Privacy and Security Audits of Electronic Health Information (2013 update)

Save to myBoK

Editor's note: This update supplants the March 2011 practice brief "Security Audits of Electronic Health Information (Updated)."

In a perfect world, access controls alone would ensure the privacy and security of electronic protected health information (ePHI). However, the complexities of today's healthcare environment make it extremely challenging to limit access to the minimum information necessary that members of the workforce require to perform their jobs.

In smaller organizations and community-based hospitals, employees may perform multiple functions, each of which requires different levels of access. Without having access to specific portions of every patient's health record, employees' effectiveness could be significantly inhibited, and patient care and safety could be compromised. Organizations must develop security audits and related policies and procedures to hold members of the workforce accountable for their actions when accessing ePHI through the electronic health record (EHR).

Organizations must perform security audits 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, modifications, 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 (Note: 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 the organization's policy and user education regarding appropriate access and use of patient information (Note: This includes comparing actual workforce 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.

Audit Definitions

Audit logs are records of sequential activities that the application or system maintains.

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

An **audit** is the process of reviewing log records. It is an integral part of a security and risk management 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 healthcare organizations to 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 (American Express, MasterCard Worldwide, Visa Inc., Discover Financial Services, and JCB International) worked collaboratively to create a common industry standard for security known as the **Payment Card Industry Data Security Standard (PCI DSS).** The standard states that 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 performed with administrative privileges, such as root privileges) 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, and provide online availability for a minimum of three months

HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (and finalized in the HITECH Omnibus Rule in January 2013), also includes provisions requiring organizations to conduct audits. In essence, healthcare organizations and third-party payers are expected to monitor for breaches of PHI from both internal and external sources.

Section 164.404(a)(2) of 45 CFR Parts 160 and 164 of the *Breach Notification for Unsecured Protected Health Information; Interim Final Rule* and finalized in the HITECH Omnibus Rule, implies that organizations perform reasonable due diligence by actively auditing and monitoring for PHI breaches. Exercising this due diligence protects organizations in the event that a violation occurs, and it may help to identify violations that wouldn't have otherwise been uncovered.

Meaningful Use

EHR and electronic medical record (EMR) vendors must demonstrate that their products meet the Technical Safeguards in the HIPAA Security Rule, including audit requirements, in order to become certified through the Office of the National Coordinator (ONC).

Stage 1 of certification criteria for Meaningful Use, Section 170.302(r), Audit log[1], requires:

- **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)

Stage 2 of the certification criteria for Meaningful Use includes section §170.314(d)(3) Audit report(s). This section requires the following[2]:

- Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards at §170.210(e).

The federal government requires vendors to implement appropriate controls and reporting mechanisms. Covered entities are expected to use these controls and reporting mechanisms to monitor the behaviors of their workforce and to prevent unauthorized access and disclosure of ePHI.

The Joint Commission

The Joint Commission includes two information management (IM) standards in its manuals that address a healthcare organization's responsibility to maintain (monitor) privacy and security:

- **IM.02.01**, The hospital protects the privacy of health information.
- **IM.02.01.03**, The hospital maintains the security and integrity of health information.

Elements of performance for both of these standards require written policies, the enforcement of those policies, monitoring policy compliance, and monitoring of information to improve privacy, confidentiality, and security.

HIPAA Audit Program Protocol

In June 2012, the Office for Civil Rights released criteria that its auditors use to validate compliance with HIPAA[3]. The table below lists some of the protocol's criteria pertaining to the audit.

Key Activity	Audit Procedures
Determine the Activities that Will be Tracked or Audited	• Obtain and review documentation relative to the specified criteria to determine whether audit controls have been implemented over information systems that contain or use ePHI.
Select the Tools that Will be Deployed for Auditing and System Activity Reviews	• Inquire of management as to whether systems and applications have been evaluated to determine whether upgrades are necessary to implement audit capabilities. • Obtain and review documentation of tools or applications that management has identified to capture the appropriate audit information.
Develop and Deploy the Information System Activity Review/Audit Policy	• Obtain and review formal or informal policies and procedures and evaluate the content in relation to the specified criteria to understand whether a formal audit policy is in place to communicate the details of the entity's audits and reviews to the work force. • Obtain and review an email, or some form of communication, showing that the audit policy is communicated to the work force. o Alternatively, a screenshot of the audit policy located on the entity's intranet would suffice.
Develop Appropriate Standard Operating Procedures	• Obtain and review management's procedures in place to determine the systems and applications to be audited and how they will be audited.

