Audit Trail Use in Medical Negligence Cases

By: Elie A. Maalouf & Nick E. Abramson

I. Introduction

In medical negligence cases, the dogged pursuit of complete audit trail data can help achieve favorable results. In a recent case, the defendant medical practice produced an incomplete audit log with its answers to the plaintiff's discovery requests, which revealed that the defendant medical provider edited the medical record, but failed to identify what alterations were made. Our determination to discover the changes made by the provider ultimately paved the way to a successful resolution. This article will review the state and federal audit trail regulations that guided our pursuit of the audit data and it will demonstrate one of the many ways an audit trail can be used advantageously in a medical negligence case.

II. Audit Trail Regulations

An audit trail is an electronic log that documents each time a patient's electronic medical record is accessed. Both federal law—The Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act")—and New Hampshire law require audit trails as a security measure to protect the integrity of the protected health information contained within a patient's electronic medical record.[1] Health care providers are required to maintain an audit trail as part of every electronic medical record to ensure there is no unauthorized access or improper modification to that record.[2]

Federal audit regulations require that audit logs maintained by healthcare providers satisfy certain requirements such as recording access to patient records and showing who viewed or changed information. Specifically, audit trail logs must contain, among other elements:

> 7.1.8 *Type of Action (for example: creations additions, deletions changes, queries, accesses, copy, print, and copy and paste)*—Specifies inquiry, any changes made (with pointer to original data state), and a delete specification (with a pointer to deleted information).[3]

Indeed, "[f]ull transparency of modifications or deletions or both is mandatory…record changes shall not obscure previously recorded information."[4]

The ASTME E2147-18 publication, which is incorporated into the federal audit trail regulations and sets forth the industry standard for how audit trails must be maintained and produced, provides:

> Without exception, patients or personal representatives or both, advocates, or their designees shall have access upon request to disclosure reports, as well as audit logs, and the data contained therein.[5]

Likewise, HIPAA provides patients and their representatives an absolute right of access to their "protected health information." Specifically, 45 C.F.R. §164.524(a)(1) states:

> Right of access. Except as otherwise provided…an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set..."[6]

HIPAA also mandates that healthcare providers "provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format."[7] HIPAA also requires covered entities to develop notice of privacy practices, which provide clear explanations of a patient's rights to their personal health information, including the patient's and the patient's personal representative's right to obtain and inspect a copy of the patient's medical records.[8]

Similarly, New Hampshire law also provides that "[a]ll medical information contained in the medical records in the possession of any health care provider shall be deemed to be the property of the patient. The patient shall be entitled to a copy of such records upon request."[9] Indeed, "[w]hen an individual's medical record is maintained in electronic form, the individual has the right to a report, based on whatever audit trail of that record is then maintained, of access to the record by a health care provider named by the individual within an identified period in the prior 3 years."[10]

Healthcare entities are also prohibited under federal law from discouraging, preventing, or otherwise inhibiting a patient's access to their electronic health record. This practice is referred to as information blocking, which is defined as any "practice that…is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information," and the "provider knows that such practice is unreasonable and is likely to interfere with, prevent or materially discourage access, exchange or use of electronic health information."[11]

III. Audit Trails in Practice

In our recent medical negligence case, we represented the estate of a 52-year-old husband and father who presented to his new primary care physician seeking help for alcohol overuse and depression. As a result of the defendants' failure, among other things, to recognize the plaintiff's signs of alcohol withdrawal, assess him for alcohol withdrawal syndrome, direct him to an emergency department, and ensure that he was safely escorted from the office and to an emergency department, the plaintiff wandered into a locked stairwell at the defendant medical practice after his appointment and fell to his death.

Shortly after suit was filed in this case, we requested the defendant medical practice produce the plaintiff's complete medical records, including the audit trail data associated with those records. In response, the defendant medical practice produced an incomplete audit log, which revealed that the defendant provider made numerous edits to the plaintiff's medical records two days after he died. The audit log was clearly missing additional entries. Moreover, despite claiming in its answers to interrogatories that only one version of the medical chart existed, the practice eventually produced three different charts. We continued to request the completed audit trail data until the defendant finally produced the missing final entries, which revealed that the medical practice's chief operating officer (COO) was in the medical record at the same exact time the defendant physician was making her edits, indicating that COO was involved in the changes made to the record. Yet, the defendant practice did not identify those changes.

