Metadata, Law, and the Real World: Slowly, the Three Are Merging

Save to myBoK

*by **Reed D. Gelzer**, MD, MPH, CHCC*

Under certain circumstances, outputs such as electronic or printed documents from computerized systems can be admitted into legal proceedings as appropriate representations of business records.[1] However, in order to be valid and admissible, they must adhere to well-established business record requirements.[2] This adherence requires additional levels of proofing for outputs from electronic systems, including:

- The type of computer systems used and their acceptance as standard and efficient equipment
- The record's method of operation
- The method and circumstances of preparation of the record, including the sources of information on which it is based; the procedures for entering information into and retrieving information from the computer; the controls, checks, and tests used to ensure the accuracy and reliability of the record; and ensuring the information has not been altered[3]

Electronic records thus must meet additional criteria to ensure their validity and admissibility in legal proceedings. Newer criteria are evolving to bolster the trustworthiness of electronic records. Among these are requirements related to metadata.

The Law: Metadata a Must

To ensure the validity and admissibility of evidence from electronic systems, the legal system has further specified detailed requirements for the preservation of records and the preservation of data about those records. These requirements increasingly direct attention to supportive data, or metadata, to substantiate core authenticity functions such as the date, time, and original, actual author(s) of documentation actions, including legitimate alterations.

Although the legal system hasn't outlined what specific metadata are required in all instances, case law nonetheless has mandated that metadata are necessary for outputs to be admitted into a legal proceeding. The updated federal e-discovery rules outline procedures for identifying and submitting electronic data and its supporting metadata.

Metadata were a major determinant of a case in which an anesthesiologist's attendance attestation statement showed that he documented his presence for an entire case only a few minutes into a very lengthy surgery. The metadata provided the evidence that this statement's documentation was demonstrably false when executed.[4]

Another case, *Williams v. Sprint,* is often cited as a landmark concerning metadata. It established the following standard:

> When a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.[5]

Metadata are also inferred from the updated False Claims Act's reference to supporting materials needed to interpret electronic documentation:

> The term "documentary material" includes the original or any copy of any book, record, report, memorandum, paper, communication, tabulation, chart, or other document, or data compilations stored in or accessible through computer or other information retrieval systems, together with instructions and all other materials necessary to use or interpret such data compilations, and any product of discovery.[6]

The legal community is becoming increasingly attuned to metadata's importance and requirements. A recent article on EHRs and malpractice risk notes, "Metadata is discoverable under the federal electronic discovery rules, but courts will have to decide when and how it can be used on a case-by-case basis. The discovery rules may require that metadata created by computer prescriber order-entry systems be produced, even in situations for which hospital policy does not require the data to be integrated into a patient's permanent health record."[7]

The Real World: System Variability, Standards Lacking

Metadata have become part of functional requirements for EHRs. In part this derives from the high degree of variability in how EHR systems work. This variability includes capabilities that offer opportunities to, intentionally or unintentionally, create records that will not meet fundamental requirements for validity, accuracy, and integrity due, for example, to commonly occurring inaccuracies in authorship or the presence of evidence of record alteration without retention of original documentation.

In these instances, the metadata are required to provide supporting evidence of who actually did what and when to demonstrate compliance to well-established requirements, best practices, and standards.

In time, as system standards increase due to user demand, regulation, and law, this variability will decrease. For now, however, insofar as the legal system is one among many end users of EHR data, metadata are required to support the appropriateness of a given data set for a given end use. As case law and written law expand, these will increasingly augment the metadata requirements for HIPAA final rule mandates for "information system activity review" obligatory functions.[8]

Other end users have also spoken to the need for supporting metadata as functional requirements, as in the Department of Defense's "Design Criteria Standard for Electronic Records Management Software Applications" and the American Health Information Community's use case for biosurveillance.[9],[10]

Vendors: Priorities Needed

EHR designers and vendors reasonably ask for means to establish priorities since, theoretically one might attempt to argue that every data element for an EHR system might require field-level metadata on date, time, author, system ID, system version, et cetera. Generally, law provides a principle of "reasonable accessibility," with financial cost of access being a parameter.

