HIPAA Audit and System Activity Review: Developing a Process that Focuses on the Greatest Risks First

by Linda D. Hofler, MSN, RN, FACHE, CHP; Joy Hardee, RHIA, CPHQ, CHP; Kenneth Dildy; Deeanna Burleson, MSN, RN; and Jamie Grady

---

The privacy and security rules require audits and system activity reviews. Here is one health system's process, a systematic approach that focuses on areas of greatest risk.

Ensuring the privacy and confidentiality of patient information is fundamental to HIM, but it has taken on a new level of urgency organization-wide since HIPAA's enactment in 1996. Audit and system activity review requirements under HIPAA's privacy and security standards have forced hospitals, physician offices, and other covered entities to evaluate their policies, procedures, and auditing processes as well as their capacity to measure and document their compliance.

The process can be extremely complex because of various system audit capabilities and varying levels of access within each system. Audits and reviews also require a thorough understanding of how processes are designed to work within a system.

This article describes a systematic process for auditing privacy and security compliance and reviewing activity in information systems that store protected health information (PHI). The process focuses monitoring efforts on areas of greatest risk and vulnerability, encouraging early detection of inappropriate access of high-risk groups. It was developed within a rural health system, but it can be adopted by other covered entities, regardless of the size or scope of services provided.

Creating a Deliberate and Systematic Approach

University Health Systems of Eastern Carolina (UHSEC) is composed of a 750-bed tertiary care, level-one trauma center; five community hospitals; home health, hospice, and outpatient services; physician offices; and a free-standing surgery center and wellness facility.

Gaining an organizational commitment to security and privacy compliance required the support of executive leadership. It also involved a variety of departments. UHSEC's HIPAA task force includes representatives from HIM, risk management, finance, information systems (IS), and key departments representing the various subsidiary organizations. A member of the executive staff chairs the group. The task force has been key in eliciting support for a comprehensive, systemwide audit process. It was the initial group to sanction the process.

Two privacy officers at UHSEC have operational responsibility for compliance within the tertiary medical center and corporate oversight responsibility for the subsidiary organizations. One officer, a registered nurse, is the administrator for in-house legal; the other, an RHIA, is the administrator for the corporate compliance office. Each subsidiary organization has its own designated privacy officer. This individual has primary responsibility for the specific entity and works closely with the corporate privacy officers.

The information technology (IT) security officer position is housed in information systems. The corporate risk management department is a companion department to the in-house legal department, both of which reside within the office of general counsel. The departments are organized independently, but they engage in compliance efforts collaboratively to ensure the most efficient use of resources.

As UHSEC dealt with privacy auditing requirements, it also began more diligent preparation for HIPAA security compliance. The comprehensive process included several dimensions: physical inspection, staff interview and information gathering, review

of events relating to privacy and security, and a planned approach to monitoring and review of system activity within the automated systems.

The Audit: Taking a Walk, Noticing Notices

The privacy officers began the audit program with physical inspections. These "walkabouts" included elevator monitoring, cafeteria conversation monitoring, trash-can content review, and interviews with staff. The privacy officers looked for items containing PHI discarded in the regular trash, discussions involving PHI in public or not-so-private locations, and staff's understanding of policies and procedures. Walkabouts were always unannounced and were completed with a written report back to the manager of the unit. If issues were identified, the report included an expected remediation plan.

In conversations with staff, the privacy officers focused both on practice and knowledge and were able to evaluate compliance issues based on discussions about barriers staff perceived in the practice setting. This was an opportunity for face-to-face education about HIPAA and its implementation in the real world. If PHI was found in regular trash, for example, the privacy officers were able to talk to staff about the rationale for policies and procedures and consequences of noncompliance. At the same time, they might identify an issue with placement of the shredding containers. After evaluation of the environment, minor modifications were implemented that made compliance with policy and procedure easier for clinical staff.

The privacy officers and the information technology security officer completed site visits at each of the UHSEC facilities and met with designated privacy contacts to review the physical layout of the facility, general operational practices, and privacy challenges. As a part of the visits, the officers completed an overview and a general policy and procedure review and reviewed documentation of events. The site survey has become a part of UHSEC's annual privacy compliance review.

The audit also identified a need to ensure that patients received the notice of privacy practices (NPP) at their first visit to the facility. The corporate information system department developed a report generated from the automated patient admission system that documented delivery of the NPP. The report indicates compliance by registration area, helping to identify areas that may need additional education. It also allows a complete process evaluation to ensure that patients receive the NPP and that the date they received it is documented in the registration pathways. A manual process is used for physician offices and other entities that do not use an automated patient registration system. Monitoring has assisted in identification and correction of deficiencies and has ensured compliance with this requirement of the privacy standards.

