What nurses need to know about metadata, documentation, and legal liability

M etadata analysis of information in a patient's electronic health record (EHR) has the potential to provide valuable information to attorneys in the case of a lawsuit. This information, such as patterns of missing data, can bolster a legal case, leaving nurses vulnerable to punitive action. The best way to avoid negative results of a metadata analysis and subsequent legal action is effective documentation.

Metadata in the EHR

One of the first steps a plaintiff's attorney takes when building a potential medical malpractice case is to review the documentation in the plaintiff's/patient's EHR. An EHR stores a wealth of information, including the data entered, when it was entered, who entered it, who viewed it, and whether it was modified. It also stores when someone simply viewed something and how long they were viewing it. All this information is referred to as metadata, which can otherwise be thought of as "data about data."

Metadata can be analyzed not only to identify single incidences of error, such as choosing the wrong descriptor from a checklist, but also to detect patterns that can provide insights into the nurse's care and support an attorney's case. For example, an attorney might use a metanalysis showing that a nurse is routinely late in documenting to imply that their work is sloppy, creating a negative impression that can affect the nurse's perceived credibility and even undermine their defense.

Federal Rules of Civil Procedures recognize that metadata are "discoverable." An attorney gains access to EHR information through e-discovery, which the American Health Information Management Association defines as "the pretrial legal process used to describe the method by which parties will obtain and review electronically stored information (ESI)". ESI covers any device (such as computers and tablets) and electronic data, such as email and progress notes and radiographic images in an EHR. E-discovery is a complicated process for both the attorney and the organization maintaining the EHR. Data usually are obtained via a computer-generated record of audit trails showing user access and actions.

Protection through documentation

In the case of litigation, metadata can play an important role in determining the credibility of evidence, including a nurse's testimony and documentation. A one-time minor error in documentation is not likely to affect the outcome of a case, but more substantial errors can have a significant impact. For instance, if you testify that you notified a provider of a change in a patient's status at 1130 but EHR data show you made the entry at 1630, without noting the late entry and when you notified the provider, your credibility may be affected. Frequent errors and errors of omission can undermine a nurse's credibility in court.

On the other hand, metadata based on your complete and accurate documentation can help exonerate you by bolstering your credibility and providing evidence that you adhered to your organization's policies and procedures and the standards of practice.

Documentation recommendations

Here are some recommendations that will help ensure your documentation serves you well in court.

- **Avoid documentation gaps.** An example is neglecting to document normal vital signs or routine medication administration when required. Missing information enables an attorney to construct a narrative that may not be flattering to you.
- **Don't copy and paste text from one patient's EHR to another.** It is too easy to forget to revise the text to reflect variations between patients.

> In the case of litigation, metadata can play an important role in determining the credibility of evidence.

Complete, accurate documentation reflects your practice and is a tool that helps in defending you in case of legal action.

- **Use templates and checklists cautiously.** These tools can save time, but they also can cause errors. For example, you may forget to revise a template to reflect a patient's condition.
- **Do not share your password.** Sharing passwords not only compromises cybersecurity, it also could lead to documentation errors such as another clinician entering their documentation under your name, or your profile being logged in to multiple devices at once.
- **Make any changes to the record as soon as possible, per organizational policy.** A correction of erroneous information is typically indicated in some way in the EHR. Information should not be deleted because that alters the record. Corrections are acceptable when made appropriately. However, negative narratives can be created when late entries or corrections have not been made according to organizational policy. You should also avoid making any changes to a record after receiving notice of a lawsuit, even if you intend to clarify points. In fact, you should not even access the patient's EHR again without first speaking with your risk management team or attorney.
- **Know that what you view is recorded.** The EHR will take note of what you view and for how long. This has implications beyond your own patients. For example, if another nurse asks you to pull up a patient's record for a second opinion, the EHR will store the fact that you looked at the patient's record, and how long you accessed it. You certainly want to provide assistance, but if your conclusions differ from the requesting nurse, it may be prudent to make your own note in the EHR.
- **Document referrals and notifications of other nurses about changes in a patient's condition.** You'll also want to document the response to notifications of changes. If you fail to receive an appropriate response, take further action, such as notifying your supervisor.

Documentation as a tool

EHRs have opened the door for detailed metadata analysis that can support—or not support—a lawsuit. Complete, accurate documentation reflects your practice and is a tool that helps in defending you in case of legal action.

Organizations, metadata analysis, and e-discovery as a tool

Organizations should be aware of the implications of what metadata analysis can reveal.

For instance, in a case described by Gardner, an analysis showed that a hospital turned off alerts in a clinical decision support system because they came up so often that clinicians ignored them. A plaintiff's attorney was later able to show that one of the alerts might have prevented injury to their client.

Organizations should have a detailed plan for responding to e-discovery requests. Attorneys Hansen and Pratt note that requests must comply with Federal Rules of Civil Procedure 26(b)(2)(C)(iii). The organization will need to supply the requested information unless they can show a court that doing so will create an undue burden or expense. Cnso

References

American Health Information Management Association. E-discovery litigation and regulatory investigation response planning: Crucial components of your organization's information and data governance processes. bok.ahima.org/doc?oid=107115#.ZByfmBXMJhE

Barrett M, DeAngelo TR, DeAngelo JG. E-discovery: Metadata analysis in medical malpractice litigation. *The Legal Intelligencer*. April 9, 2020. law.com/thelegalintelligencer/2020/04/09/e-discovery-metadata-analysis-in-medical-malpractice-litigation/?slreturn=20230223103325

Conn J. Making IT legal-size; As electronic health-record systems become more complex, so do the issues involving the legal status of those records. *Modern Healthcare*. 2008;38(20).

Gardner E. The weight of the I.T. evidence; why EHRs won't reduce your malpractice premiums. Health Data Management. 2013;21(10).

Hansen MD, Pratt TJ. Follow the audit trial: The impact of metadata in litigation. *Defense Counsel Journal*. 2017;84(3). iadclaw.org/defensecounseljournal/follow-the-audit-trail-the-impact-of-metadata-in-litigation

Shwayder JM. Electronic records and metadata: Old and new liability risks. *Contemporary OB/GYN Journal*. 2018;63(9). contemporaryobgyn.net/view/electronic-records-and-metadata-old-and-new-liability-risks