Following the Digital Trail: Weak Auditing Functions Spell Trouble for an Electronic Record

by Gina Rollins

Not all EHR products deliver strong audit and verification functions. A key HIM consideration is not always a key product feature.

Given the ability of computers to log each user's every keystroke, electronic health records (EHRs) have great potential for robust auditing and record verification functions. But as more organizations bring EHR systems online, they are finding that these essential features can leave much to be desired. This poses problems in establishing the EHR as the legal medical record and in substantiating the record for billing and reimbursement purposes.

"Most EHR systems are not designed with the audit function as a primary design element, and although it's a critical functional element, EHR implementation has been proceeding in advance of adequate attention to audit functions and standards," explains Reed Gelzer, MD, MPH, CHCC, chief operating officer of Advocates for Documentation Integrity and Compliance in Wallingford, CT. Gelzer and Patricia Trites, MPA, CPC, CHCC, CHP, identified a variety of potential audit concerns in a review of nearly 30 major EHR products.

Those concerns are not intended to discourage EHR adoption, say Gelzer and Trites, but they do underscore the important role HIM professionals can play in ensuring the integrity and legality of electronic records. HIM professionals are among the healthcare professionals necessary to determine audit requirements in an EHR system as well as the appropriate level of audit detail for their individual organizations.

"HIM has to fight for a seat at the table at the time an organization is selecting an EHR, and once the system's in place they need to document any issues and educate providers and management about those issues," says Trites, chief executive officer of Healthcare Compliance Resources in Augusta, MI. "The HIM community also needs to be a solid voice in fixing these systems."

Trouble for Data Integrity

Gelzer and Trites found a range of concerns in their review of EHR products. These included the ability to turn the audit function on and off without generating a record of who took the action, when it was done, or why it was done. In some systems they found it possible to identify document changes without producing the original. Some systems allow encounter documents to be left open indefinitely, enabling them to be altered at any time up until signature; in the most extreme situation, there is no requirement for signature at all. Still other systems--particularly older ones--fail to provide adequate reporting functions, requiring users to go back to the vendor or have programmers compile the desired audit information.

Gelzer and Trites also note the potential for trouble in convenience functions such as record cloning or copying. This occurs when new-encounter documents use data from previous encounters, typically in the form of templates. An audit mechanism should be able to differentiate the newly created parts of a record from the copied parts, says Gelzer, but not all do.

Record cloning also raises reimbursement issues, since payers require documentation that is specific to and accurately reflective of each unique encounter. Medicare cites instances in which documentation of physical examinations were nearly identical on subsequent visits, even when diagnoses changed. In other instances, multiple patients had the exact same findings upon follow-up visits. Medicare warns that defaulted documentation of this kind can harm quality of care as well as result in reporting a more extensive history and physical examination than is medically necessary.

Ambulatory systems in particular hold the potential for errors of this sort, as many enable a single user to complete both documentation and coding. "This risk exists with virtually every EHR on the market," contends Steve Lefar, president of MediRegs Inc., in Wellesley Hills, MA, a firm that provides regulatory and compliance management software and databases.

Certification for the Next Generation

HIPAA privacy and security rules provide guidance for EHR audit functions but not strict standards. Both rules call for organizations to scale solutions based on individual circumstances. State laws governing medical records apply to EHRs, but they typically do not prescribe detailed audit requirements. However, further standards are in the offing from efforts such as the Certification Commission for Healthcare Information Technology (CCHIT).

A voluntary, private-sector initiative to certify health IT products, CCHIT has outlined nine audit criteria that will be used in certifying ambulatory EHR products. Six criteria will be effective with the initial product certification beginning this month.

The initial criteria will address issues such as the system's ability to generate an audit record when auditable events happen, such as when users log in and log out or when a chart is created, viewed, updated, or deleted. Criteria also detail the standard information captured, such as date and time of the event, type of event, user identity, and success or failure of the event. Proposed criteria for inpatient EHRs are planned for later this year.

