Trouble with Audit Controls

Save to myBoK

by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

The 2004 Phoenix Health System/HIMSS HIPAA compliance survey indicates that providers find audit controls the most difficult of the HIPAA security standards to implement.
While it is recognized that every organization must conduct a risk analysis to determine the systems or activities that should be audited and the tools and procedures to be used, the standard offers little guidance on specifics:

> §164.312(b) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

This column offers suggestions for the who, why, what, where, when, and how of audit controls.

Who Is Responsible for Audit Controls?

Responsibility for determining what audit controls will be implemented should be a shared effort between the information security official (ISO) and executive management. The ISO is responsible for ensuring that audit controls are addressed for HIPAA compliance. The determination of what is audited, how frequently, and what actions will result is the responsibility of executive management and must be reflected in the audit control policy.

In order to make informed decisions about audit controls, executive management needs to understand the degree to which the organization is at risk, the ongoing costs, what comparable organizations are doing, what level of risk presently exists, and what the residual risk would be given various options. Reaching a decision about the most appropriate audit controls for the organization must also take into consideration executive management's position with respect to sanction policies when audit controls identify misuse, abuse, or fraudulent activities.

Audit controls consume considerable resources, requiring monitoring by the information technology staff and follow-up from supervisors, managers, and human resources personnel. Most healthcare organizations also enlist the HIM staff to provide the initial investigations into potential confidentiality breaches. Risk managers and legal counsel may also be called upon when findings suggest a potentially compensatory event.

Why Are Audit Controls Needed?

If an organization has strong access controls and authentication mechanisms, there may be questions about why audit controls are needed. Apart from the fact that they are required by HIPAA, audit controls serve four important functions:

1. Individual accountability holds users personally responsible for their actions. The fact that auditing is being performed deters users from circumventing security policies.
2. Reconstructing events after a problem has occurred helps identify the cause of the problem, extent of damage, and in some cases the ability to restore the situation as appropriate.
3. Monitoring is a more proactive function in which detection of problems can be done in real time. This includes not only a potential breach of confidentiality, but also technical problems such as disk failures, over-utilization of system resources, or network outages.
4. Intrusion detection is the process of identifying attempts to penetrate a system and gain unauthorized access. While intrusion detection is often performed to thwart external attacks, determining what internally generated events to audit can also help identify potential misuse of access privileges.

Choosing What to Audit

Most healthcare organizations are struggling with the question of what should be audited. Audit controls potentially can be applied at various levels and track various actions, producing an audit trail (or log):

- System-level controls track successful and unsuccessful log-ons, log-offs, devices used, and applications accessed.
- Application-level controls track file opening and closing; reading, editing, and deleting records or fields; and printing, faxing, or e-mailing.
- User-level controls track all commands directly initiated by the user, identification and authentication attempts, and files and resources accessed.

One reason for concern about what must be audited is that many information systems currently in use have very limited audit control capability. For example, the most minimum of controls may only be able to log that a user accessed a specific application, not what record was accessed. Other systems include controls that can identify only records where there have been entries made, not records that were merely accessed (i.e., read or viewed). The most sophisticated audit controls can identify any action (create, read, update, delete) on any field within any record, including the date and time of the action.

Organizations also worry about bogging down their networks. When audit controls are turned on in certain systems, there may be degradation of system performance. This is because current servers supporting the application may not be powerful enough to handle the additional processing load. Enhanced auditing capability may then require upgrading a server. Additionally, different applications from different vendors may not integrate audit trail data. If the current auditing capability is deemed insufficient, third-party software may need to be acquired, with the potential still existing for upgrading a server.

Many security experts recommend putting audit data on a separate server—both as a means to archive and potentially integrate the data across applications as well as to afford the data special security protections. Someone who is intent on gaining access to data or causing harm to a system could well know how to eradicate audit data if it resides on the same server as the original data.

If audit data is on a separate server, there is sufficient storage capability for it to be kept for the length of time necessary to support investigations. Experts often disagree on how long audit trail data should be kept. It is a good idea to decide this up front in the risk analysis and incorporate the retention period in policy.

When and How Should Audit Trails Be Reviewed?

Audit trails can be reviewed after an event has occurred, when an event is suspected to have occurred, periodically, or in real time.

Healthcare organizations have typically used audit controls in an ad-hoc, case-by-case manner. Sometimes audit controls are only turned on when there is a suspected problem. Unfortunately, this may be too late—as the misuse, abuse, or fraudulent activity could have been an isolated event, or a regular user may recognize the change in system performance and curtail inappropriate behavior.

Randomly turning audit logging on and off is another option, and so is logging continuously and only reviewing logs periodically or in response to an event. Although none are ideal, the best of these solutions is continuously logging and periodically reviewing the results, especially if the organization believes its risk for problems is low, has limited resources for reviewing logs, or does not want to expend the funds for sophisticated review tools.

The ideal would be a real-time capability for alerts to trigger investigations. Healthcare organizations that believe they have significant risk for problems may want to invest in tools that support such capability.

Tools available to assist review of audit trails include:

- Audit reduction tools that can review audit trail data against predefined criteria and remove records known to have little security significance. For example, nightly backups often generate a good proportion of all accesses and could be eliminated from the review.
- Trends and variance-detection tools look for anomalies in user or system behavior, providing an alert that there may be a potential problem. For example, if a user who typically logs on between 8 and 9 a.m. appears on a log as having logged on at 2 a.m., the record would be flagged.

- Attack signature-detection tools look for a specific sequence of events indicative of an unauthorized access attempt, such as repeated failed log-in attempts.

These tools may be used for ad-hoc or periodic monitoring, although they are highly effective for real-time monitoring.

The key factors in deciding on the level of audit controls necessary for a given organization include the degree to which potential problems exist, the capabilities of current information systems, and the level of investment executive management wants to make in both implementing controls and using their results.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "The Trouble with Audit Controls." *Journal of AHIMA* 75, no.9 (October 2004): 78-79.