Authenticating EHR Metadata

by **Thomas R. McLean,** MD, JD, FACS, Esq.

Any medical malpractice action involving electronic records is likely to raise issues concerning metadata. Metadata are tantamount to an audit trail of how an electronic record was used and modified.

However, before this audit trail can be used in court, it must be authenticated. While electronic health records (EHRs) may be authenticated using several techniques, an analysis of the EHR's metadata is likely to be the most reliable and the least likely to mislead a jury.

Authenticating Metadata

From a computer programmer's point of view, an EHR consists of the document's text and its metadata. The document's text is what the EHR user sees when viewing the record. The metadata, which are invisible to the user, consist of machine-made marks necessary for the EHR to function.

Before metadata can be used in a medical malpractice trial, it must be authenticated. In lay terms, authentication is the legal process that demonstrates that an e-document is an original; or alternately, that it is a "true copy," an uncorrupted version of the original document. More generally, authentication is a legal process that certifies the integrity of an e-document.

Metadata are introduced into court as either hearsay or nonhearsay evidence, depending on their type. The authentication process for each type of evidence differs.

The two basic types of EHR metadata are system and application.[1] System metadata consist of the automatically generated markings that an EHR places on all e-documents (such as notes, reports, and radiographic images) during the course of routine use. EHRs rely on system metadata to function properly. While many types of EHR system metadata exist, perhaps the most important are the unique physician identification number and the time-signature stamp.

System metadata are nonhearsay evidence because they are produced by an automated process (i.e., not by a human), do not involve a statement, and nothing is asserted.[2] In many other fields, documents such as newspapers that are produced by machines can be admitted into evidence directly because they are considered to be self-authenticating.[3]

However, self-authentication cannot be used to assure the integrity of EHR system metadata, because they contain symbols that are incomprehensible to lay people. Accordingly, EHR system metadata are likely to be authenticated when their integrity has been certified by some combination of a witness with knowledge; expert testimony; identification of distinctive characteristics; or evidence that the system's output is known to be reliable.

A Record Custodian's Word Is No Longer Enough

EHR application metadata, on the other hand, are classic hearsay evidence. Application metadata are the record of changes made to an e-document by the user. Every physician's note is hearsay because it is composed of a set of written statements that assert the truth. As EHR application metadata are derived from EHR entries, they too are hearsay evidence.

Therefore, like the EHR itself, authentication of EHR application metadata will likely occur under the business record exception to hearsay evidence.[4]

The exception is established for an EHR, just as it is for a paper record, by having the medical records custodian testify that the EHR and its metadata were created at or near the time that the patient received care and the EHR has not been altered because it remained in the custody and control of the custodian when it was not being used clinically.

Yet, custodians cannot truthfully testify that an intangible EHR was ever in their custody or that the EHR has not been altered. For example, the EHR and its metadata may be inadvertently corrupted by physical forces, such as strong magnetic fields, or intentionally corrupted by an authorized user with the ability to alter the record.[5]

Consequently, authenticating an EHR is likely to require that the audit trail created by its metadata be examined for evidence of corruption. System metadata can provide assurance that a user has not selectively deleted e-documents, and application metadata can demonstrate whether the contents of an e-document were altered. Absent an examination of an EHR's metadata, a printout or CD-ROM version of the EHR is merely uncorroborated hearsay.[6]

Drawbacks of Alternative Methods to Metadata Authentication

Not everyone agrees that metadata are needed to authenticate an EHR. In particular, some commentators would argue that if the custodian's testimony were ramped up or if hash-value comparison analysis were performed, an EHR could be authenticated without the use of metadata. Both of these techniques, however, have significant drawbacks.

Edward Imwinkelried, professor of law at the University of California, Davis, proposed an elaborate 11-step process for authenticating an EHR that is not necessarily dependent on the use of metadata. A key step in this process requires the medical record custodian to testify that when the patient's EHR was retrieved from the computer, he or she conducted a proper search of the system, which was functioning properly. Providing such testimony is often difficult because even Fortune 500 companies with sophisticated IT departments often cannot truthfully make such statements.[7]

Thus, in a medical malpractice action some custodians may find they have a conflict of interest. If the EHR system was not functioning properly or not appropriately searched, the custodian will either have to prevaricate or admit to negligence (something that may cost the custodian his or her job). To eliminate such a conflict of interest it would seem preferable to authenticate an EHR by examining the objective metadata.

