the involved user, the application triggering the event, the workstation where the event happened, and a description of the event (e.g., modification, deletion, etc.) must be captured.

Audit trail records require a retention schedule just like records generated from other applications. The retention schedule for audit trail records must adhere to legal and compliance needs, but it must also take into consideration records management and IS needs.

HIM professionals must manage the audit trails within an EHR system. EHR audit trail records come under the purview of the HIM director, who is generally the legal custodian of the electronic health record. The custodian must ensure that the audit trail records for those systems contributing to the EHR contain adequate metadata. This will ensure identification and isolate violations.

In addition, HIM must make sure that audit trail records are retained for an adequate time to comply with HIPAA investigations, HR questions, or other types of requirements. For example, under the new American Recovery and Reinvestment Act (ARRA), "meaningful use" of EHRs must be established in order for healthcare entities to qualify for government funds intended for EHR implementations. A well-developed audit trail function could provide the necessary data to support an organization's case for meaningful use of its EHR.

An Acceptable Level of Risk

In response to HIPAA's privacy and security requirements, most covered entities determined that a gap analysis was a good initial step. After gap analysis revelations, they determined what risk each could sustain, including what measures they would or would not implement based on cost and IS resources.

With HIPAA audits now occurring around the country resulting in judgments of substantial fines, organizations may well be willing to sustain less risk and turn on long-dormant audit trails for, at the very least, their clinical applications. However, covered entities now need to consider what other laws, regulations, and rules may require audit trail records as part of routine inquiries.

The December 2006 amendment to the Federal Rules of Civil Procedure introduces the rules by which the federal government will conduct its legal affairs in an electronic environment. Greater leniency will be granted to those healthcare entities who manage their information with "good faith practices." A foundation of sound, well-constructed audit trails with actionable results will go a long way in the demonstration of good faith practices.

The advent of ARRA closes a number of loopholes in the HIPAA regulations and makes breaching patient information considerably more expensive and public. Audit trail records will be an important venue to help ascertain the potential sources of breached patient information.

Retention and Storage of Audit Trails

Access to audit trail records must be strictly controlled to ensure the integrity of the records. HIM professionals must first ensure that all audit trails associated with the EHR are turned on and fully functional. The functionality of audit trials associated with the EHR must be tested just as the electronic health record functions should be tested prior to implementation.

HIM must work with IS to develop test scenarios to check audit trail functionality. The numbers of those with security clearance for EHR audit trail record reviews should be quite small. Policy should determine what course will be taken if there is any evidence of modification of audit trail information.

Upon investigating the retention and management of audit trails associated with their EHR system, HIM professionals may be surprised to learn that audit trail systems are not active or that records created from such systems are retained for only short periods of time. There are very reasonable causes for these situations, including the cost of storing large numbers of records that will be accessed infrequently and the difficulty of prioritizing the retention of this type of record in the context of retaining other more important records including the EHR itself.

Hopefully HIM professionals are hard at work on the construction of organizational retention schedules that will help IS staff determine how long records must be stored prior to deletion. Many IS departments are looking at tiered storage; that is, "some data will only be retained for a few days and may be on-line for rapid access for a short period (e.g., 14 days) and then archived off-line for an extended period (e.g., 2 years)."[4]

With the increased visibility of audit trail records as discoverable information, HIM must team with IS to ensure fully functional audit trail documentation capable of restoration from archival media for the retention times determined by law and organizational risk tolerance. HIM professionals can help IS manage what may be long-term retention periods for these voluminous, critical records.

Notes

1. Brodnik, Melanie, et al. *Fundamentals of Law for Health Informatics and Information Management*. Chicago, IL: AHIMA, 2009, 215.
2. Joint NEMA/COCIR/JIRA Security and Privacy Committee. "Security and Privacy Auditing in Health Care Information Technology." November 2001. Available online at www.medicalimaging.org/documents/Security_and_Privacy_Auditing_In_Health_Care_Information_Technology-November_2001.pdf.
3. Ibid, page 3.
4. Ibid, page 5.

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

Article citation:
Nunn, Sandra L.. "Managing Audit Trails" *Journal of AHIMA* 80, no.9 (September 2009): 44-45.