CCHIT certification eventually will be a differentiating factor among EHR systems and spur adoption of its recommended audit functions. "It will separate the wheat from the chaff. Any vendor that wants to compete will do what it needs to do to become certified," predicts Charlene Underwood, chair of the EHR Vendors Association and director of government and industry affairs for Siemens in Malvern, PA.

Yet CCHIT certification alone will not be a cure-all, particularly when it comes to meeting provisions of the Federal Rules of Evidence, which outline discovery and admissibility rules in legal proceedings. An EHR is admissible if the system is shown to be accurate and trustworthy.

A key factor in establishing accuracy and trustworthiness is demonstrating that the information has not been altered. CCHIT criteria may not automatically provide for this. The ambulatory criterion S10 requires that "the system shall continue normal operation even when security audit facility is non-functional." The ability for an EHR system to continue operating even when audit functions are not--when the audit log reaches capacity and overwrites the existing log, for example--is not in keeping with Federal Rules of Evidence, according to Gelzer. Nor would this capability be "adequate to protect providers in case of an audit by a third-party payer...if there is any question of the timing, authorship, or other areas that could be challenged and there is no record to protect the provider," he observes.

Dealing with Legacy Systems

As debate about these issues continues, organizations must address the here and now of the legacy systems they currently have in operation. HIM professionals are important players in this process. When there are perceived problems with an application, the first step is an overall risk assessment, including a review of HIPAA regulations and state and federal laws. This analysis and any related discussions should be conducted with the participation of legal counsel. "The discussion may be subject to attorney-client privilege, and you want open and frank discussions made at the appropriate level," observes Mike Hubbard, a partner in Smith Anderson, a law firm in Raleigh, NC.

Risk assessments should include a survey of all departments to understand how each uses the system. "I encourage people not to focus on the trees of the audit trail but to look at the whole system and see who has access to what features and what security levels are required," says Bill Shenton, a partner with the law firm Poyner and Spruill, also in Raleigh, NC. Doing so will help clarify necessary fixes, amend policies guiding operation and maintenance of the system, and gain support from users for any changes made, he says.

Review of EHR contracts goes hand-in-hand with risk assessments. Some vendors tout their products as HIPAA compliant, but the actual contract language may not be so simple. Others may pledge to comply with governmental laws and regulations but remain silent on standards or certifications by private groups such as CCHIT or Health Level 7. Trites has seen at least one contract state explicitly that the software would not meet requirements for a legal medical record.

Vendors may be more or less receptive to making changes to their products depending on the requested modification. "If the vendor's goal is to make the customer happy, and it's a rational request, the vendor will work to put a plan in place," says Underwood of the EHR Vendors Association. If the vendor is unable to solve the problem directly, organizations should push for other solutions, such as retention backups or hard copies of records, advises Lefar, who previously was an executive with an EHR vendor. User groups may be a promising venue for addressing issues, since vendors may be more willing to make modifications requested by multiple clients. Any agreed-upon modifications should be specified clearly in contract amendments.

As their organizations search for comprehensive fixes to EHR auditing challenges, HIM professionals should look for ways to beef up record verification and audit mechanisms in the meantime, advises Kathy Westhafer, RHIA, CHPS, program manager for clinical information access at Christiana Care in Wilmington, DE. "It's easy to be a defeatist and say the system's not robust, but see if there are some things you can hold on to and accomplish with what's there," she says.

Doing so may require a return to paper, at least temporarily. "The computer's just a tool, and you may not be able to automate 100 percent of processes," observes Soloman Appavu, director of systems planning at Cook County Bureau of Health Services in Chicago and cochair of the CCHIT security and reliability work group. "You may have to do some things manually. There may be no other way around it."

Improving verification and auditing processes in the short term may mean changing policies or not activating certain EHR system functionalities. For example, after compliance, legal, and HIM staff reviewed its clinical information system, Christiana Care decided not to enable the physician coding function, which allows physicians to complete documentation and coding for the same encounter, says Westhafer. The feature is only used for training residents.

