March 2014
Chicago Lawyer®
Volume 37 Number 03 • chicagolawyermagazine.com

MedMal Matters > column

Another high-tech tool for plaintiff lawyers

By Thomas A. Demetrio
Corboy & Demetrio

By Kenneth T. Lumb
Corboy & Demetrio

According to a report issued last month by the inspector general of the U.S. Department of Health and Human Services, many hospitals have not implemented important safeguards in hospital electronic health record (EHR) technology. Nearly all hospitals with EHR technology have audit-trail capabilities, but nearly half of hospitals surveyed reported that their systems allowed inappropriate opportunities to delete, disable or alter audit trail information. Though the purpose of HHS' survey and report was to minimize fraud, its findings are equally relevant to lawyers who try medical negligence cases.

EHRs replace paper records with computerized record-keeping to document and store a patient's medical information. According to HHS, EHRs may contain patient demographics, progress notes, medication lists, medical history and clinical test results from healthcare encounters. According to a bulletin published by the National Institute of Standards and Technology's Computer Security Resource Center (CSRC), an audit trail is a record of computer events about an operating system, an application and/or user activities. Audit trails maintain a record of system activity both by system and application processes and by user activity of those systems and applications.

In general, according to CSRC, an audit trail is a technical mechanism that helps managers maintain individual accountability. By informing users that their actions are tracked by an audit trail that logs user activity, employers promote proper user behavior. One type of audit trail the CSRC describes provides information about users "suspected of improper modification of data." An audit trail in this situation can reveal "before and after versions of records." It is particularly important, the CSRC notes, to "ensure the integrity of audit trail data against modification." Audit trail data must be protected, the agency writes, because intruders or violators may try to "cover their tracks" by changing audit trail records.

According to HHS, audit trails or log-in EHRs track access and changes within a record chronologically by capturing data such as date, time and user information for each update to an EHR. Audit logs should always be operational and should be stored as long as the clinical record itself. In addition, HHS writes, users should not be able to alter or delete the contents of the audit log.

The potential benefit of audit trail information in a medical negligence case involving EHRs is obvious. No longer must an attorney hire a handwriting expert to analyze ink colors and handwriting samples in an effort to determine when an exculpatory note was actually drafted.

According to a 2009 article by Patricia McCartney in *The American Journal of Maternal/Child Nursing*, a properly prepared audit trail will conclusively demonstrate the identity of each system user, the date and time of access and what the user did each time the record was accessed: "view the record, create an entry, edit an entry or delete an entry."

The possible uses for this metadata are endless. A clinician claims he never saw a radiology report? Check the audit log to prove he accessed the report before he sent the patient home from the ER without telling the patient about a suspicious mass on his lung.

A nurse testifies, based on a "contemporaneous" note, as to the textbook response to a code? Check the audit log to learn that her entries were made three hours after the patient died and after she had spoken to the risk manager.

In spite of the manifest value of audit trail information, custom has not yet caught up with technology. Most lawyers' standard requests to produce in medical negligence cases do not include requests for audit-trail information. Indeed, the Illinois Supreme Court's standardized "medical-malpractice interrogatories to defendant hospital" do not include audit logs and do not even mention EHRs.

When queried, many hospitals claim that they have no capability to retrieve audit trail information or that they aren't required to preserve it. They are simply wrong. A combination of various federal statutes and regulations, including the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act require hospitals using EHR systems to create and preserve audit trail information.

Plaintiff lawyers should ascertain in every case whether and to what extent an EHR exists. Many hospitals maintain both paper records and electronic records as they transition to a pure EHR system. Some facilities will produce the paper records with no indication that electronic records exist or vice versa. The patient's lawyer should also request a complete but targeted audit trail early in relevant cases and make sure the information received is complete. A complete log should contain every electronic entry for the time period requested; the time each entry was made; the identity of each user accessing the record and the time the access occurred; the part of the record accessed; and what the user did: created a note, changed a note, viewed a note, etc.

Audit trail capabilities in EHRs may be a boon to government anti-fraud efforts but they are at least as valuable to patients' lawyers trying to discover the truth. ■

TAD@corboydemetrio.com
KTL@corboydemetrio.com