System Activity: Choosing Whom, What to Review

The privacy officers, IT security officer, and risk management staff met with the HIPAA task force to discuss the development and implementation of a review mechanism that identified and resolved inappropriate access to automated information systems. The shared goal was a process that emphasized the most important matters, retrieved the most useful data, and made data collection and evaluation easy for users. Further, the new process would ensure that the entire health system followed a standardized approach in monitoring system activity.

The first step was identifying individuals essential to the development of the process. Accordingly, a work group comprised of representatives from privacy, IT security, risk management, and IS was convened.

Focusing on the Highest Risk

The group began by evaluating which data would assist in organizing the system activity review. Data from the corporate risk management department's existing audit process were used to identify high-risk groups, system users and patients, and the best use of resources. The process focused on the main IS patient management, patient accounting, and order entry systems and included high-profile patients, patient complaints, and routine employee surveillance.

Based on the risk assessment, the group identified two key types of reviews: surveillance (or random reviews) and high-risk patient reviews. The latter category includes high-profile patients (e.g., patients well known in the community or employees and their families), patient complaints, and requests for restrictions. A matrix was developed that outlines the initial approach to each of the categories and the focus of the review (see "Information Systems Activity Review Process," below). The matrix was useful in determining a realistic volume of activity to review per month and where staff hours should be allocated to perform reviews within the automated systems.

Information System Activity Review Process

This matrix outlines a framework for routine monitoring, responsibility for review, and the frequency with which the review will be performed.

Random Audits of User Access shows the users whose access will be randomly reviewed. The process will select a random day, random user, and random patient chart review. A percentage of total users that are employees, physicians, residents, physician assistants, students, school of medicine employees, and other nonemployees will be selected.

At Risk and/or Review Request. All patients will be reviewed who are on security alert (e.g., flagged as domestic violence victims or victims of child abuse), confidentiality alert (e.g., requested removal from directory listing), complaints regarding inappropriate access, audit request, or a request for restriction.

User Validation is a quarterly review to validate that users who have access to our systems should retain that access for business reasons and to ensure that terminated staff have been removed.

IT Infrastructure Activity. This review will evaluate potential hacking or denial of service threats, inappropriate transmittal of confidential information, compliance with software licenses, Internet and e-mail use, and file-sharing policies. The details are still being determined. Based on the volume of data that is produced from logging these items, automatic notifications are being established for the most severe security warning flags.

Random Audits of User Access[1]	At Risk and/or Request for Review[2]	User Validation	IT Infrastructure Activity
Responsible party: Review group Frequency: Monthly Reviewed: • Physicians, residents, physician assistants, nurse practitioners • Employees • Students • Medical school employees • Other nonemployees Note: Random day, random chart, random employee	Responsible party: Review group Frequency: Monthly Reviewed: • High profile[3] • Security alert • Confidentiality • Complaints • Audit request • Request for restrictions Note: Look at entire record access	Responsible party: IT security Frequency: Quarterly Reviewed: • Access validation	Responsible party: IT security Frequency: TBD Reviewed: • Network traffic (router, switches) activity • Firewall activity • Intrusion detection system activity • Wireless activity • E-mail activity • File transfer activity • Virus management • Internet activity • Remote activity • Software licenses

1. Five percent or more of users with access to the high-risk system(s) will be reviewed over a one-year time period.
2. 100 percent of accesses performed against these patient records.
3. High profile includes board members, political and community dignitaries, physicians and employees and their family members as patients, and individuals in news reports.

The matrix was developed in conjunction with an evaluation of historical risk management data. This assessment assisted the group in identifying areas of greatest risk for inappropriate access to PHI. The information was used to prioritize the use of resources, identify the most likely areas of inappropriate use, and determine the best avenue for identifying inappropriate use and effectively and efficiently investigating it. For example, random surveillance is not as likely to identify access misuse as is a

patient complaint of privacy violation or the knowledge that an employee is currently a patient and runs the risk that fellow workers might access protected information out of curiosity.

The review process continues to evolve. UHSEC began the journey with the goal of auditing every employee with system access at least once every 12 to 18 months. As the process developed, the emphasis shifted to determining where resources are best spent and how they should be actively engaged. Staff determined that the most effective use of resources and the best way to identify priority issues was 100 percent review of high-risk categories and random monitoring of a percentage of the general employee population.

Tracking Down the Data to Track

Decisions were then made regarding which information systems to review. Based on discussion and past history, the work group chose to focus on systems that contained the most PHI and that had the most users with access. The process will eventually grow to review all information systems containing PHI across the health system, but for now the focus is on the areas with the greatest risk for inappropriate access.

