Security Audits of Electronic Health Information (2011 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 November 2003 practice brief "Security Audits (Updated)."

Introducing the AHIMA Compendium http://compendium.ahima.org [Note: the Compendium was retired in 2011]

Throughout this brief, sentences marked with the † symbol indicate AHIMA best practices in health information management. These practices are collected in the new AHIMA Compendium, offering health information management professionals "just in time" guidance as they research and address practice challenges.

In a perfect world, access controls alone would ensure the privacy of electronic protected health information (ePHI). However, the complexities of the healthcare environment today make it extremely challenging to limit worker access to the minimum information necessary to do their jobs.

For example, many jobs in smaller organizations and community-based hospitals require workers perform multiple functions. Without access to at least select portions of every patient's health record, some employees' effectiveness could be significantly inhibited and patient care could be compromised.

Organizations must develop security audits and related policies and procedures to hold workers accountable for their actions while utilizing ePHI and an electronic health record (EHR).

Security audits are conducted using audit trails and audit logs that offer a back-end view of system use. Audit trails and logs record key activities, showing system threads of access, changes, and transactions. Periodic reviews of audit logs may be useful for:

- Detecting unauthorized access to patient information
- Establishing a culture of responsibility and accountability
- Reducing the risk associated with inappropriate accesses (behavior may be altered when individuals know they are being monitored)
- Providing forensic evidence during investigations of suspected and known security incidents and breaches to patient privacy, especially if sanctions against a workforce member, business associate, or other contracted agent will be applied
- Tracking disclosures of PHI
- Responding to patient privacy concerns regarding unauthorized access by family members, friends, or others
- Evaluating the overall effectiveness of policy and user education regarding appropriate access and use of patient information (comparing actual worker activity to expected activity and discovering where additional training or education may be necessary to reduce errors)
- Detecting new threats and intrusion attempts
- Identifying potential problems
- Addressing compliance with regulatory and accreditation requirements

This practice brief identifies and defines the components necessary for a successful security audit strategy. It also outlines considerations for legal and regulatory requirements, how to evaluate and retain audit logs, and the overall audit process.

Legal and Regulatory Requirements

Many regulatory requirements drive how and why security audits are conducted. HIM professionals should consider the following legal and regulatory requirements when developing the organization's security audit strategy.

HIPAA Security Rule

The HIPAA security rule includes two provisions that require organizations perform security audits. They are:

- **Section 164.308(a)(1)(ii)(c),** Information system activity review (required), which states organizations must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."
- **Section 164.312(1)(b),** Audit controls (required), which states organizations must "implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Payment Card Industry Data Security Standard

In 2006 the five major credit card companies worked collaboratively to create a common industry standard for security known as the **Payment Card Industry Data Security Standard**. Any organization that accepts credit cards for payment may be fined or held liable for losses resulting from a compromised credit card if it lacks adequate security controls.

The standard mandates organizations implement the following audit requirements:

- Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user
- Implement automated audit trails for all system components to reconstruct the following events:
  - All individual accesses to cardholder data
  - All actions taken by any individual with root or administrative privileges
  - Access to all audit trails
  - Invalid logical access attempts
  - Use of identification and authentication mechanisms
  - Initialization of the audit logs
  - Creation and deletion of system-level objects
- Record at least the following audit trail entries for all system components for each event:
  - User identification
  - Type of event
  - Date and time
  - Success or failure indication
  - Origination of event
  - Identity or name of affected data, system component, or resource
- Secure audit trails so they cannot be altered
- Review logs for all system components at least daily
- Retain audit trail history for at least one year, with a minimum of three months' online availability

HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, also included provisions requiring organizations conduct audits. In essence, healthcare organizations and third-party payers are expected to **monitor for breaches of PHI** from both internal and external sources.

The phrase "covered entity or business associate did not know (and by exercising reasonable diligence would not have known) of a violation" implies active auditing and monitoring for PHI breaches would be expected as reasonable due diligence.

Meaningful Use

In addition, the Office of the National Coordinator's EHR certification criteria for the meaningful use program include audit requirements. Section 170.302(r), Audit log, requires the ability to:

- **Record actions.** Record actions related to electronic health information in accordance with the standard specified in §170.210(b)
- **Generate audit log.** Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at §170.210(b)

The stage 1 meaningful use criteria also point to the HIPAA security rule, stating that provisions of the rule (including audits) must be met.

The Joint Commission

The Joint Commission accredits hospitals and has two information management (IM) standards that indirectly address a healthcare organization's responsibility to maintain (monitor) privacy and security:

- **IM.2.10,** Information privacy and confidentiality are maintained
- **IM.2.20,** 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.

Audit Definitions

Audit logs are records of sequential activities maintained by the application or system.

An **audit trail** consists of the log records identifying a particular transaction or event.

An **audit** is the process of reviewing those records and an integral part of a security and risk management process.

E-Discovery

Audit log information may also be useful for **legal proceedings** such as responding to an electronic discovery, or e-discovery, request. E-discovery is the common name for the revisions to the Federal Rules of Civil Procedures, which went into effect December 1, 2006. It refers to the information that an organization could be requested and expected to produce in response to litigation.

