Follow the Audit Trail

May 2014 - Jennifer Keel

Every activity and entry in a patient's medical records. These online logs can provide crucial evidence in your client's medical malpractice case if you know how to obtain and use them.

Every time a user views, edits, prints, deletes, downloads, exports, or otherwise manipulates any part of a patient's electronic medical record (EMR), the system makes a contemporaneous record of that activity as it occurs. This audit trail provides direct evidence of exactly what was done — when, where, and by whom — to a patient's EMR.

Another way to think about the audit trail is metadata about the patient's chart itself. Consider an ordinary document on your computer. With a few clicks, you can view its properties — that information is metadata about the document. If you open the document, even without making changes, the metadata will change. Similarly, the audit trail is the metadata for a patient's chart that changes every time the chart is accessed or altered.

The use of EMRs has been on the rise since 2004, when President George W. Bush launched an initiative to computerize health records.[1] This progression advanced exponentially when the Centers for Medicare and Medicaid Services offered incentive payments to clinicians and hospitals when they used electronic records to achieve improvements in patient care.[2] Along with this increasing use came more concerns about privacy and security. Despite these concerns, audit trails have become an integral part of the medical system and medical malpractice litigation. They are an important tool at your disposal, but first you must know how to obtain them and use them to your client's advantage.

HIPAA set the national standard for maintaining patients' medical information, including electronic data. One of its purposes was to ensure that medical records could not be altered without detection, to "protect the security and privacy of individually identifiable health information,"[3] but the statute alone was insufficient to fully address the expanding range of issues inherent in the transition to completely electronic systems. In 2003, the HIPAA Security Rule was passed. It requires regular monitoring of system activity, including audit logs and access reports, by IT personnel or compliance officers on a quarterly basis (if not more frequently), as well as the implementation of hardware, software, and procedural mechanisms to record and examine system activity.[4]

The documentation systems other departments use may not show up on an audit inquiry of the main clinical documentation system.

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was passed to promote meaningful use of health care technology.[5] Unlike older laws, which were written with paper records in mind, newer laws contain provisions addressing technological advances in health information. The HITECH Act specifies that EMR systems must satisfy certain requirements, such as recording access to patient records, showing who viewed or changed information, when this was done, and from what location. Together, these statutes provide a legal framework that requires organizations using EMRs to track and maintain a log of all access to electronic records.[6]

EVIDENTIARY CLUES

What can you learn from an audit trail to help your client? The possibilities abound. Suppose your client was discharged from the emergency room without discharge instructions, a key issue in your case. Many months into litigation, a copy of discharge instructions appears for the first time. The hospital tells you that it existed all along and was inadvertently omitted from every certified copy of the chart previously produced. In the past, you had little choice but to take the hospital's word for it, but today you can check the audit trail. It may reveal conclusively that no one printed discharge instructions for your client before she left the hospital, but that after suit was filed, someone accessed the chart and printed the instructions, just days before they were disclosed to you.[7]

We have all taken depositions where providers claim to have a clear recollection — years later — that they made key entries contemporaneously and were at your client's bedside during every important event in his or her care. Don't believe them? Get the audit trails showing which computer terminals they used to enter information and when. You may learn that all the entries were made hours later, and that a nurse was in another patient's room entering information into someone else's chart when he or she claims to have been with your client. In fact, audit trails can be run to show a certain care provider's activity and do not have to be confined to a particular patient. This might be done to demonstrate, for example, patterns of documentation failures or suspicious narcotics handling by a particular nurse.[8]

If you want to know whether the nurse who claims to have charted contempo-

1. George W. Bush, Address, President Bush Discusses Quality, Affordable Health Care (White House, Washington, D.C. Jan. 28, 2004), www.georgewbush-whitehouse.archives.gov/news/releases/2004/01/20040128-2.html.
2. 42 C.F.R. §495.2—Standards for the Electronic Health Record Technology Incentive Program.
3. Smith v. Am. Home Prods. Corp. Wyeth-Ayerst Pharm., 855 A.2d 608, 611 (N.J. Super. L. Div. 2003); see also R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 720 (W. Va. 2012), cert. denied, 133 S. Ct. 1738 (2013).
4. 45 C.F.R. §§160, 162, 164 (2014); 45 C.F.R. §164.308(a)(1)(ii)(c); 45 C.F.R. §164.312(b).
5. 42 U.S.C. §300jj (2014), §17901 (2014).
6. See e.g. 42 U.S.C. §1320d (2014); see also 45 C.F.R. §§160, 164, 170.
7. See e.g. Pl.'s Mot. to Compel Prod. of Audit Trail Docs. at 8, Hand v. Girard, 2012 CV 353, (Colo. Arapahoe Co. Dist., July 19, 2013.)
8. Nimoh v. Allina Health Sys., 2011 WL 4008313 (Minn. App. Sept. 12, 2011).

