Health Record Audit Trails: How Useful is the Metadata that is Associated with a Patient's Health Record?

By Jennifer A.W. Rush, Esq. Gone are the days when your doctor carried a manila folder into the exam room with her, shuffling through it to find the last office visit note or your current list of medications. Paper charts have been replaced by electronic health records, or "EHRs," which are now in wide use in hospitals and medical practices around the country. Now, doctors carry their laptops everywhere with them, retrieving and creating health information with a click of a button. We are slowly catching up with what this technology has to offer, and the problems it creates, when it is used in litigation. By now, we have all heard about electronic discovery. In fact, almost every time we request a medical record, we are engaging in a form of electronic discovery because the "record" can no longer be photocopied from a chart on a shelf, but must be transferred from an electronic format into a format that is compatible with production. Not being able to inspect the original paper chart at a deposition and instead trying to determine if everything has been printed from the computer is a task to which all those who litigate injury claims have become accustomed. We are also mindful of the fact that what the physician or nurse sees on the screen when viewing a patient's record looks markedly different from the format in which it is printed. Moreover, information in the EHR changes over time in ways that information in a paper chart cannot. Added to these changes is the fact that with EHRs, there is "information about the information" – metadata about the record that never existed with paper charts and is kept in an "audit trail." We are beginning to see routine requests for the "audit trail" associated with the EHR, and the benefits and problems that these requests bring to litigation are just beginning to surface. A.What is an "audit trail"? An audit trail can be defined in basic terms as a "record that shows who has accessed a computer system, when it was accessed, and what operations were performed." Brodnik, Melanie, et al., *Fundamentals of Law for Health Informatics and Information Management*. Chicago, IL: AHIMA, 2009, 215. Pursuant to the Health Insurance Portability and Accountability Act (HIPAA), medical providers who use EHRs must have systems in place to review and audit access to records, as well as prevent unauthorized access. 45 C.F.R. §§ 164.308(a)(1)(ii)(D), (a)(3)(i), 164.312(1)(b). Compliance with HIPAAs requirements is routinely obtained through the use of audit trails, which track the information required by HIPAA and provide a mechanism for determining if there has been a security breach. One of the problems is that there are a variety of different vendors of EHRs and thus, a variety of different formats for audit trails. If you are using audit trails in litigation, you cannot count on the audit trail from Hospital X to look anything like, or contain the information contained within, the audit trail from Hospital Y. EHR certification requirements mandate that the following data be recorded in an audit trail: type of action (additions, deletions, changes, queries, print, copy); date and time of event; patient identification; user identification; and identification of the patient data that is accessed. *Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology*, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule (September 4, 2012). Beyond these basic requirements, there is a wide variety of information recorded among different EHR vendors. B.How are audit trails used in litigation? Audit trails are not part of the "patient record" and should not be automatically produced when there is a request for the record. Instead, they must be specifically requested and the

©2026 Norman Hanson DeTroy LLC All Rights Reserved

validity of the request must be analyzed on a case-by-case basis. The request for an audit trail, like any other discovery request, is subject to Maine Rule of Civil Procedure 26's requirement that the request be "reasonably calculated to lead to the discovery of admissible evidence." As everyone involved in litigation knows, Rule 26's standard is a broad one. Nonetheless, there is a duty on the part of the individual making the request to at least articulate why the audit trail might provide admissible evidence in the case. By far, the most common use of audit trails is in medical malpractice actions. For example, if there is a question of when a physician viewed an x-ray report, or a lab result, the audit trail may be able to provide that information. This may have a significant impact on the liability of the medical provider. If the timing of a particular chart entry is important to the prosecution or defense of a case, then the audit trail may be able to shed light on that issue. In any personal injury case where the plaintiff's compliance may be an issue, audit trails may be able to reveal information regarding how many times the patient changed or failed to show for his appointment, for example. Moreover, if the plaintiff's presentation at a specific office visit is important and the chart does not identify the nurse who admitted the patient, then the audit trail should contain that information and lead to the identity of a potentially key witness. C.Audit trails cannot be used in a vacuum; they require explanation. In general, audit trails make poor witnesses and are simply launching pads for additional discovery. They are indecipherable to most people, inconsistent between medical practices, and often unreliable. When justifying their request for an audit trail, requesting parties often argue that the trail will tell them exactly what information was accessed and modified by what user, and when, but in reality the story told by an audit trail is rarely that straightforward. The audit trail seldom reveals the substance of the information that was changed or added. We also know that even though they are supposed to do so, system users often fail to "log off." For example, if a physician and a nurse happen to be in the emergency department exam room at the same time, they may both enter information into the computer but will use only one person's log-in information. A case example involving Northshore University Health System provides an excellent example of why the use of audit trails should be approached with caution. In that particular case, the parties had already spent an extraordinary amount of time and resources on the production of the EHR and the plaintiff held a fair amount of suspicion regarding the accuracy, completeness, and reliability of the HER itself. Chris Dimick, *EHRs Prove a Difficult Witness in Court*, Journal AHIMA (Set. 24, 2010). When it came time to producing and dissecting the audit trail, even more suspicion arose, even though the explanations for the purported inconsistencies were explained by technology and completely outside of the hospital's control. By way of background, when audit trails are printed, they look like Excel documents. One column will include the patient's identifier, which is usually a unique combination of letters and numbers assigned to that specific patient. Sometimes, however, an individual patient will have several different identifiers that are unique to the hospital admission or the type of care received. Radiology departments, for example, usually use their own electronic record systems that interface with the patient's other electronic records. Another column, or columns, will provide one or more date stamps, depending on the vendor of the EHR. Additional columns will identify the user of the record by name, a unique code, or both. The general description of the portion of the record accessed will be provided in another column, but the description is generally not specific enough to provide true substantive information. For instance, the description may be "VITALS GRAPHIC I&O REPORT," which will reveal that the user viewed the patient's record of volume input and output, but does not tell us what information on that I&O report was viewed. Or, the entry may simply read "NURSES NOTES PROGRESS NOTE REPORT," which tells us absolutely nothing about what progress note during a multi-day admission was viewed by the user at that particular time. Another column in the audit trail will indicate the "action," which is where Northshore University Health Systems ran into problems. The "action" is usually described by one word – query, modify, accept, view, etc. As with most audit trails, Northshore's audit trail's use of the word "accept," meant

