Access Audit Trails: En Route to Security

by Aviva M. Halpert, MA, RHIA

An electronic access audit trail can be an effective security tool if the right conditions are in place. In this article, learn how to ensure that your organization has the right technology, procedures, mechanisms, and plans to implement an audit trail.

Working with healthcare information today is a balancing act. Providers want instantaneous access to patient information. But patients want their information—and their privacy—to be kept intact. With technology continuing to change and privacy advocates becoming more vocal, can there be a compromise?

Possibly. The healthcare community at large—physicians in particular—is increasingly adopting a position that allows unfettered access to a well-defined and vetted user group that has been schooled in the proper way to handle confidential information. Such a compromise can be made effective by using an access audit trail.

How can this seemingly simple solution be implemented? In this article, we'll look at four conditions that must exist for access audit trails to be effective.

To Access or Not to Access?

In the ideal information access model, an organization's access policies are carefully delineated and users are authorized to access information according to their defined job categories. Individual providers are trained in the proper use of patient information systems and the importance of maintaining patient confidentiality. Each user is then required to sign a confidentiality statement that includes a pledge not to share his/her logon ID or password with anyone under any circumstances.

Actual access is then monitored on an ongoing basis, and those who do not abide by the institution's policies face sanction up to and including termination. This system allows providers to rapidly access information during unforeseeable situations, but curtails inappropriate access through close scrutiny and justice that is rendered swiftly, but equally, to all offenders.

The key to this system is the access audit trail, which tracks every instance of data access, whether for data entry, correction, or retrieval. In New York state, the audit trail's use was mandated by a 1998 amendment to the state health code; nationally, it has been proposed in HIPAA and implied in the revised Medicare Conditions of Participation issued in August 1999.

Implementing an audit trail requires adequate technology, effective procedures, mechanisms to enforce the procedures, and a plan for use of the information generated. If an organization fails in any of these areas, its audit trail is useless.

Time-sensitive Technology

To create an access audit trail, an information system must be able to log every instance of data access by time and access point. It must also be able tie the event to an individual user. Before Y2K, most commercial packages on the market did not have this capability. Although the majority of products then in existence could time and date transactions and some could identify the terminal of origin, very few could document all the components of all transactions, i.e., date, time, logon ID, and terminal of origin, for every access event. Now that Y2K is over, more vendors are addressing this issue, although appropriate modifications to add this feature to existing systems can be quite extensive.

Foolproof Procedures

Even if new systems have access audit capability, individual users can be tracked by location only if they can be identified. To use such utilities effectively, organizations should:

- create a strict system of logon IDs, in which each user is assigned a unique logon ID tied to a predetermined user profile, which is known to and kept on file by the system administrator
- implement a foolproof system for authorizing and terminating access expeditiously. In particular, the system should be able to immediately identify system misuse by individuals who have never been authorized access or who have been terminated from the system
- establish a high comfort level that unique identifiers truly represent their owners' activity. To that end, establish strict penalties for sharing logon IDs and publicize and enforce them

The Long Arm of the Law: Enforcing Procedures

How can these policies be enforced? To ensure compliance, an organization should:

- **prohibit sharing logon IDs.** To enforce one user/one logon ID policies, it is critical to be just as stringent in enforcing the rules when breaches occur for management or physician convenience as when breaches occur for employee convenience. For example, do not issue temporary and group logon IDs during start-up periods or unusual situations. Make sure emergency IDs can be created during all hours of system operation, even if that means running a 24-hour help desk. Try to anticipate potentially difficult situations and agree on realistic solutions before they arise, to avoid compromising strict access policies. For instance, you might consider the need for one-time access for a changing roster of outside reviewers, enabling temporary employees to start work immediately, or enabling new house staff whose credentials have been processed but who have, for some reason, encountered a delay in processing to enter orders for the patients they are treating
- **render swift, impartial justice when breaches are identified.** If sharing a logon ID is grounds for suspension, then this penalty must apply to the chief of service as well as to the entry-level file clerk. Meting out such justice requires either a strong administrative backbone or careful thought prior to developing policy. But if the policy is enforced at a high level just once, the power of the grapevine may make a second breach less likely
- **streamline authorization and termination procedures.** Unless an organization has a seamless, comprehensive electronic medical record in a completely controlled electronic environment, it is almost inevitable that local systems will spring up, each with its own system administrators. The only way to ensure that official access policies are followed is to design, implement, and monitor a standard set of access authorization and termination procedures. Such a difficult feat depends on closely tracking the emergence of such new systems, publicizing the approved authorization and termination procedures, and implementing a monitoring system to ensure that the procedures are being followed consistently

Sample Audit Trail

Medical Center Audit Report

Patient Name	Accessor Name	Job Class	Date	Time	Term ID
David	David B.	Rehab Resident	6/16/00	20:15:47	8-006
Adolph	David B.	Rehab Resident	6/6/00	12:18:30	8-006
Abraham	David B.	Rehab Resident	6/16/00	07:11:34	4-035
Lillian	David B.	Rehab Resident	6/6/00	20:40:13	8-006

Buried in Data

Audit trails produce voluminous data. For this data to be useful, it must be reported in such a way that meaningful information is readily apparent; if it is buried in thousands of lines of output, it will never be seen. Therefore, give careful thought to tailoring valid flags and alarms. Some principles to bear in mind include:

