Audit Functionality and the EHR: the Importance of Sound Reports and Clear Policies

Save to myBoK

by Sheila Green-Shook, MHA, RHIA, CHP, and Carol Ann Quinsey, RHIA, CHPS

In organizations with paper records, it is difficult—if not impossible—to determine whether records were looked at for any purpose, much less when carrying out job duties. However, electronic health record (EHR) systems have the capacity to electronically capture who has accessed what components of the record and when. Organizations with EHRs should be able to accurately determine access (both appropriate and inappropriate) to health information through the use of audit tools. The trick is to be sure that the information produced in audit reports is useful.

It is also vitally important that organizations outline clear policies for appropriate access of information in the EHR and that the policies are reviewed with staff. Organizations must clearly document that staff members both understand and agree to adhere to privacy policies. Without support in policies, inappropriate access documented through the use of audit tools will be useless in disciplining employees.

This article outlines what organizations should include in EHR audit reports, as well as the importance of audit reports when it comes to accessing the EHR.

Audit to Include…

If your organization has implemented or is planning to implement an EHR, it is critically important for HIM professionals and privacy officers to partner with the IT department to create audit reports. At a minimum, the reports should identify:

- Users who accessed the record
- Patient records that were accessed
- Date and time records were accessed
- Location within the EHR the user accessed

Something to consider when developing audit reports is how they will be obtained and used. In some facilities the privacy officer can run defined reports at his or her convenience. In other organizations it is necessary to call the IT department and request that a special report be run.

In either case, it is imperative that the reports be available promptly and in a format that is useful to the persons required to review and make recommendations from them.

Audit Report Formats

Reports should have the capability to be generated in two ways: an audit by individual patient or an audit by individual user.

Having these options allows for easier auditing, depending on the purpose of the report. For example, if the privacy officer receives a complaint from a patient who is concerned that his or her record has been accessed inappropriately, the report can be generated by patient name. The report will then include a list of all users who have accessed that individual patient's record.

Conversely, there may be concern that an employee has been inappropriately accessing patient records. In this case, the report can be generated by the individual user's name. The report will include a list of every patient's record the employee has accessed.

Once audit reports have been created the appropriate persons can then review them and determine whether the access was necessary in the course of carrying out job duties. Typically the privacy officer will work with a department manager to determine whether or not a problem exists that may require further action. Evaluation of whether access was necessary is an important step in the process.

Case Study: Realizing the Benefits

The benefits of sound audit reports and good policy practices are clear in two instances involving a termination and a disciplinary action. In the first, an EHR audit report proved to be instrumental in the outcome of arbitration.

An employee was terminated for performance issues and alleged inappropriate access of family records. The organization's policy stated that employees cannot access their own records or records of family members using the EHR. According to the policy and procedure, an employee who wants copies of his or her records must go to the business office and follow the same procedure used for all patients. Employees cannot use their employment status to gain access to the electronic medical record.

In this case, the employee appealed the termination. The termination went to arbitration, and during testimony the EHR audit reports were used to demonstrate that the employee not only accessed her record (violation of organizational policy) but also accessed her minor son's record (violation of organizational policy) and her husband's record (violation of organizational policy, state law, and HIPAA). Copies of the signed confidentiality and security agreement were introduced during testimony.

The defense attorney tried to discredit the accuracy and integrity of the audit report but was not successful. The audit report clearly identified the employee, the records she had accessed, and when they were accessed.

While reviewing the audit report prior to arbitration, there were other inappropriate accesses noted as well. The employee also had accessed coworkers' records without a legitimate business need. The employee stated that a coworker had used her log-on to access the family members' records without her knowledge.

The organization's policy stated that each individual is responsible for the security of his or her own user ID and password. Any transactions performed using those two identifiers are the responsibility of the individual to whom they belong.

In this case, the audit reports served as an objective reference that chronologically listed all accesses by the individual user. It documented which records had been accessed and when. Clear organizational policies helped support the expected behavior of the employee as well.

In another facility a manager observed that a staff member in the admitting department was routinely admitting and pre-admitting her family members, including adult children. In addition, she seemed to give no thought to opening the electronic records of coworkers to learn their ages and other information that was not needed in the course of carrying out her duties. Departmental policy strictly prohibited staff members from performing their job with family members and prohibited accessing records of coworkers unless necessary to perform their jobs.

In this situation the staff member admitted deliberately ignoring policies, which she believed were "silly," not caring that she had broken several state and federal laws in addition to organization and department policies. Had she denied these actions the facility could have used audit reports to validate the inappropriate activity in disciplinary action. Again, having clear policies at both the organization and department level that had been reviewed during the course of a recent evaluation supported appropriate disciplinary action.

Putting It in Writing

These examples highlight how important it is for organizations to have audit reports and clear policies and procedures regarding access. They also emphasize the need for IT policies safeguarding user ID and passwords.

It is imperative that organizations document that employees know both the policies and their actions related to the policies. Documentation of an employee's knowledge can be made in departmental meeting minutes where relevant policies are reviewed and individual employees noted as being present.

Documenting that employees both understand and agree to adhere to policies may also be done during orientation and by reviewing expected actions in a confidentiality statement that is reviewed and signed annually by the employee.

Sheila Green-Shook *(sgreen-shook@evergreenhealthcare.org) is the director of health information management at Evergreen Hospital in Kirkland, WA.* ***Carol Ann Quinsey*** *(carol.quinsey@ahima.org) is a practice manager at AHIMA.*

Article citation:
Green-Shook, Sheila; Quinsey, Carol Ann. "Audit Functionality and the EHR: the Importance of Sound Reports and Clear Policies" *Journal of AHIMA* 78, no.6 (June 2007): 62-63.