MedMal DIRECT
Insuring a Healthy Practice

Putting an Audit Log Review & Reporting Program in Place

Why Audit?

First and Foremost – It is required by the HIPAA Regulations.

The HIPAA Security Rule: Information System Activity Review
Section §164.310(a)(1)(ii)(D) "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."

§164.304: Definitions. "Administrative safeguards are…to manage the conduct of the covered entity's workforce in relation to protection of that information."

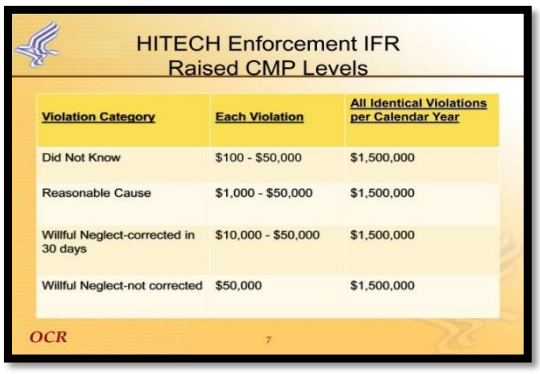
HIPAA Privacy Rule:

§164.530(c)(1): Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

§164.530(i)(1): Administrative Requirements: Policies and Procedures. "…The policies and procedures must be reasonably designed, taking into account the size of and the type of activities related to protected health information undertaken by the covered entity, to ensure such compliance."

Second: In order to protect and secure electronic protected health information (ePHI) you need to know who is accessing patient records and monitor user activities. Audit logs record all events taking place in your electronic health records systems as well as events of your servers, firewall, work stations and networking devices. Log files contain complete audit trails of access, additions, deletions or manipulation of key information.
Third: Under HIPAA you bear the "Burden of Proof". Accusations made against your organization are assumed to be correct. Access log data may be the only "proof" your organization has that a record was not beached or used in a manner not allowed under the HIPAA Privacy Rule.
Fourth: Legal Liability – Federal Rules of Civil Procedure "Greater leniency" – of manage information with "good faith intentions".
Fifth: Meaningful Use requires audit log generation and compliance with HIPAA Security Rule. You may face Accreditation standards that require audit log review. Payment Card Industry Data Security Standard (PCI) includes audit requirements, and there are E-Discovery legal requirements.
Sixth: It's the right thing to do to protect your patients. According to Experian, 1.4 million Americans were victims of medical identity theft in 2009.

Finally: It could save you huge Civil Monetary Penalties (CMPs)



The HIPAA Security Rule Requires That Your Practice Have "Robust" Measures in Place to Review System Activity.

"The breach is considered discovered by a covered entity or business associate as of the first day on which a breach is or should have reasonably been known to have occurred… It is a difficult concept… basically prompting covered entities and business associates to have robust programs in place to identify when breaches happen and to respond immediately to these breaches…BECAUSE THEY CAN'T PUT THEIR HEAD IN THE SAND AND SAY WE DIDN'T KNOW."

Iliana Peters, Health Information Privacy Specialist, Office for Civil Rights

Definitions:

Audit log – record of sequential activities maintained by the application or system.
Audit trail – the log records that identify a particular transaction or event (view/access). *Fundamentals of Law for Health Informatics and Information Management* defines an audit trail as a "record that shows who has accessed a computer system, when it was accessed, and what operations were performed."
Audit – review of the records to determine appropriateness of access and a required part of security and risk management process.
Burden of Proof - A party's job of convincing the decision maker in a trial that the party's version of the facts is true. In a civil trial, it means that the plaintiff must convince the judge or jury by a preponderance of the evidence that the plaintiff's version is true -- that is, over 50% of the believable evidence is in the plaintiff's favor. Definition from Nolo's Plain-English Law Dictionary
E-discovery - 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.
Minimum Necessary - make all reasonable efforts to use or release only the "minimum necessary" identifiable health care information to achieve the intended purpose. The minimum necessary standard does not apply to 1) treatment-related requests or disclosures of health care information, or 2) situations in which an individual has signed an authorization for the use or disclosure of identifiable information (such as in a clinical trial), and 3) other limited exceptions that apply to administrative requirements.
Sensitive PHI – PHI that could have an "Impact", reputational or financially on the patient. Examples would be HIV/AIDS relate information and/or records HBV, TB or Other Communicable Diseases, Mental Health Information and/or Records, Domestic Violence, Genetic Testing Information and/or records, and Drug/Alcohol diagnosis, treatment or referral information.