Alternatively, the Sedona Conference has recommended that e-documents be authenticated by comparing hash values.[8] A hash value is a unique number obtained by running an e-document through a hashing algorithm. Hashing algorithms, in turn, are capable of detecting the change of a single bit of data in a multigigabyte e-document.[9]

According to the Sedona Conference, which is composed of prominent attorneys, law professors, and judges, e-document authentication by hash-value comparison is preferable to review of metadata because of its simplicity.[10] For many forms of class action litigation, where large-scale e-discovery can result in the production of millions of pages of documents, hash-value comparison has clear appeal as a screening tool.

Weaknesses of Hash-value Comparison

Unfortunately, authentication by hash-value comparison is undesirable in medical malpractice litigation. First, hash values are too sensitive for EHR authentication because the mere act of opening a patient's EHR will change its hash value. Such sensitivity means EHR authentication via hash-value comparison would require that the medical record custodian account for every person who opened the patient's record.[11] Such an accounting would likely involve an examination of the unique physician identification number metadata, which would defeat the purpose of generating hash values.

Second, while a hash-value comparison can indicate that two e-documents are different, it cannot alone distinguish the original e-document from an altered copy. Finally, without an objective reference point like the EHR's metadata, there is no assurance that the hash value brought to court is identical to the hash value of the same e-document in the EHR system.

In part, the Sedona Conference's preference for hash-value comparison is predicated on its concern that metadata analysis may mislead juries. In particular, the Sedona Conference has reservations about metadata authentication because metadata can be corrupted by commercially available software.

Certainly corruption is a possibility, but it is not a sufficient reason to jettison EHR metadata authentication from medical malpractice. First, the text of EHR e-documents can be corrupted just as easily by commercial software as can the EHR metadata. Second, the act of corruption of an EHR by commercial software will leave behind metadata indicating that the document has been corrupted.

But in part the Sedona Conference's concern that authentication of e-documents through metadata analysis may mislead juries is related to the conference's concerns for the logistics of large-scale e-discovery itself. When litigation involves the disclosure of tens-of-millions of pages and the production of millions of pages, it is not hard to imagine mistakes being made. Moreover, as much of the information that is initially disclosed may ultimately prove to be irrelevant and cannot be used in litigation, the conference has legitimate concern that routine production of metadata will increase the cost of large-scale electronic discovery.

Yet, in a medical malpractice case, many of the issues raised by the Sedona Conference are not applicable. The EHR is unlikely to be more than a few thousand pages in length. Moreover, in any particular medical malpractice case either the plaintiff or the defendant will view metadata as friendly testimony, and thus one side or the other will seek to have the metadata authenticated.

Consequently, as the volume of motions for EHR metadata production expand, it is not unreasonable to believe that courts will tire of ruling on individual motions to authenticate EHR metadata. It seems likely that in medical malpractice actions that the courts will promulgate a local rule that all *relevant* EHR metadata should be produced.

That will make metadata authentication a fixture of litigation.

Notes

1. The Sedona Conference. "The Sedona Conference Commentary on ESI Evidence and Admissibility." March 2008. Available online at www.thesedonaconference.org/content/miscFiles/publications_html.
2. Fed. R. Evid. 801.
3. Fed. R. Evid. 901.
4. Fed. R. Evid. 803(6).
5. Gaylord, Chris. "Digital Detectives Discern Photoshop Fakery." *USA Today,* August 30, 2007. Available online at www.usatoday.com/tech/news/techinnovations/2007-08-30-photoshop-fakery_N.htm.
6. Dimick, Chris. "E-discovery: Preparing for the Coming Rise in Electronic Discovery Requests." *Journal of AHIMA* 78, no. 5 (May 2007): 24–29.
7. In re Vee Vinhnee, 336 B.R. 437 (9th Cir. BAP 2005).
8. Lorraine v. Markel American Ins, 241 F.R.D. 534, 547 (D. Md. 2007).
9. Losey RC: "HASH: The New Bates Stamp." *Journal of Technology Law and Policy* 12, no. 1 (June 2007). Available online at http://ralphlosey.files.wordpress.com/2007/09/hasharticlelosey.pdf.
10. The Sedona Conference. "Complex Litigation V." April 2008. Available online at www.thesedonaconference.org/conferences/20030424.
11. Surety, LLC. "The Power of Proof." 2008. Available online at www.surety.com/news/article/sedona_conference_commentary_on_esi_evidence_admissibility.

Thomas R. McLean (tmclean@dnamail.com) is CEO of Third Millennium Consultants, LLC, in Shawnee, KS. He is also an attending surgeon at the VA Eastern Kansas Health Care System, Leavenworth, KS. Nothing in this paper should be construed as Department of Veterans Affairs policy or procedure.

Article citation:
McLean, Thomas R. "Authenticating EHR Metadata" *Journal of AHIMA* 80, no.2 (February 2009): 40-41;50.