©2026 Norman Hanson DeTroy LLC All Rights Reserved

different things depending on the type of record and the circumstances. It could mean that the record was pended, filed, shared, or actually accepted by a physician. Chris Dimick, *EHRs Prove a Difficult Witness in Court*, Journal AHIMA (Set. 24, 2010). This became a problem when the audit trail documented an "accepted" physician order that did not appear in the EHR. Northshore did not erase the order from the record or withhold it from production as one might infer, however. Instead, "accepted" in that particular instance meant that the order was "pended." Because the order was never executed, it never appeared in the EHR even though it appeared, from the audit trail, as though it was an "accepted," or final, order. *Id*. There have been other cases were time stamps have proved unreliable. In one case, the audit trail produced by a hospital showed that the user opened dozens of documents within the same second. The IT department demonstrated that it was physically impossible to open all of the documents at the same time, and likewise physically impossible to view them all at the same time. The best explanation provided by the IT department was that when one document was opened, the system showed all the documents in that "batch" or grouping as having been opened. The audit trail in that instance proved meaningless when trying to sort out whether a specific person actually viewed a specific document. D.Practical implications in litigation. Parties who request and use audit trails must be aware that although they may prove useful in some cases, they will, invariably, require explanation. At a basic level, the parties must become educated on what the information in the various columns means, and whether it is reliable. If the audit trail comes from a hospital, then the hospital may need to produce a member of its IT department for a deposition. Smaller medical practices, however, may not employ anyone who possesses enough knowledge about the audit trail to provide litigants with meaningful information. After all, the audit trail was not designed to be used in litigation. It is a compliance tool that enables medical providers who use EHRs to meet the requirements set forth by HIPAA. In these cases, parties may need to go to the source – the vendor of the EHR – or hire experts in order to give meaning to the information in the trail. The added time and cost associated with this discovery is not warranted in every case. By the time the parties have concluded that the information in the audit trail justifies the added burden, however, the medical provider may have changed vendors for its EHR, archived the trail (which can make the data even more incomprehensible), or otherwise lost or destroyed the data that the parties seek. Accordingly, at least in medical malpractice actions where the health provider is a party, a well-crafted litigation hold letter in lieu of an automatic discovery request for the audit trail makes practical sense. Parties must also remember that audit trails contain protected health information. Accordingly, requests for audit trails that are maintained by non-parties must be accompanied by a Court order or a valid release that is signed by the patient. Moreover, litigants should not be surprised if health care providers require subpoenas in addition to patient releases before they will produce audit trails; the obligation on the part of a provider to produce the audit trail, as opposed to some other method of "accounting of disclosures" is not well-defined under HIPAA regulations. In summary, we are just beginning to understand the potential uses and burdens that are associated with the metadata attached to EHRs. The request for this metadata is not subject to the Rules of Civil Procedure alone, but must be analyzed within the framework of HIPAA and IT considerations. One thing is for certain, the change from paper records to electronic health records means that litigants must change their practices in how they request, interpret, and use medical records. And, in cases where the audit trail is a relevant source of information, this change will mean added cost and burden to litigants.

©2026 Norman Hanson DeTroy LLC All Rights Reserved