As the cost of data storage continuously falls and the sophistication of software rises, "reasonable accessibility" will shift and will increasingly become distinguishing features among existing products. Existing products demonstrate that a high degree of metadata capture and reporting is feasible and cost effective.

Also, as specific functions become better defined, variability should diminish. For example, currently systems vary in when they allow and how they represent "cloned" documentation in a record. Payers have stated that cloned data do not meet their requirements for documentation.[11] So, until there is a uniform standard for how to represent cloned versus noncloned information, metadata and audit reporting may be a necessary way to distinguish between the two. Is this a legal requirement? It may become so when the payer decides to make a case of it, whether literally or figuratively.

Users: Due Diligence Required

While views vary on the depth and breadth of requirements for metadata, the necessity remains: those using these systems must exercise due diligence. It remains the burden of the user to ensure that basic and priority requirements for medical records documentation integrity are met by the documentation and records management systems they use.

Fortunately, the wide range of EHR systems available includes some with very robust metadata capabilities already. Furthermore, resources are growing for functional testing and integrity assurance, with basic HIM principles providing tools for prioritization; for example, baseline assurance of authorship, amendments and corrections, and user-configurable application metadata.

Competition will increasingly favor the better designed products and stimulate the less well-designed to improve. In the meantime, case law, legislation, and best practices will accumulate to further demonstrate in e-health records, as they have in other business records domains, the utility and necessity of metadata.

Supporting the interoperability, validity, and integrity of electronic information will prove sufficient motivation alone as EHR systems are required to achieve our universal objectives of accurate information for improving healthcare quality and efficiency while providing the additional benefit of protecting the enterprise against risks that documentation systems will prove insufficient to legal challenge.

Notes

1. Kerr, Orin S. "Computer Records and the Federal Rules of Evidence." *USA Bulletin,* March 2001. Available online at www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm.

2. AHIMA e-HIM Work Group on Maintaining the Legal EHR. "Update: Maintaining a Legally Sound Health Record—Paper and Electronic." *Journal of AHIMA* 76, no. 10 (Nov.–Dec. 2005): 64A–L.

3. Ibid.

4. Dimick, Chris. "E-Discovery: Preparing for the Coming Rise in Electronic Discovery Requests." *Journal of AHIMA* 78, no. 5 (May 2007): 24–29.

5. Baldwin-Stried, Kim. "E-Discovery and HIM: How Amendments to the Federal Rules of Civil Procedure Will Affect HIM Professionals." *Journal of AHIMA* 77, no. 9 (Oct. 2006): 58–60.

6. False Claims Act § 3733. Civil investigative demands; (l) Definitions Subsection (5).

7. Korin, Joel B., and Madelyn S. Quattrone. "Electronic Health Records Raise New Risks of Malpractice Liability." *New Jersey Law Journal,* June 19, 2007. Available online at www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1182194746807#4.

8. Department of Health and Human Services, Office of the Secretary. "45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule." *Federal Register,* February 20, 2003. Available online at www.gpoaccess.gov/fr.

9. Department of Defense. "Design Criteria Standard for Electronic Records Management Software Applications." June 2002. Available online at www.dtic.mil/whs/directives.

10. Office of the National Coordinator for Health Information Technology. "Harmonized Use Case for Biosurveillance (Visit, Utilization and Lab Result Data)." March 19, 2006. Available online at www.hhs.gov/healthit/usecases.

11. "Requirements for the Payment of Medicare Claims—A Selection of Some Important Criteria." *Medicare B Update!* 4, no. 3 (third quarter, 2006): 4.

Acknowledgments

The author thanks Patricia A. Trites, Kim Baldwin-Streid, Katherine Ball, and Ellen Anderson.

Reed D. Gelzer (rdgelzer@docintegrity.com) is chief operating officer of Advocates for Documentation Integrity and Compliance in Wallingford, CT.

Article citation:
Gelzer, Reed D.. "Metadata, Law, and the Real World: Slowly, the Three Are Merging" *Journal of AHIMA* 79, no.2 (February 2008): 56-57;64.