Addressing Issues up Front in New Purchases

Organizations in the process of purchasing EHR applications should address record verification and audit concerns up front, provided HIM, compliance, legal, and internal audit staff are involved. These personnel are crucial in establishing and realizing security and access-related goals and policies. "If you're not invited to the table, invite yourself and be knowledgeable when you get there. Do research and cough up staff if necessary," advises Westhafer.

Defining how you want to maintain and monitor records helps more than your own organization, says Underwood. It also helps the vendor understand and better meet your needs. HIM should be part of any team that meets with existing clients of vendors under consideration. "Talk with four or five who have a lot of data and ask them to show how they do process audits. Be sure you can do the type of audit you want," advises Lefar. Organizations should specify desired functionalities in requests for proposal, and vendor commitments should be carefully spelled out in contracts.

Once an application has been chosen, extensive testing both before and after implementation can pinpoint any unforeseen glitches. "You can only do so much testing before going live," observes Michael Hoper, vice president of organizational integrity and audit services at Trinity Health in Novi, MI. "Don't listen to people who say you don't need to test much afterward. These are highly complex processes that cross multiple areas, and you need to test extensively after you go live."

Discussion and group problem solving are probably the best tools for meeting audit and record verifications challenges. "Keep the conversation going," advises Westhafer. "The more people you engage, the more solid ideas will surface and the more you'll come to know the right course for your organization."

Too Much Information?

Is there such a thing as too much auditing? EHR applications with robust verification and auditing capabilities have the potential to capture an enormous amount of data--likely more than an organization may need or can manage. In such cases, the question becomes how to capture and process the right data.

"Are you really going to follow up on 100 potential inappropriate uses to get to one? You can hire an army to do auditing, but that's probably not a good use of time and resources," contends Westhafer. Determining the appropriate level of scrutiny is a function of each organization's characteristics. "If

you're in a solo practice physician office, that's a different risk proposition than a 1,000-bed teaching hospital that has enabled community physicians to access certain parts of the medical record," explains Hubbard. "It boils down to meeting the legal requirements and your own comfort based on organization-specific risk."

An organization's place within its community can be another consideration in determining appropriate audit levels. Christiana Care is a major employer in Wilmington, and it is entirely conceivable that an employee would have legitimate reason to access records of a neighbor in the normal course of business, Westhafer explains. Auditing that type of transaction might produce unmanageable and ultimately fruitless audit results. In such instances, it is necessary to pinpoint transactions that should prompt actionable audits.

A New View of Security Audits

There is growing distinction in the industry between tracking actions at the application level and monitoring security at the broad system level, notes Harry Rhodes, MBA, RHIA, CHPS. This has come about as the industry has gained more experience implementing and managing EHRs. "Originally security audits were seen as the way to track all events that occur in an EHR system," says Rhodes, director of practice leadership at AHIMA. "With experience, there is the realization that proper security administration focuses on assigning and enforcing user access levels and privileges."

In other words, it is outside the scope of an IT security administrator to track and investigate every content change that occurs in an EHR system. If a data entry mistake occurs, says Rhodes, a designated user with assigned privileges enters the system and updates the record. That update should be tracked and logged--but at the application level, not the system security level, because the user acted within his or her access privileges. Security auditing at the system level should be limited to investigations of users that have exceeded their assigned access levels or privileges. Attempting to track every authorized update made at the system security level will bog down the system, says Rhodes.

System performance is an important factor, agrees Appavu. The more data collected, the greater the demand on an organization's processing capability. "If you track every little interaction, the system will come to its knees," he says. To avoid information overload, organizations must balance risks and resources to capture a manageable amount of data.

Gina Rollins *(rollinswrites@worldnet.att.net) is a freelance writer specializing in healthcare.*

Article citation:
Rollins, Gina. "Following the Digital Trail: Weak Auditing Functions Spell Trouble for an Electronic Record" *Journal of AHIMA* 77, no.3 (March 2006): 38-41.