Prior to Developing Your Auditing Program

1. Review all staff member security privileges and settings in the EHR/Practice Management System. Document the level of access to both paper and electronic records and use job descriptions to determine level of access.
2. Be sure to apply “minimum necessary”.
3. Help your staff comply by locking records of employees, VIPs and records containing sensitive PHI.
4. Prevention through Education. Education is a required standard that will aid in the success of a security audit strategy. Organizations must train their staff on all policies and procedures related to privacy and security. This education must extend to business associates and their sub-contractors. Inform all employees and business associates of the security auditing policy and sanctions policy that reinforces it is a HIPAA violation to access records in an inappropriate manner. Again documentation is key so have each staff member sign an acknowledgement and make sure this policy notice is in your business associate agreement.

Training Of Staff Related to Audit Logs

- Need to Know
- Minimum Necessary
- Protection of Username and Password
- Consequences of Violations – Sanctions Policy
- Employee Acknowledgement of Education with Documentation

Planning Strategies/Defining a Plan
Your Goals: Compliance, Protection of Patients, and Protection of your Organization.

In setting up strategy and process, you should consider:

 Developing a flow chart of your network, servers, security appliances, workstations, laptops and other mobile or remote devices that connect to the network. Be sure to document the location of all ePHI and where it is stored, even if only temporarily as in the case with fax servers or scanning workstations.

 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."

 Determine how random audits will be conducted.
 Develop 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.
 Require cooperation in security audits, and investigation and follow-through when breaches occur.
 Evaluate the impact of running audit reports on system performance.
 Determine what or if 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.

Look for:

- PHI accessed by anyone not directly related to the patient's treatment, payment, or healthcare.
- Information not corresponding to the role or privileges of the user.
- PHI of VIPs or well-known persons.
- Records that have not been accessed in a long time. (Over 120 days)
- An employee's medical record.
- PHI of a terminated employee.
- Sensitive PHI records such as psychiatric records.

Audit logs and the audit log program are useful in:

1. Detecting unauthorized access to patient information.
2. Establishing a culture of responsibility and accountability.
3. Reducing the risk associated with inappropriate accesses (behavior may be altered when individuals know they are being monitored).
4. Providing forensic evidence during investigations of suspected and known security incidents.
5. Tracking disclosures of PHI.
6. Responding to patient privacy concerns regarding unauthorized access by family members, friends, or others.
7. 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).
8. Detecting new threats and intrusion attempts.
9. Identifying potential problems.
10. Addressing compliance with regulatory and accreditation requirements.

Where Do You Need To Audit?

Small practices should limit their auditing to the EHR audit logs and locations where ePHI is stored such as fax servers and scanning workstations. Even this is a daunting task as the audit records could be thousands of pages of entries each month. For practices without EHR, and with Practice Management systems that do not create audit logs, the windows server logs, firewall and router logs need to be reviewed.

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
- 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.
- Records of terminated employees (organizations should verify that access has been rescinded)

Content of Audit Records

The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any user or subject associated with the event. (Note – you must have individual user names and passwords for both windows and the EHR/Practice Management system to be able to track individuals and meet this requirement.) Audit record content that may be necessary to satisfy the requirement of this control Includes time stamps, source and destination addresses (ip address), user/process identifiers, event descriptions, success/fail indications and filenames involved.