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 refers to the revisions to the Federal Rules of Civil Procedures and Uniform Rules relating to discovery of electronically stored information, which went into effect December 1, 2006. It refers to the information that an organization can request and expect to produce in response to litigation such as audit trails, the source code of a program, metadata and any other electronic information subject to motion for compulsory discovery[4].

Establishing Strategy and Process

A multidisciplinary team is essential to developing and implementing an effective security audit strategy. At a minimum, the team should include IT, risk management, and HIM. The organization’s designated security official should lead the team in coordination with the designated privacy official.

The team should take the following actions when identifying a strategy and process:

- Create a diagram of how ePHI flows within the organization to help determine which applications and systems to audit. This flow diagram may also help to differentiate appropriate vs. inappropriate access to ePHI.
- Identify the capabilities of applications and systems to understand what is auditable; disparate systems may require modified audit plans.
- Create and place 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.”
- Involve application and system owners, when appropriate, to determine what user activities should trigger an entry in the audit trails.

- Ask department or unit leadership to review audit trails to determine the appropriateness of ePHI access based on workforce roles and tasks.
- Involve department or unit leadership who most familiar with job responsibilities in interpreting findings and identifying questionable circumstances that require additional investigation. Leadership can also help determine the appropriate frequency of audit trails.
- Determine how random audits will be conducted as well as the frequency of those audits.
- Involve 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.
- Develop a standard set of documents used to investigate and record potential violations and breaches (i.e. information collection forms for interviews, actions taken, and reporting).
- Add a provision to contractual agreements requiring adherence to privacy and security policies, cooperation in security audits, and investigation and follow-through when breaches occur.
- Evaluate the impact of running audit reports on system performance.
- Determine what audit tools will be used for automatic monitoring and reporting.
- Determine appropriate retention periods for audit logs, trails, and audit reports.
- Ensure 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 will be applied against a workforce member, business associate, or other contracted agent.

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.

When determining what to audit, healthcare organizations must identify and define ‘trigger events,’ meaning the criteria that will flag questionable access of confidential ePHI and prompt further investigation. Some trigger events will be appropriate, 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 necessary.

Examples of trigger events include employee viewing of the following information:

- 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 or attempted homicide)
- Patient files with isolated activity after no activity for 120 days
- Other employee files across departments and within departments (Note: Organizations should set parameters to omit legitimate caregiver access)
- Records with sensitive health information, such as those involving 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 (Note: Organizations should verify that access has been rescinded)
- Portions of a record that an individual would not ordinarily have a need to access based on his or her discipline (e.g., a speech therapist accessing a pathology report)

Those individuals who review the audit logs should evaluate the number of trigger events 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 or Stage 2 Meaningful Use criteria will also meet health IT audit criteria. The health IT audit criteria may provide enough detail to determine whether unauthorized access into a patient's record occurred.

These built-in audit logs easily store millions of entries of application transactions. It can be extremely time consuming to search through these detailed logs to find the specific information necessary to conduct an investigation regarding a particular encounter. Analyzing the audit logs also requires 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 manual 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 healthcare organizations rely on third-party audit tools that systematically and automatically analyze data and quickly generate reports based on search criteria that match 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 perform an in-depth analysis of information.
- 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 timekeeping 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. Upfront 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 that 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 upfront costs because the vendor supplies and owns the necessary hardware and software. The vendor also provides the programming support. Healthcare organizations pay 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, healthcare 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 crucial for a healthcare organization's security audit strategy to outline the appropriate procedure for responding to a security incident. However, the strategy 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 as possible after an event occurs. This is especially important for audit logs that 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 healthcare organization's information security and privacy officials must provide education to the directors, managers, and supervisors who are responsible for reviewing security audit report findings. This ensures that these individuals are equipped to interpret results and determine appropriate access based on defined and approved access permissions.

Presenting Audit Report Findings to the Workforce

If an audit reveals that an employee has potentially inappropriately accessed PHI, the healthcare organization must first notify certain individuals before reporting the findings to the entire workforce. These individuals include a member of human resources or risk management as well as a union representative (if the workforce is unionized) and legal counsel (as appropriate).

Organizations should consider factors such as education, experience, privacy and security training, and barriers to learning (i.e.., language) when evaluating workforce actions. Remember that an individual may have had a reasonable explanation for the access, even if the initial review indicates otherwise. For example, a physician may request a nurse to look up a patient's lab results as a favor. In addition, organizations should avoid interrogating the workforce member involved in the inappropriate access. Instead, treat the questioning as an inquiry.