raneously at the terminal in your client's room was telling the truth, focus the audit request on that nurse without limiting it to your client. In that instance, you might ask for the audit records that show every time that nurse accessed the system from any terminal during a certain period. Defense counsel will balk at this and claim that your request violates other patients' HIPAA rights, but the audit records can be pulled without patient identifiers if the query specifies that, or they can simply redact the confidential information.[9]

You might discover that someone accessed or altered your client's records for inappropriate reasons, and reviewing audit records can reveal such activity.[10] Or, you may discover that people whose names do not appear in the medical record or were not disclosed as witnesses accessed the chart and had a role in providing care. They may be unit clerks responsible for clerical duties, nurses assigned to other patients who stepped in to lend a hand, or technicians in other departments, such as radiology. Hospital employees may have made entries in sections of your client's chart that were never produced to you, such as a telephone log or radiology records system. A detailed timeline will begin to unfold in your client's audit trail — as well as an inventory of witnesses and documents — that is not apparent from the medical records alone.

AUDIT TRAIL PRODUCTION

Request the audit records you want in discovery, but be prepared to file motions to obtain the information. Defense counsel may deny that it exists, argue that they cannot access it, that it is irrelevant, or that you're not entitled to it. I have not yet encountered a claim of privilege in response to an audit trail request, but that too may be inevitable. None of these objections holds up under close scrutiny.[11]

Know what you are seeking, and tailor your requests. Audit trail records are obtained by querying a database with various search terms—such as information identifying a patient, a provider, a location in the hospital, a particular EMR system, a date or time span, and a specific visit. The fewer parameters entered, the wider the inquiry will be. For example, your client's name and date of birth may produce a large pool of information, but adding a date of care would narrow the results. Specificity in your search terms is likely to increase your chances of success.

Before making any discovery requests, obtain a copy of the hospital's policy manuals to improve the odds of receiving the audit records. These manuals contain policies that specifically address data security and auditing capabilities within the EMR systems. Often, these policy manuals also contain additional data about how the facility is organized and what information is available. Armed with this knowledge, you can tailor the language in your discovery requests. It will be far more difficult for your opponent to claim they do not understand your requests when you can refer them to their own internal policies.

Once you receive the audit trail documents, be skeptical. Although federal law prohibits editing the audit trail records in the EMR system,[12] the information can be altered once it is exported to a spreadsheet. Key items might be deleted or changed before the document is produced in discovery. Insist on the unedited, original electronic format of the document, and have a forensic expert examine it to ensure no one tampered with it. Do not accept other formats, such as a PDF document.

Be wary of audit trail records that omit evidence of EMR access at the time the audit report is run and/or after the patient was discharged.

For example, suppose your client was discharged from the hospital on Dec. 1, 2012, and you request a copy of the patient's records for that visit today. The audit trail should show that the records were accessed, viewed, and printed shortly after your request to be produced. It should also contain other entries concerning billing, doctors' post-release notes, and other housekeeping matters. If the audit trail simply ends at the time your client was discharged, you know that something is missing.

Also question audit records that lack evidence of any EMR access from the lab, radiology, pharmacy, or other departments within a hospital. Many of the EMR platforms are "closed systems," which means they cannot be integrated with other systems in the hospital. The documentation systems other departments use may not show up on an audit inquiry of the main clinical documentation system. Each database that is not directly connected to the main clinical charting system must be queried as part of a records search.

9. Courts may order other patients' identifying information be redacted. See Or. re Pl.'s Mot. to Compel Cir. at 3, Ruchotzke v. Roberts, 13-L-78 (Ill. Peoria Co. Cir., Jan. 22, 2014).
10. See Bryant v. Jackson, 2013 WL 5529322 (Mass., Suffolk Co. Super. Sept. 17, 2013); Yath v. Fairview Clinics, N. P., 767 N.W.2d 34, 38, (Minn. App. 2009).
11. See e.g. Pl.'s Mot. to Compel Prod. of Audit Trail Docs. & Def. Resp. to Mot. to Compel (Aug. 9, 2013), Hand, 2012 CV 353; see also Pl.'s Mot. to Compel (Nov. 27, 2013), & Def. Resp. to Mot. to Compel (Jan. 17, 2014), Ruchotzke, 13-L-78.
12. See 45 C.F.R. §170.302(s)(3) (2014) (regarding integrity of audit logs).

