Following the Electronic Trail

Save to myBoK

How can you protect patient information while maintaining immediate access for qualified employees? HIM professionals across the country are taking leadership roles in developing and managing audit trails for computerized health information. Here are a few of their success stories.

Random Reviews Reduce Incidents

Our hospital information system has a module that pulls information from all the clinical and financial aspects of the patient's medical record into one screen. Every other month, we randomly select users from every department and pull an audit trail that shows what they have viewed. The module lists the patient's name, terminal used, date and time, and what module (i.e., lab results, history and physical, etc.) the employee was viewing from. We route these audit trails to the employee's manager. The manager is responsible for reviewing the audit trails and investigating if it appears that the patients that were viewed were not appropriate for the particular employee.

One of our biggest problems was employees viewing a family member's information. Now that they know their name could be pulled for an audit review, inappropriate viewing of information has been reduced.

—Patti Brooks, RHIA, IS Director Avera Queen of Peace Health Services, Mitchell, SD

The Numbers Tell the Story

I investigated, selected, and implemented software for medical transcription that allows control/auditing of creation, editing, printing, and viewing of documents based on user security levels. The software has been in place for almost five years now and is viewed as a real benefit to the care team. We reduced the number of ad hoc/unscheduled record pulls for phone calls by more than 30 percent, while the number of patient visits increased by more 25 percent in three years. Online access to the records was certainly a tremendous factor in easier and quicker access for the staff.

—Eve Frisell, RHIT, Document and Records Specialist ADV Document Systems, Inc., Minneapolis, MN

Taking an Aggregate View

At my facility, we have a computer-dependent consumer database of all critical information documenting the delivery of clinical services to consumers, which automatically creates the required billing information for third-party payers. We have several data entry screens that contain numerous data entry points for more than 7,000 consumers currently managed in the database.

Access to this confidential information is controlled by managerial decisions. These decisions are implemented by our network administration staff, who assign varying levels of rights to the database users.

Also built into this proprietary database are numerous activity reports that can indicate to management the number of times users access the database, the screens used, data entered, and other reports that aggregate the critical utilization management data related to access. In addition, we have fundamental policies in place regarding restricted access to and appropriate use of this database, all of which can also be aggregated by network-level user reports.

—Jane McCoy, Coordinator of Medical Records Spindletop MHMR, Beaumont, TX

Database Leads to Far-reaching Results

We created a database to track every regional information system user account for Providence Health System in the Oregon region. The database lists an employee's accounts and the attendant level of access to patient data and system resources, as well as department, position, and the date(s) the accounts were created or modified. Regional information system accounts must be authorized by a manager or manager's delegate and appropriate to the user's department, position, and function.

This database is audited regularly and updated for changes to user employment status. Application-level audit trails have been implemented where applicable, and Internet access is audited regularly.

—*David Thornton, RHIA, IT Security Analyst Providence Health System, Tigard, OR*

Article Citation:

"Following the Electronic Trail." *Journal of AHIMA* 71, no. 8 (2000): 49.