Establishing Strategy and Process

A multidisciplinary team is essential to developing and implementing an effective security audit strategy. The team should include at a minimum IT, risk management, and HIM representation, and it should be led and managed by the organization's designated security official in coordination with the designated privacy official.[†]

In setting up strategy and process, the team should consider:

- Identifying all electronic systems and their capabilities to understand what is auditable; disparate systems may require modified audit plans.

- Creating and placing warning banners on network and application sign-on screens to notify computer users that activities are being monitored and audited to help enforce workforce awareness. For example, a warning banner may state "WARNING! Use of this system constitutes consent to security monitoring and testing. All activity is logged and identified with your user ID. There is no expectation of employee privacy while using this system."
- Involving application and system owners when appropriate to determine what user activities should trigger an entry in the audit trails.
- Having audit trails reviewed by department or unit leadership to determine the appropriateness of PHI access based on workforce roles and tasks.
- 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.
- Involving the human resources department for protection of employee rights when a manager suspects employee wrong-doing and requests review of employee activities via an audit trail.
- Developing a standard set of investigatory documents used to record potential violations and breaches, interviews, and actions taken, including reporting.
- 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.
- Evaluating the impact of running audit reports on system performance.
- Determining what audit tools will be used for automatic monitoring and reporting.
- Determining appropriate retention periods for audit logs, trails, and audit reports.
- Ensuring top-level administrative support for consistent application of policy enforcement and sanctions.

Audit information may also be useful as forensic data and valuable evidence during investigations into security incidents and privacy breaches, especially if sanctions against a workforce member, business associate, or other contracted agent will be applied.

Determining What to Audit

It would be prohibitive to perform security audits on all data collected. Good-faith efforts to investigate the compliance level of individuals educated on privacy and information security issues can be achieved through a well-planned approach.

In determining what to audit, organizations must identify and define "trigger events," or the criteria that will flag questionable access of confidential ePHI and prompt further investigation. Some triggers will be appropriate to the whole organization, while others will be specific to a department or unit. Once identified, trigger events should be reviewed on a regular basis, such as annually, and updated as needed.[†]

Examples of trigger events include employees viewing:

- The record of a patient with the same last name or address as the employee
- VIP patient records (e.g., board members, celebrities, governmental or community figures, physician providers, management staff, or other highly publicized individuals)
- The records of those involved in high-profile events in the community (e.g., motor vehicle accident, attempted homicide, etc.)
- Patient files with isolated activity after no activity for 120 days
- Other employee files across departments and within departments (organizations should set parameters to omit legitimate caregiver access)
- Records with sensitive health information such as psychiatric disorders, drug and alcohol records, domestic abuse reports, and AIDS
- Files of minors who are being treated for pregnancy or sexually transmitted diseases
- Records of patients the employee had no involvement in treating (e.g., nurses viewing patient records from other units)
- Records of terminated employees (organizations should verify that access has been rescinded)
- Portions of a record that an individual's discipline would not ordinarily have a need to access (e.g., a speech pathologist accessing a pathology report)

Those individuals who review the audit logs should evaluate the number of trigger events and the breadth of the coverage chosen as well as the system's ability to log the data desired for such reviews.

Implementing Audit Tools

Certified EHRs that meet the stage 1 meaningful use criteria will also meet health IT audit criteria and may provide enough detail to determine if there was an unauthorized access into a patient's record.

These built-in audit logs can easily contain millions of entries of application transactions. Searching through these detailed logs to find the specific information needed when conducting an investigation regarding a particular encounter can take a significant amount of time and requires some specialized skills in reading and interpreting the data.

Breaches often go undetected in manual reviews of audit logs due to the sheer volume of data. Conducting random audits of user access is like the old cliché "searching for a needle in a haystack."

To help ensure greater efficiency in audit reviews, many organizations rely on third-party audit tools, which systematically and automatically analyze data and quickly generate reports based upon search criteria matching the organization's audit strategy or defined triggers.

Specialized audit tools can be programmed to:

- Detect potentially unauthorized access to a patient's record, often using a variety of prewritten queries and reports such as a match between the user's and the patient's last names.
- Collect and automatically analyze information in-depth.
- Detect patterns of behavior.
- Provide privacy and security officers or compliance personnel with alert notifications of potential incidents or questionable behavior.
- Collect the audit logs from other applications for correlation and centralized storage and analysis. For example, the logs from a time-keeping system may be used to verify if an employee was on the clock when an unauthorized access occurred.
- Present reports in an easy-to-read Web page or dashboard.

Third-party tools can be expensive to purchase and install. Up-front costs may include audit software, server and operating system for running the software, and labor costs for installation, training, and modification. In addition, there may be annual licensing and support fees, which must be factored into an organization's operating budget.

Some vendors offer audit tools as software as a service, or SaaS. This eliminates many of the up-front costs because the vendor supplies and owns the necessary hardware and software and provides the programming support. The healthcare organization pays a monthly fee to use the tool, usually through a Web interface.