We repeatedly attempted to obtain a complete copy of the audit trail data in an effort to determine what was altered and why three different versions of the record existed. The defendant medical practice, however, continued to withhold the complete audit data, claiming its EMR system could not display what edits were made. Since federal audit trail regulations require healthcare providers to maintain audit logs that show any changes made to the record, we knew this could not be true. We retained an electronic medical records expert who was intimately familiar with the defendant practice's EMR system and he confirmed the EMR system was capable of showing the edits made by the defendant medical provider.

We sent a letter to defense counsel providing a detailed explanation from our expert about how to obtain the data and offered to have our expert participate in an informal conversation with the defendant practice's IT personnel or expert about how to obtain the data if the practice was unable to produce the requested information. We also informed defense counsel that if the practice was unable or unwilling to participate in an informal conversation with our expert we would file a motion with the court to compel the inspection of the plaintiff's electronic medical record, to which the plaintiff was entitled

under Federal law, New Hampshire law, and the defendant practice's Notice of Patient Privacy Practices.

Despite our numerous attempts to informally resolve this discovery dispute, the defendant practice failed to produce the requested data and declined our expert's assistance because it knew that providing this information would be harmful, if not fatal, to its case. Accordingly, we filed a motion to compel the inspection of the plaintiff's EMR, which immediately prompted defense counsel to agree to an inspection. We ultimately withdrew our motion but we are confident—as was defense counsel presumably—that the court would have granted the motion.

Shortly before the inspection was to take place, we successfully resolved this matter. Although we never learned what changes were made to the record, we were able to come to a resolution largely because the defendant medical practice did not want the inspection of the plaintiff's EMR to occur.

IV. Conclusion

Audit trails play a critical role in medical negligence cases and are essential in the search for the truth. As demonstrated by the foregoing case, the pursuit of the complete audit trail alone can help plaintiff's lawyers achieve favorable results for their clients and hold medical providers and their employers accountable.

---

[1] "Protected health information" is defined as "individually identifiable health information…that is (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium." 45 C.F.R. §160.103. "Individually identifiable health information" is further defined as health information that is created by a health care provider that relates to the provision of health care and can be used to identify the individual. *Id.* A patient's audit trail data is a part of that patient's "protected health information" because it is created by the healthcare provider, it relates to the provision of health care, it can be used to identify the patient, and it is transmitted and maintained in electronic media.

[2] *See* 45 C.F.R. §§ 164.306 & 164.312; N.H. R.S.A. 332-I:3(III).

[3] *See* ASTM E2147-18 at §7.1.8, Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems (incorporated by reference in 45 C.F.R § 170.210(e)-(h)).

[4] *Id.*, ASTM E2147-18 at §1.2.

[5] *Id.* at § 9.1.

[6] 45 C.F.R. §164.524(a)(1); see also 45 C.F.R. §164.502(g)(1) (stating that covered entities must treat personal representatives as the individual).

[7] 45 C.F.R. §164.524(c)(2)(i).

[8] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html#:~:text=The%20HIPAA%20Privacy%20Rule%20requires,plans%20and%20health%20care%20providers; https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#:~:text=With%20limited%20exceptions%2C%20the%20HIPAA,care%20providers%20and%20health%20plans.

[9] N.H. R.S.A. 332-I:1(I).

[10] N.H. R.S.A. 332-I:2(I)(g).

[11] 42 U.S.C.S. § 300jj-52(a)(1); see also Prieto v. Rush University Medical Center, No. 2018 L 003531, at *6 (Ill. Cir. Ct. 2022) (concluding "federal law says that audit trail data, including metadata associated with a patient's [electronic health record], is included in the patient's right of access and that it constitutes information blocking to refuse to produce such data").