Security Audits (2003 update)

Save to myBoK

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

Editor's note: This update supplants the September 2000 practice brief "Security Audits."

Background

Access controls are critical tools for ensuring privacy and security of electronic protected health information (PHI). They serve as gatekeepers for front-end compliance with the privacy standard of "minimum necessary" and the security principle of "need-to-know." But even with an ideal access-control plan, the complexities of the healthcare environment are unavoidable. Security audits must be performed to hold the users of information systems accountable for their actions.

Protection of individually identifiable health information is a patient right. Besides being mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), security audits offer a back-end look at system and policy effectiveness for ensuring that patient right. Audit information may also be useful as forensic data during investigations of security incidents and breaches to patient privacy.

Job positions with broad, random functions may require electronic access to at least select portions of all patients' medical files. Without such access, employee and provider effectiveness could be significantly inhibited. For paper records, a locked file room and record-request system provide control over the physical record, but these measures offer no control over what is viewed when a complete record is accessed. For electronic records, access may be controlled down to the data-item level, but it is much more difficult to control and defend when random access is required. Decisions to grant broad access should be carefully evaluated and justified.

Unlike paper records, where evidence of inappropriate viewing can be nonexistent, computerized audit logs of electronic file access make tracking possible. IT systems have the capability of logging key activities. Audit trails-computer reports showing threads of activity occurring within the electronic system-can be used to investigate individual access patterns, either by user or for a particular file.

Audit logs are records of system activity. Reports of this activity can be produced according to predetermined report parameters. Security audits use audit trails and audit logs to compare actual system activity to expected activity. It's helpful to distinguish the difference in these terms: Audit logs are records of activity maintained by the system. An audit trail consists of the log records identifying a particular transaction or event. An audit is the process of reviewing those records. An audit can be a periodic event or it can be done as a result of a patient complaint or suspicion of employee wrongdoing.

Legal and Regulatory Requirements

HIPAA security regulations directly and indirectly relating to audits include:

- Information system activity review (required)-"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." (164.308(a)(1)(ii)(c))
- Evaluation (required)-"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirements [of the Security Rule]." (164.308(a)(2)(8))
- Audit controls (required)-"Implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." (164.312(1)(b))

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

Accreditation Requirements

The 2004 Joint Commission on Accreditation of Healthcare Organizations hospital standards have been modified to be consistent with HIPAA. Standards IM.2.10 and IM.2.20 respectively address a healthcare organization's responsibility to maintain privacy and security.

IM.2.10 states, "Information privacy and confidentiality are maintained."

IM.2.20 states, "Information security including data integrity is maintained."

Elements of performance for both of these standards require written policies, an effective process for enforcing policies, monitoring policy compliance, and the use of monitoring of information to improve privacy, confidentiality, and security.

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 the privacy officer, security officer, the CIO, representation from HIM, risk management, legal affairs, human resources, quality management, the medical staff, IS, and compliance officer and internal audit and data analysis experts as appropriate.

Approach

When setting up a security audit process, consider:

- your system(s) capabilities; disparate systems may require modified audit plans
- creating screen warning banners to notify computer users that activities are being monitored and audited
- involving data owners when appropriate (often the same as department or unit leadership) to determine what activities should trigger an entry into audit trails
- having audit trails reviewed by department or unit leadership to determine appropriateness of PHI access based on workforce roles and tasks
- directly involving department or unit leadership most familiar with job responsibilities in interpreting findings and identifying questionable circumstances needing further investigation
- determining how random audits will be conducted
- obtaining human resource department involvement when a manager suspects employee wrong-doing and requests review of employee activities via an audit trail (for protection of employee rights)
- adding a provision to contractual agreements requiring adherence to privacy and security policies, cooperation in security audits, and investigation and follow-through when breaches occur
- the impact of running audit reports on system performance
- conducting occasional "check the checker" audits, whereby an individual is assigned to assess viewing access of those who are conducting the department, unit, or entity audits
- ensuring top-level administrative support for consistent application of disciplinary and plenary actions
- enhancing the quality management process to enfold 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"-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 other highly publicized individuals)
- patient files with isolated activity after no activity for 120 days
- employees viewing other employee files; this should be cross-departmental as well as interdepartmental (set parameters to omit legitimate caregiver access)
- diagnosis related (set parameters to omit caregivers)
- sensitive diagnoses such as psychiatric disorders, drug and alcohol problems, AIDS
- files of minors who are being treated for pregnancy or sexually transmitted diseases
- department- or unit-specific circumstances (brainstorm a customized approach according to function and job responsibilities):

    - nurses viewing files of patients on other units(e.g., medical and 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)
- all-hits audit (a random review that checks who users are, where they work, and if they should be accessing the file)
- focused audit (use 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 (e.g., every third file until a sample of 30 is accrued).
Frequency: Security audits can encourage the swift detection of security breaches. To encourage immediate review and investigation, examine your organization's ability to generate ongoing reports for trigger factors that are expected to be infrequent. 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, et cetera. 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 audits themselves (e.g., 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 privacy and security training and renewing the signature commitment each year. Some organizations find annual appraisal intervals to be the most consistent. Warning statements placed on network and application sign-on screens help ensure top-of-mind awareness of monitoring and audit practices for the workforce and physicians.

Evaluating Findings

It is recommended that organizations work through management staff for deciphering pertinent report results. 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 can be very beneficial in the investigation of abnormal audit findings. This team may be the same as the confidentiality team mentioned earlier. Significant involvement of the security officer is recommended for focused and consistent handling of all aberrant activity.

Be thorough in your investigation. As appropriate, get human resources, risk management, and legal counsel involved 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. Making exceptions can be dangerous, both for maintaining workforce trust and in legal defense. 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 valuable. For example, if an employee becomes a patient of the hospital in which he or she works, hospital policy may allow the employee to request an audit trail of access to his or her PHI. If this is feasible within the system, existence of the policy may discourage employees from looking at the medical information of their coworkers.

Reporting Findings

Security audits constitute a monitoring practice that lends itself to performance improvement for responsibilities with high-risk potential. Security audit activities can be appropriately tied to quality-improvement reporting for executive-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 an audit protection and retention policy. These reports detail any findings and demonstrate regulatory compliance.

Consider these important elements in creating your plan:

- storing audit logs and records on a server separate from the system that generated the audit trail
- restricting access to audit logs to prevent tampering or altering of audit data
- retaining audit trails for network activity and application activity based on a schedule determined jointly by IS and department or unit leadership

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 disciplinary action and policy enforcement.

Audit information may also be useful as forensic data during investigations of security incidents and breaches to patient privacy. A structured audit process-with strong controls, oversight, document protections, and appropriate record retention policies and procedures-will ensure that audit findings stand up to challenges of accuracy and validity.

References

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

Derhak, Mike. "Uncovering the Enemy Within: Utilizing Incident Response, Forensics." *In Confidence* 11, no. 9 (2003).

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

Joint Commission on Accreditation of Healthcare Organizations. 2004 Accreditation Standards for Hospitals. Oakbrook Terrace, IL.

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 Standards Final Rule. 45 CFR Parts 160, 162, 164. *Federal Register* 68, no. 34 (February 20, 2003).

Prepared by

Beth Hjort, RHIA, CHP, Professional Practice Manager, AHIMA

Acknowledgments

Dale Miller, CISSP, CHP
Don Mon, PhD
Carol Quinsey, RHIA
Harry Rhodes, MBA, RHIA, CHP
Tom Walsh, CISSP

Source: Hjort, Beth. "AHIMA Practice Brief: Security Audits" (Updated November 2003)