Determining When and How Often to Audit

Due to a lack of resources, organizations typically examine their audit trails only when there is a suspected problem. Although this is a common practice, it is definitely not a best practice.

It is imperative an organization's security audit strategy outlines the appropriate procedure for responding to a security incident. However, it must also define the process for the regular review of audit logs. At a minimum, review of user activities within clinical applications should be conducted monthly. It is best to review audit logs as close to real time as possible and as soon after an event occurs as can be managed.† This is especially true for audit logs, which could signal an unauthorized access or intrusion into an application or system. Automated audit tools can be helpful for providing near real-time reports.

Evaluating Audit Findings

Department managers and supervisors are in the best position to determine the appropriateness of staff access. Therefore, they should review the audit reports.

The organization's information security and privacy officials must provide education to the directors, managers, and supervisors responsible for reviewing security audit report findings so they are equipped to interpret results and determine appropriate versus inappropriate access based on defined and approved access permissions.[†]

Presenting Audit Report Findings to Employees

In the event that an audit reveals potentially unauthorized access by an employee, human resources, risk management, and legal counsel (as appropriate) may need to be involved before addressing the report findings with the employee.

Organizations should consider factors such as education, experience, privacy and security training, and barriers to learning (e.g., language) when evaluating an employee's actions. They should remember that an individual may have had a good reason for out-of-the-ordinary access, even if the initial review indicates otherwise. In addition, organizations should consider treating the questioning of an employee as an inquiry, rather than an interrogation.

Organizations must be consistent in the application of their security and privacy audit policies and sanctions with no exceptions. Making exceptions to the policy risks the trust of the workforce and consumers and poses a risk to legal defense.[†] Healthcare facilities leave themselves open to both individual and class action lawsuits when they do not have a strong, consistent enforcement program.[1]

Organizations should develop and implement graduated sanctions so that the punishment fits the incident. Sanction policies should allow management some limited flexibility. For example, sanctions to physicians and other licensed caregivers with specialized skills may negatively affect patient care and business operations if these individuals are removed from their job as a result of a violation.

In conjunction with sanction policies, organizations must develop and implement strong policies and procedures to address the processing of breaches, compliant with federal and state laws and regulations, in the event any security audit findings indicate a breach has occurred.

Protecting and Retaining Audit Logs

HIPAA requires that covered entities maintain proof that they have been conducting audits for six years. Such documents may include policies, procedures, and past audit reports. State statutes of limitations relative to discoverability and an organization's records management policies may require that this information be kept longer.

Organizations must review pertinent regulatory requirements, including applicable federal and state laws, in determining the appropriate retention period for security audit logs. Security and privacy officials should collaborate to establish the most effective schedule for the organization.[†]

The Payment Card Industry Data Security Standard requires organizations "retain audit trail history for at least one year, with a minimum of three months' online availability."

At a minimum, an organization's audit strategy must stipulate the following actions to protect and retain audit logs:

- 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 based on a schedule determined collaboratively with operational, technical, risk management, and legal staff †

Prevention through Education

The new mantra in healthcare should be, "Just because you can, doesn't mean you should." Education is a preventive measure that must be executed and re-executed to ensure optimal outcomes in the success of a security audit strategy. Organizations should:

- Ensure that patient rights such as an accounting of disclosures and policies and procedures related to privacy and security are understood by all involved employees, providers, associates, and contractual partners.

- Inform all involved employees, providers, associates, and contractual partners of the security audit practice and management support to enforce it. However, it should 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 and provide annual refresher training for current employees. 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, the existence of the policy may discourage employees from looking at the medical information of their coworkers.

Note

1. AHIMA. "Sanction Guidelines for Privacy and Security Breaches." *Journal of AHIMA* 80, no. 5 (May 2009): 57–62. Available online in the AHIMA Body of Knowledge at http://www.ahima.org.

References

AHIMA. "Building an Effective Security Audit Program to Improve and Enforce Privacy Protections." Online course. Available online at http://www.ahimastore.org.

Department of Health and Human Services. "45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule." *Federal Register* 68, no. 34 (Feb. 20, 2003). Available online at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

Prepared by

Tom Walsh, CISSP

Assisted by

William Miaoulis, CISA, CISM

Acknowledgments

2010 Privacy and Security Practice Council:
Susan W. Carey, RHIT
Angela K. Dinh, MHA, RHIA, CHPS
Gwen Jimenez, RHIA
Karen Lawler, MPS, RHIA
Monna Nabbers, MBA, RHIA
Lori Nobles, RHIA
Deanna O'Neil, RHIA, CCS
Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA
Mary H. Stanfill, MBI, RHIA, CCS, CCS-P, FAHIMA
Allison Viola, MBA, RHIA
Diana Warner, MS, RHIA, CHPS, FAHIMA
Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Prepared by (Original)

Beth Hjort, RHIA, CHP

The information contained in this practice brief reflects the consensus opinion of the professionals who developed it. It has not been validated through scientific research.

† Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium, http://compendium.ahima.org.

Article citation:
AHIMA. "Security Audits of Electronic Health Information (2011 update)." *Journal of AHIMA* 82, no.3 (March 2011): 46-50.