DEPOSITIONS

Once you have the documents, you may find that the complexion of your case changes. If you have witnesses who have already been deposed, go back and compare their answers to the evidence in the audit trails. Use those discrepancies to your advantage when deposing future witnesses. If you can obtain the documents before deposing anyone, you have the option of either cornering a witness with the information in the audit trail or letting him or her advance unaware through your questions to his or her detriment. In either case, it is often surprising how many providers forget that their activity is monitored in the EMR. They will assert their clear recollection of a story that serves their interests in almost every case, without regard to whether your next line of questions may trap them in a lie.

OVERCOMING OBJECTIONS

You will encounter objections when requesting audit trail records, and a few of the most common are discussed here.

The audit trail is too burdensome to collect or produce. This is by far the first and loudest objection, and it is simply untrue — audit trail information is easy to collect and produce. Hospitals employ highly trained IT staff, including database administrators and technicians, whose principal job is managing the hospital's databases and running queries against them. Producing audit trail reports is an ordinary function of this job. While the defense will try to portray your request as unique and bizarre and one that they have little hope of being able to comply with, you are not the first person to demand production of audit trails during litigation.

Facilities using EMRs must keep these logs and provide access to them as required by law (and must demonstrate compliance with these statutes to maintain their federal accreditation), so there is already a maintenance and retrieval process in place for audit trails — which is described in the policy manuals. In short, defendants know what you're asking for and how to provide it. They may need to do it for Medicare or Medicaid, for internal purposes, in response to concerns or complaints about HIPAA violations, or for various other reasons.

Defense counsel may argue that such a request is unduly burdensome for their client, but audit trail production is a simple database query usually done by IT staff, and it does not take clinicians away from their patient care responsibilities. Someone types in the search terms and sets the search engine to work. The completed report is exported into a format for use — usually a spreadsheet. Your requests should always be for the unaltered, native electronic format of the audit trail (not a printout). And, because the files are electronic, there is no burden of printing a voluminous record.

The audit trail is not part of the medical record. To the contrary. Because the audit trail is metadata about the medical record, it is undeniably part of the record. In fact, it cannot be separated from the EMR, because every time someone accesses the record, a corresponding entry in the database is generated, tracking access. This data is an integral part of the record and provides direct evidence about the care your client received from the facility and the individual medical providers. Although the audit trail will not provide medical assessments, such as the patient's vital signs, it will tell you who charted these observations; whether they were changed; and who viewed the information subsequent to its entry, printed it, or deleted it, and when. This data is a more accurate record about the care that was rendered than the chart alone.

The audit trail is irrelevant. You can show how this evidence is pertinent to your case in numerous ways. At a minimum, it can give you a list of every person whose credentials were used to access the chart, which will reveal potential witnesses who were not apparent from the records themselves.

The audit trail is the only objective account of when your client's data was viewed and charted. The timing of when providers looked at test results or made entries often becomes a critical issue. Just as the EMR provides a more accurate account of what happened with the patient at the time in question than recollections years later during litigation, the audit trail gives a more precise snapshot of who manipulated the record, wwhen, and for what purpose. If you cannot locate a provider, that provider's audit trail may be the only reliable "testimony" you can obtain.

Because providers cannot document every detail associated with patient care, the audit trail often fills in gaps about undocumented occurrences: when your client's discharge instructions were printed, when the doctor viewed test results, or whether he or she did so from home or at the patient's bedside. Of all the hurdles you may face in obtaining an audit trail, the relevance objection should be the easiest to overcome.

Discovery of audit trails is a relatively new and underused tool for plaintiff lawyers. In the future, audit trails may be routinely provided as part of a medical records request, but you need to know how to obtain them now. The effort will pay off in developing cases for trial. ❧

Jennifer L. Keel, JD, is a shareholder at Burg Simpson Eldredge Hersh & Jardine in Denver. She holds a BS (SCL) and Master's in Intelligence and National Security Studies, was a paramedic for six years in a large urban area, and served as a tissue procurement team leader for a human parts and eye bank. She co-teaches a class in medical malpractice litigation with the Sturm College of Law in Denver. She has published articles on various topics in medical negligence, and has lectured in various continuing legal education programs across the country. She may be contacted at jkeel@burgsimpson.com or 303-792-5595.