An area of weakness identified in the process is the lack of adequate audit trail capability within individual automated systems. The group continues to evaluate new systems and products and work with vendors to influence the technical development of adequate and efficient activity logging systems. The process led to the development of a formal policy and procedure that will be implemented as a part of the security compliance initiative systemwide. (The policy appears below.)

Once the structure for the review process was in place, the group identified where data existed and how best to approach data collection. A review of activity logs revealed that necessary data were missing. The activity logs did not supply all relevant information required to conduct a review in one place.

The logs captured which users accessed the patient information, the date and time, and the type of function performed (e.g., read, create, or update); however, the logs did not indicate the user's job title or work location. This information was maintained by IS in a database that interfaces daily with a human resources application to maintain employee information for security administration functions. The logs also could not indicate when physicians accessed the records or their clinical rotation for the date under review.

The group identified the need to know the admitting diagnosis and the room location for each patient whose record was reviewed. It also determined the need to identify each physician that had a relationship to the patient (e.g., referring, attending, or consulting). The group worked with an IS specialist to gather and customize all information required, which includes data from the patient management system, the IT security administration database used to maintain access records for all systems, and the medical support staff for the rotation of the physicians or residents.

This data refinement-and the inability to have this detail in a single automated system-has taken considerable time and created considerable manual work within the IS department. The lack of integration between the system activity logs made the retrieval of necessary data tedious and time consuming. The work group continues to work with IS teams, providing guidance in system selection and development of activity review logs. The IT security officer is involved in, or made aware of, new system selection, and performs a security assessment to determine the audit logging and reporting capabilities before the systems are selected. An awareness and training process within IS also helps by having an IS systems analyst ask similar questions of vendors.

These enhancements will provide more complete information for analyzing system activity without the intense labor commitment presently required to obtain reliable information. By designing reports that give employee information, complete information about what kind of data the employee is accessing, the location where the access took place, the dates and times, and details about the patients, there is better data to judge the appropriateness of access by employees.

Linking to Education, Sanctions

In order for a covered entity to demonstrate compliance with the HIPAA regulations, it is important that its auditing and system activity review processes are linked to its HIPAA education program and its sanctions and disciplinary action process. It is essential for organizational review of compliance, performance improvement activities, and consistent application of

remediation and sanctions that objective data are gathered. It is also key to ensuring that staff is held accountable for compliance with policies and procedures.

The information obtained in UHSEC's auditing and system activity review processes is analyzed to determine if the access or action was appropriate or inappropriate. If it is determined that access or an action involving PHI may be inappropriate, a referral is made to the corporate risk management clinical analyst for an investigation. The clinical analyst leads the investigation to either substantiate or disprove the potential allegation or suspicious activity.

If an activity is found to be inappropriate, risk management initiates the sanctions process. This triggers a review of the event by an executive-level administrative group specific to each facility within the system. The group reviews the case, and sanctions are recommended. The manager of the department where the incident occurred is responsible for implementing the sanctions. This systematic process of review and action ensures consistency in the investigation process as well as consistency in the application of sanctions and disciplinary action.

The process supports the existing human resource method for employee discipline and ensures the same violations, regardless of location, are treated in the same manner. This clearly communicates the organization's commitment to dealing with these matters seriously and fairly across the system. The outcomes of all events are documented in an automated database for tracking and trending. This facilitates identification of trends that require a system approach for follow up.

On a monthly basis, the privacy officers meet with the corporate risk management staff to discuss privacy events and to identify potential trends across the organization. On several occasions, trends in activity were noted and specific education and follow-up across the organization was completed to address the issues.

The systematic and deliberate approaches that UHSEC has created to address HIPAA requirements are working well as a tool for compliance analysis. The process is also essential for monitoring activity in automated information systems that store PHI. The work group anticipates continued refinement to the process and that it will be a process always in evolution.

Policy/Procedure

Manual	**Information Technology Security Manual**	**Subject**	**Activity Review and Monitoring**
Number: A.02		**Effective Date: 10/2004**	
Version: 1.0		**Revised Date:**	
Prepared by:			
Approved by (president or designee):			

Purpose

Establish the process to conduct, on a periodic basis, an operational review of system activity including, but not limited to, system access, file access, security incidents, appropriate software licensing, etc. The operational review shall:

- Ensure access to and utilization of protected health information (PHI) and other confidential sensitive information in our electronic systems is appropriate
- Identify and respond to inappropriate access and or utilization
- Monitor compliance with organizational policy and procedures
- Ensure regulatory and accreditation requirements are met
- Identify and respond to security incidents
- Identify and recommend changes to the information security program as applicable

Policy/Procedure

Application Monitoring
The level of risk, volume of users, and the type of confidential information accessed will be used to identify the systems to monitor. The activity review list contains the listing of systems and components to be reviewed. Criteria for establishing the level of risk are:

1. If the information maintained within the system is highly sensitive (e.g., diagnosis of condition, type of test ordered, results of test, and information that is susceptible to identity theft)
2. Whether other incidents have occurred by users of the same system

Workstation Security
On a periodic basis, the information technology security office (ITSO) will coordinate or conduct a walkthrough at random locations of UHSEC to assess compliance with security measures contained within the workstation use and security policy.

