Security Audits (2000)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Background

Healthcare organizations have a responsibility to provide comprehensive information systems (IS) plans with provisions for privacy and security of patient information. Some security concerns can be controlled by system access functions such as using passwords, terminal restrictions, access configuration specific to job function, and module availability, but others must be addressed through administrative policy adherence where software capabilities may not reach.

Job positions with broad, random functions require employee access to at least certain portions of all patients' medical files. Without such access, employee/provider effectiveness would be significantly inhibited. For paper records, a locked file room and record request system provide control. For electronic records, access is much more difficult to control and defend.

With the advent of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) proposed regulations, organizations are under greater pressure than ever to show that their efforts are delivering the results their privacy policies intend. Protection of patient information is a patient right. Security audits offer a back-end look at system and policy effectiveness—and they are mandated by HIPAA.

Security expectations for electronic information are much the same as for paper records. With paper records, though, the evidence of inappropriate viewing can be nonexistent. The computerized audit trail of electronic file access makes tracking possible because IT systems have the capability of logging all activity. Audits trails, which are computer reports showing threads of activity occurring within the electronic system, can be used to investigate individual access patterns, either by the user or for a particular file in question.

Audit logs are reports of aggregate system activity, produced according to predetermined report parameters. Security audits use audit trails and audit logs to compare actual system activity to expected activity.

Legal and Regulatory Requirements

HIPAA proposed regulations relating to security are explicit in their scope:

- physical access control requirements include mandatory need-to-know procedures for personnel access
- information access control requires maintenance of "formal documented policies and procedures for granting different levels of access to health information"
- the access control section addresses the requirement that restricts access to resources to those who have a business need for it
- the security management process involves "creating, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches." It calls for the mandatory risk analysis and risk management features
- the internal audit section establishes a requirement "for an ongoing internal audit process, which is the in-house review of the records of system activity (example: file access)…to enable the organization to identify potential security violations"

- the audit control section states, "each organization would be required to put in place audit control mechanisms to record and examine system activity"

The basic tenets of the Privacy Act of 1974 apply to any organization. The act directs that data may only be used for the purpose for which it was collected.

Accreditation Requirements

The Joint Commission on Accreditation of Healthcare Organizations charges healthcare organizations with the responsibility of protecting records and information against loss, destruction, tampering, and unauthorized access or use in information management standard IM.2.3.

The intent for Standards IM.2-2.3 notes that an effective process defines:

- who has access to information
- the information to which an individual has access o user's obligation to keep information confidential
- when release of health information or removal of the medical record is permitted
- how information is protected against unauthorized intrusion, corruption, or damage
- the process followed when confidentiality and security are violated

Recommendations

Security audits, besides being a mechanism to address regulatory and accreditation responsibilities, are an investment in risk reduction. A confidentiality task force can be an excellent opportunity for key individuals to explore and determine a security audit procedure that protects the entire organization. Such a task force would typically include representation from HIM, risk management, human resources, quality management, the medical staff, IS, and the CIO, security officer, and internal audit and data analysis experts as appropriate.

Approach

Consider the following points when setting up a security audit protocol:

- the IS plan includes a provision for employee/provider access to electronic information based on need to know
- the IS plan optimally secures patient information through technology features and process restrictions
- the IS plan builds in strong monitoring controls and audit trails so that every transaction is recorded and logged
- the IS plan establishes security audits as a method of review to detect policy breaches where access cannot be totally controlled by technology features
- all security audits are unannounced
- department or unit leadership most familiar with job position responsibilities are directly involved in interpreting findings and determining questionable circumstances that require further investigation
- contractual agreements include provision for adherence to organizational policies for privacy and security and require participation in security audits and follow-through when breaches occur
- audits are all-inclusive: a practice of "checking the checker" is instituted whereby an individual is assigned to assess viewing access of those who are conducting the department/unit/entity audits

- breaches of policy have plenary ramifications supported by top-level administration and dealt with via the organization's established disciplinary program
- the quality management process is enhanced to enfold the security audit responsibility into each department's, unit's, or entity's performance improvement monitors

Security Audit Process

It would be prohibitive to perform security audits on every data field. Good-faith efforts to investigate the compliance level of individuals educated on privacy issues can be achieved through a well-thought-out approach.

Identify "trigger events," which are the criteria that raise awareness of questionable conditions of viewing of confidential information. Some will be appropriately applied to the whole organization, some will be department- and unit-specific. Examples include:

- users that have the same last name, address, or street name as in the patient file being viewed
- VIPs (board members, celebrities, governmental or community figures, authority figures, physician providers, management staff, or highly publicized individuals)
- patient files with isolated activity after no activity for 120 days
- employees viewing other employees' files. This should be cross-departmental as well as inter- departmental (set parameters to omit caregivers)
- diagnosis related (set parameters to omit caregivers)
- sensitive diagnoses such as psychiatric disorders, drug/alcohol problems, AIDS
- files of minors who are being treated for pregnancy or sexually transmitted diseases
- department- or unit-specific examples (brainstorm a customized approach according to function and job responsibilities):
    - nurses viewing files of patients on other units, e.g., medical/surgical nurses viewing files of patients treated only in emergency services or psychiatric services
    - transcriptionists viewing files of services or patients for whom they did not transcribe reports
    - emergency department nurses viewing files of emergency patients from shifts and days when they were not working
    - Medicare billers viewing insurance categories they do not process
- terminated employees (checks that access has been rescinded)
- employees with home access
- physicians viewing records of patients they did not treat as attending physician, consultant, or surgeon
- nonclinical staff audit (nonclinical staff viewing clinical information inappropriately)