Best Practices

- Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

- Individual accountability
- Enough information to determine the date and time of action the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.
- Successful and unsuccessful logons and logoffs.
- Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion.
- Denial of access resulting from an excessive number of unsuccessful logon attempts.

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.

Audit trails can also be built to monitor the modification, viewing, and deletion of information. For example, a healthcare entity's security officer could create policy, with organizational approval, to search access to PHI by anyone not directly related to the patient's treatment, payment, or healthcare Information not corresponding to the role of the user

The Following Two Pages Are A Sample Audit Plan To Meet Best Practices For The Small Covered Entity Audit Program Policies and Procedures

Purpose of Our Auditing Program

- ✓ *Tracking Employee Behavior& Holding individuals accountable for their activity.*
- ✓ *Scanning for External Intrusions of those Unauthorized to Enter PHI Databases.*
- ✓ *Detecting Inappropriate Access to PHI.*
- ✓ *Reducing the Risk for the Organization and Our Patients.*
- ✓ *Investigate Complaints.*
- ✓ *Supporting Our Culture of Compliance.*

Determining What to Audit

- *User Information*
- *Patient Information*
- *Time*
- *Location of Access*
- *Duration of Access*
- *Information Accessed*
- *System Activity (Printing, modification, downloads, etc.)*

Targeted Activity- what are we looking for

- ✓ *Same last name/address – confirm unique records*
- ✓ *VIP – no one tagged as VIP*
- ✓ *Co-worker illness – does someone else access*
- ✓ *Deceased patients after established time frame*
- ✓ *Inactive files – no activity or access*
- ✓ *Sensitive records*

Evaluation of Findings & Documentation of the Audit Log Activity

Our goal with an audit program is to reduce risk to an "Acceptable Level" based on our unique circumstance, resources and in response to the potential threats identified by a risk assessment.

As the HIPAA Compliance Officer I receive monthly reports from our IT staff / vendor that details the audit log activity. I review these reports and store them for the required 6 years. Audit log review is our method to assure, within reasonable and appropriate risk measures, that there is no unauthorized activity occurring on our network.

Evaluating Audit Findings

Audit Logs are just the beginning of the audit log review process. Do not jump to conclusions, audit logs are the beginning of the investigation process. Check schedules is someone filling in? Are your findings in the normal workflow? Was the information inappropriately accessed further used or disclosed? Was the information "sensitive" in nature? What is the risk of either financial or reputational harm to the patient? Consider if pattern of access could indicate any sort of identity theft. You must follow you data breach assessment policy. Have a policy and consistently FOLLOW it or prepare to be investigated. Being inconsistent poses a risk to your organization from a disgruntled employee.

Retention and Storage of Audit Trails

Access to audit trail records must be strictly controlled to ensure the integrity of the records. Audit logs should be stored for a period of six years which will usually require additional storage space. Storage of all audit logs should be encrypted as it contains PHI.

HIPAA requires that covered entities maintain proof that they have been conducting audits for six years. If you have not had an audit program get started immediately. Remember: State statutes of limitations relative to discoverability and an organization's records management policies may require that this information be kept longer. Audit Log Programs need to be developed and reviewed by senior management and the HIPAA Compliance Officer to establish the most effective plan for the organization.

Sanction process

The HIPAA regulations require that imposed sanctions be consistent across the board irrespective of the status of the violator, with comparable discipline imposed for comparable violations. This practice will enable application of general principles that will lead to fair and consistent outcomes. Sanction implementation will follow the following steps. However, depending on the Category level of the incident, an escalated process can be followed if cause is shown:
Documented conference with recommendations for additional, specific, documented training, if necessary.

- Consider levels of violations so the “punishment fits the crime”.
- Determine if additional education is required.
- Review any barriers to compliance.
- Make sure you have proper safeguards in place.
- Document a Sanctions Policy you will enforce.