Organizations must apply security and privacy audit policies and sanctions consistently and without exceptions. Therefore, organizations should develop and implement graduated sanctions so that the punishment fits the incident. Making exceptions to the policy jeopardizes the trust of the workforce and consumers, and it poses a risk to legal defense. Healthcare organizations leave themselves vulnerable to both individual and class action lawsuits when they do not have a strong and consistent enforcement program.[5] For non-employed physicians, medical staff bylaws may also be used in determining appropriate sanctions.

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

Protecting and Retaining Audit Logs

HIPAA requires covered entities to maintain proof (i.e., documentation) that they conduct ongoing audits. Such documents may include policies, procedures, and past audit reports. This documentation must be retained for six years. State statutes of limitations relative to discoverability and an organization's records management policies may require that this information be kept longer.

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

There is no HIPAA requirement, standard, or prevailing practice that dictates how long the actual audit logs must be retained. Covered entities and business associates should consider retaining EMR and EHR audit logs for three years because of the length of time in can take for civil cases to proceed.

However, proof of compliance with the HIPAA Security Rule (i.e., proof that audit logs are reviewed and that the covered entity has an audit strategy) must be retained for six years.

An organization's audit strategy should also stipulate the following actions to protect and retain audit logs:

- Store audit logs and records on a server separate from the system that generates the audit trail
- Restrict access to audit logs to prevent tampering or altering of audit data
- Retain audit trails based on a schedule determined collaboratively with operational, technical, risk management, and legal staff

Prevention through Education

Healthcare organizations should reinforce this message to employees: "Just because you can access PHI, doesn't mean you should access PHI." Education is a pssreventive measure that organizations must execute and re-execute to ensure optimal outcomes and the success of a security audit strategy. To ensure success, organizations should:

- Ensure that all employees, providers, associates, and contractual partners understand patient rights, including accounting of disclosures as well as policies and procedures related to privacy and security.
- Inform all employees, providers, associates, and contractual partners of the security audit practices.. The workforce should be made aware that their activities are being audited and monitored. They may be held accountable for any logged activities by their user ID. However, don't reveal the details of the audits (e.g., trigger points, timing, scope, and frequency).
- Ensure that orientation for new employees includes focused training such as setting the expectation and identifying the acceptable practices for the access of PHI as well as policies and procedures for PHI use, auditing, and monitoring. 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 ePHI. 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. Meaningful Use, certified EHR Test Procedure for §170.302.r Audit Log, available online at http://healthcare.nist.gov/docs/170.302.r_AuditLog_v1.0.pdf.
2. Meaningful Use, certified EHR Test Procedure for §170.314(d)(3) Audit report(s), available online at http://www.healthit.gov/sites/default/files/170.314d3auditreports_2014_tp_approvedv1.2.pdf.
3. Department of Health and Human Services. HIPAA Audit Program Protocol is available online at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
4. AHIMA. *Pocket Glossary of Health Information Management and Technology*, 3rd Edition. AHIMA. 2013, 117-118.
5. 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.

The Payment Card Industry Data Security Standard, available online at the PCI Security Standards Council website at https://www.pcisecuritystandards.org.

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 78, no.17 (January 25, 2013)

Department of Health and Human Services. HIPAA Audit Program Protocol is available online at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

The Joint Commission. 2013 Joint Commission Hospital Accreditation Standards. Oakbrook Terrace, IL: Joint Commission Resources, 2013.

Prepared by (2013)

Tom Walsh, CISSP

Assisted by (2013)

William Miaoulis, CISA, CISM

Acknowledgments (2013)

Becky Buegel, RHIA, CHP, CHC
Marlisa Coloso, RHIA, CCS
Jane DeSpiegelaere-Wegner, MBA, RHIA, CCS, FAHIMA
Kathy Downing, MA, RHIA, CHPS, PMP
Elisa R. Gorton, RHIA, CHPS, MAHSM
Lesley Kadlec, MA, RHIA
Susan Lucci, RHIT, CHPS, CMT, AHDI-F
Kelly McLendon, RHIA, CHPS
Harry B. Rhodes, MBA, RHIA, CHPS, CDIP, CPHIMS, FAHIMA

Prepared by (2011)

Tom Walsh, CISSP

Assisted by (2011)

William Miaoulis, CISA, CISM

Acknowledgments (2011)

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.

Article citation:
AHIMA Practice Brief. "Privacy and Security Audits of Electronic Health Information (2013 update)" (Updated November 2013)