- **design reports by exception.** Exclude categories of people you would expect to find accessing certain information (e.g., psychiatric staff on a psychiatry unit)
- **use valid criteria that will pinpoint breaches.** For instance, don't track off-shift system employee access during a period when the employees are routinely authorized to work overtime
- **use sampling techniques** to select representative intervals if you plan to look at every instance of access for patients in a particular category. (If you track every access to VIP records one day a month only, knowledge of such random monitoring can be a deterrent itself.) Take care, however, to keep your sampling strategy secret, or you will invalidate your findings
- **track a variety of data elements** to monitor access from multiple perspectives. Geographic indicators will highlight inappropriate access to patient populations that are attached to a specified location. Time and date indicators will highlight inappropriate access on the part of users who work clearly defined shifts and schedules. System functionality indicators will highlight inappropriate access on the part of users with well-defined job descriptions (e.g., pharmacists should not be entering radiology orders). Diagnostic code indicators can be tailored to highlight inappropriate access to patient populations with sensitive conditions, such as HIV-related diseases

Building a Better Report

Both ad hoc and standard reports play a role in monitoring system access. Ad hoc reports are useful when tracking an individual user's activity or activity with regard to an individual patient record. Standard reports are useful for tracking all system access, as well as for monitoring data integrity by verifying compliance with documentation policies. In either instance, a report tailored for the search at hand can provide the specific information needed. To be most effective, the audit mechanism must have search capability.

A report tracking system access can be designed to list unexpected access patterns involving the various data elements discussed above. For instance, it could include the details of the access event and the logon ID of individuals who engaged in off-hours access (logon ID and time), access from an unusual location (logon ID and terminal), unauthorized access of data for special patient populations (logon ID and diagnostic code), or unusually high volume of system access (logon ID and number of accessions in a given time period).

A report monitoring data integrity by highlighting noncompliance with institutional policies could indirectly flag system breaches while addressing improper documentation. Consider a report listing all verbal orders not signed within 24 hours or all nursing admission assessments not completed within 24 hours. In addition to providing a snapshot of documentation complianc—a valuable finding itself—the report could potentially identify the following system breaches:

- verbal orders entered for a physician no longer on staff, because the system's physician default was not updated after the individual's departure. (In other words, failure to expeditiously terminate system access for a user who has resigned)
- failure to enter all admission data concurrently due to an inadequate supply of terminals and an overwhelming amount of data entry for a single clerk. (In other words, a clerical employee has been assigned to key in data for all the nurses using their logon IDs for the data entry)

Keep the Future in Mind

At this time, there are no specifications with regard to mandatory retention periods for audit trails. The current wisdom is that if an organization has a policy delineating what is reasonable and prudent and it acts accordingly, you are in compliance. In determining what is reasonable and prudent, however, consider that in the future, there may be a requirement to inform patients, upon their request, who has accessed their information and when. The information collected in access audit trails would be extremely useful in providing such data.

We have been presented with a daunting challenge. We must make our new technology flexible and open enough to provide instantaneous and simultaneous access to patient information, while implementing enough system controls to prevent that very openness from jeopardizing the equally precious privacy of patients. With some care and forethought, we can meet that challenge by designing sophisticated audit trails and implementing the right procedures to ensure that they are used as they are intended.

The Technology/Privacy Conundrum

There are two imperatives currently vying for priority in healthcare—the need to provide easy, instantaneous access to medical information to improve patient care, and the need to restrict such access to avoid compromising patient privacy. Instead of resolving the issue, technology further complicates it with very sophisticated tools that can address either issue separately but not simultaneously.

Currently, we can apply uniform standards to electronic health information, thus enabling seamless data exchange. The finalization of the Health Insurance Portability and Accountability Act's transaction and code set standards, which were expected this summer, will likely take effect in 2002. These sets comprise strict national standards for all bills to be submitted and will ultimately lead to universal provider, payer, and possibly patient identifiers as well.

At the same time, some sophisticated data security mechanisms on the market can structure system access so that, if implemented properly, access to specific data elements can be limited to a select few. The challenge is to effect a compromise that is acceptable to all—reasonable data transfer capability tempered by reasonable access limitations.

At the heart of the issue is the medical record, which provides information to enable provision of medical care (first and foremost). When the record is in electronic format, instantaneous provider access to it can potentially improve quality of care by providing up-to-the minute information. It can also save money, for example, by providing access to test results ordered by other providers and eliminating the need for unnecessary tests. The provider community is clamoring for unfettered access for all potential caregivers at all times, lest an emergency arise and lack of immediate access result in harm to the patient.

At the same time, there are many secondary uses of the record, including justification for reimbursement for care rendered, proof of delivery of quality care, documentation to argue either side in litigation, and the raw data necessary to fuel medical research. The user groups who represent these needs also want swift and unhampered access to legible but authentic documentation.

The conflict arises when allowing entry to caregivers (a group to which most patients would readily allow access if asked) brings with it unlimited access for many other individuals (including those who most patients would not grant access to their private information, if given the choice). It is fear of uncontrolled access that spurs privacy advocates to demand implementation of strict controls to preclude all access to private information, unless it meets well-defined criteria controlled by law and, absent legislation, by the patient.

Aviva Halpert *is director of clinical information resources at the Mount Sinai Hospital in New York City. Her e-mail address is aviva.halpert@mountsinai.org.*

Article citation:
Halpert, Aviva M. "Access Audit Trails: en Route to Security." *Journal of AHIMA* 71, no.8 (2000): 43-46.