- patient self audit (provide patients with the option of reviewing an access audit trail of their own file)
- all hits audit (a random review that checks who the user is, where they work, and if they should be accessing the file)
- focused audit (use this to investigate periodic patient or staff complaints of suspected breaches)

Sample size: When possible, use a 100 percent capture in an ongoing manner for trigger events that identify only inappropriate access. Some triggers will be unwieldy at 100 percent, so consider performing a 100 percent audit for a shorter time period. Some trigger factors will lend themselves to application within certain departments, units, or services. For triggers with expectations of large-volume logs, consider drilling down on a select number (for example, every third file until a sample of 30 is accrued).

Frequency: Security audits can encourage the swift detection of security breaches. Investigate your organization's capability of ongoing report generation for trigger factors that are expected to be infrequent to encourage immediate review and investigation. Define sporadic and random monitoring periods for triggers that are not ongoing and are more effectively reviewed for patterns one day of the week (rotate the day), one week out of the quarter, one entire month, etc. Not every trigger event needs to be audited every period. Consider rotating trigger events so that different audits are conducted each period. Include follow-up audits for those triggers previously uncovering problem areas.

Scope: The extent of the audit can likewise be varied according to department, unit, or corporate entity. A department may choose to monitor all employees viewing other employee files during one monitoring period and elect to review only third shift for another. The following elements can help to focus the scope and make it more meaningful:

- day of the week or time of day the access occurred
- where the access occurred
- number of accesses

The number of trigger factors and the breadth of the coverage chosen should be paced for reasonableness by the individuals reviewing the audit logs.

Educate, Educate, Educate

Make certain that patient rights and policies and procedures related to privacy and security are understood by all involved employees, providers, associates, and contractual partners. Inform them of the security audit practice and management support to enforce it, but do not reveal the details of the audit itself (e.g., the trigger points, timing, scope, and frequency). Include this focused training in orientation for all new employees.

Signed confidentiality statements are a mechanism of documentation showing completion of training and employee commitment to comply with expectations. Consider initiating these with completion of the initial training and renew the signature commitment each year. Some organizations find annual appraisal intervals to be the most consistent. Periodically repeat in-service education covering individual responsibility. Warning statements placed on computer sign-on screens can be an ongoing alert to remind users of audit activity practices.

Evaluating Findings

Work through management staff for deciphering pertinent report results whenever possible. As department and unit leaders, they know the job functions of their staff and, in some cases, can quickly discern need for further investigation. Formation of a computer incident response team (CIRT) can be very beneficial to assist in the investigation of abnormal audit findings. This can be the same as the confidentiality team mentioned earlier. If your organization employs a security officer, significant involvement of this individual is recommended for focused and consistent handling of all aberrant activity.

Be thorough in your investigation before confronting an individual. Even after all likely factors are exhausted, an individual may have good reason for out-of-the-ordinary access; treat the questioning as an inquiry, rather than interrogation. Consistency in

application of policy is critical; do not make exceptions. Provide for a graduated penalty process so that the punishment fits the crime. Policy should not be so rigid that it does not allow flexibility in taking action against breach activity.

The idea that individual behavior may be altered when individuals know they are being monitored, known in research circles as the Hawthorne Effect, can be most valuable. A policy allowing patient request of an audit trail would include employees treated in their place of employment. This widely known practice may discourage security breaches. Provide support for report interpretation.

Reporting Findings

Security audits constitute a monitoring practice that lends itself to performance improvement for a responsibility with high-risk potential. Security audit activities can be appropriately tied to quality improvement reporting for top-level involvement all the way to the board of directors.

Protecting and Retaining Audit Logs

To demonstrate compliance with HIPAA regulations, it is important to institute a protection and retention policy for the audit logs used and the reported findings. These are the proof that you did the study and allow you to detail the findings if necessary. HIPAA requires that security audit logs be producible and that they have not been tampered with. Know your state's statute of limitations relative to discoverability. Should you need to take disciplinary action against an employee or contracted agent, these records will also allow the facility to demonstrate consistent policy enforcement and support the defense of the disciplinary action.

References

Borten, Kate. "Using an Audit Facility to Protect Patient Data at the Massachusetts General Hospital". Presented at Toward an Electronic Patient Record, 1995.

Henenberg, Joel. "Developing a Computer Incident Response Team". In Confidence 7, no. 5 (1999).

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Hospitals.* Oakbrook Terrace, IL: 2000.

Jones, Russell L. "The Internet and Healthcare Information Systems: How Safe Will Patient Data Be?" *Information Systems Control Journal* 1, 1998.

Mead, Kevin. "An Internal Audit Model for Information Security". *In Confidence* 8, no. 4 (2000).

O'Donnell, Charles P. "Constructing Effective Audit Trails." *In Confidence* 7, no. 4 (1999).

Rhodes, Harry. "Physician Peer Review: A Response to Confidentiality Breaches." *In Confidence*, 7, no. 4 (1999).

Security and Electronic Signature Standards, 45 CFR Part 142, Proposed Rule, part iii (1998).

Prepared by

Beth Hjort, RHIA, professional practice manager, AHIMA

Acknowledgment

Harry Rhodes, MBA, RHIA

Issued September 2000