Malicious Code
Information system (IS) and/or departmental system administrators or a designee will conduct reviews of malicious code logs and change control components to ensure workstation and IS system servers are complying with processes contained within the workstation use and security policy and the malicious software policy.

Software License
On a periodic basis, the ITSO will coordinate or conduct a review of randomly selected workstations to ensure software installed on these workstations have legal licenses and system users are in compliance with the workstation use and security policy. Any nonverifiable license will result in a request to IS for removal of software.

Wireless Activity
The IS network administrator or designee will conduct, on a periodic basis, a review of wireless activity to determine if any inappropriate access points or other security exposures have been introduced into the UHSEC wireless infrastructure.

Internet Activity
Based on a request for information by management staff, risk management, in-house legal affairs, or audit and compliance, a review will be conducted against Internet activity of specific users or workstations.

E-mail Activity
Based on a request for information by management staff, risk management, in-house legal affairs, or audit and compliance, a review will be conducted against e-mail activity of specific users or workstations.

File Transfers
Periodic reviews will be conducted against file transfer processes at UHSEC, to ensure proper sharing of information is being conducted and documented as required, based on privacy and security policies.

Network Intrusions
The IS network administrator or designee will conduct a review of activity logs captured by network firewalls and/or intrusion detection systems to identify exposures to the UHSEC network infrastructure.

Physical Access
The ITSO will conduct, on a periodic basis, a review of physical access entry to areas that contain

sensitive information systems equipment to ensure proper access controls are maintained.

Security Policy Exceptions
The ITSO will conduct annual reviews of approved security policy exceptions that have been granted to validate the exception continues to be required.

Activity Recording and Archival
Records that are collected to be used for activity review processes must be maintained in accordance with the information property rights and record retention policy.

Procedure

An evaluation will be conducted using the access components listed in the activity review process. Risk management or the ITSO will manage this and any special review requests.

1. Using schedule, ____**A**____ will identify what records to be pulled and will run the activity data.
2. ___**A**___ will attach the activity review tool and forward to _**C**_.
3. ___**C**___ will review data and determine if there is inappropriate access or use.
4. If inappropriate access or use is identified, ____**C**____ sends information to risk management for investigation and follow-up. Documentation is housed in risk master. Risk management runs follow-up report quarterly for _**C**_.
5. If the access or utilization is appropriate, _**C**_ sends data to _**A**_ who archives the documentation.
6. Summary of review findings will be sent to UHSEC committees, as deemed necessary.

   A = ITSO or risk management
   C = Risk management analyst, or ITSO, or IS/departmental system administrator, or IS network administrator

Accountability

Any failure to abide by this policy may result in disciplinary action in accordance with the personnel policies and procedures, and/or medical staff bylaws, rules, and regulations.

References

Information Technology Security Manual-Workstation Use and Security
Information Technology Security Manual-Information Property Rights and Record Retention
Information Technology Security Manual-Malicious Software
Information Technology Security Manual-Activity Review List
Information Technology Security Manual-Activity Review Process
Information Technology Security Manual-Activity Review Tool
HIPAA Safeguards-164.308(a)(1)

Definitions

Confidential information-information that includes, but is not limited to, employee records, research data, copyrights, intellectual property, PHI, corporate information including budgetary or strategic, and any other information deemed confidential. This information may be generated, received or collected by UHSEC.
Protected health information (PHI)-individually identifiable health information transmitted by electronic media, maintained in any medium described in the definition of electronic media, or transmitted or maintained in any other form or medium.

Revision History

Date	Version Number	Comments
10/2004	1.0	New

Linda D. Hofler *(lholfer@pcmh.com) is administrator of in-house legal affairs and privacy officer,* ***Joy Hardee*** *is administrator of corporate compliance and privacy officer,* ***Kenneth Dildy*** *is information technology security officer,* ***Deeanna Burleson*** *is risk management clinical analyst, and* ***Jamie Grady*** *is risk management clinical analyst at University Health Systems of Eastern Carolina in Greenville, NC.*

Article citation:
Hofler, Linda D., et al. "HIPAA Audit and System Activity Review: Developing a Process that Focuses on the Greatest Risks First." *Journal of AHIMA* 76, no.3 (March 2005): 34-38.