Electronic Medical Record Metadata: Do You Know What’s in Your Record?

Thomas R. McLean, MD, JD, FACS
Address correspondence to:
Thomas R. McLean
Third Millennium Consultants, LLC
4970 Park
Shawnee, KS 66216
Email: tmclean@dnamail.com

Thomas R. McLean, MD, JD, FACS, received his MD from the University of Chicago and his JD from the UMKC School of Law. He is CEO of Third Millennium Consultants, LLC, in Shawnee, Kansas (www.firms.findlaw.com/TMCLLC); Clinical Assistant Professor of Surgery, University of Kansas School of Medicine; and Attending Surgeon at the Dwight D. Eisenhower Veterans Administration Medical Center, Leavenworth, Kansas.

Like use of any computer record, use of an electronic medical record (EMR) generates metadata. Commonly defined as “data about data,” metadata is the record a computer automatically generates when it manipulates an electronic document.1 While most metadata is invisible to the average computer user, one place that metadata can be viewed is in the “track changes” feature of Microsoft Word. Track changes allows the user to see some of the metadata associated with the document; including:

1. Who entered or altered data;
2. What the alterations were; and
3. When the alterations were made.

More generally, the metadata associated with every electronic document is tantamount to an audit trail that cannot be easily erased or destroyed.2 Absent a willful act (like the physical destruction of the computer’s hard disk) by a computer user, it is possible to discover the contents of a metadata file;3 a process made easier because metadata is searchable.4

In the health care arena, the potential uses and liabilities of EMR metadata have been largely underappreciated. A current paper, however, demonstrates that EMR metadata can be used to profile physicians’ work habits.5 Previously, physician profiling was limited to mining administrative data; a practice that has been criticized because:

1. Absent clinical data, it does not necessarily reflect the actual care delivered to patients;
2. It is based on non-standard terminology; and
3. It is frequently misclassified.6

Other commentators have observed that mining administrative data frequently provides inaccurate physician profiles because of systematic problems in data collection.7 Therein lays the true value of profiling physicians with EMR metadata: It provides a truer reproduction of a physician’s work habits.8

CONCERNS OF E-PROFILING

George Orwell’s Big Brother would have loved EMR metadata: Never before has it been possible to examine a physician’s work habits in such detail and rapidity that a work-time analysis can be virtually completed in real-time. In the past, obtaining such information would have required a time-and-motion study. Unfortunately, these studies are rarely performed to determine physicians’ productivity because they are labor intensive.9 Extensive use of EMR metadata physician profiling seems limited to the extent that EMR use has not penetrated the market. Today only half of America’s community hospitals have partially computerized their medical records and only 11 percent of community hospitals have fully computerized their medical records.

But as the government and insurers have pushed for greater use of EMR, the potential for profiling physicians with metadata has not gone unnoticed. The American Medical Association (AMA) has already expressed concern about the potential of improper use of EMR metadata.10 According to the AMA, third parties should only have access to EMR metadata to obtain “clinical data” needed for “payment and health care operations,” and physicians should be notified “on a case-by-case basis of any [EMR] analysis undertaken.”11 Such statements leave little doubt that the AMA wants to deny third parties access to EMR metadata. Whether the AMA will be able use its influence to limit hospitals, insurers, and others access to data-mine EMR metadata remains to be seen.

PROFILING IN LITIGATION

Regardless of the outcome of the AMA’s lobbying to restrict insurers’ use of metadata to profile physicians, in the courts the battle to restrict metadata use as evidence is all but over, and many did not even realize that a war was on.

A few years ago, Feldman surveyed a large number of health care providers to determine what impact the EMR was having on medical malpractice litigation.12 Although Feldman had only a 50 percent response rate, he
concluded that EMR evidence had not been used detrimentally against any physicians during medical malpractice litigation. Depending on which side of the court you are sitting in, this blissful state of ignorance was either a blessing or a curse. Yet because technology marches forward, this state of e-discovery ignorance proved short-lived because in 2006, the first reported case where EMR metadata evidence was used against a physician was published.\(^\text{13}\)

In this case, a 58-year-old patient underwent a seven-hour back operation. When the patient awoke as a quadriplegic, the surgeon was initially thought to be at fault. But then the plaintiff stumbled upon the metadata in the patient’s EMR. The plaintiff discovered a 90-minute gap in electronic physiologic monitoring of the patient during the operation, and that the anesthesiologist’s postoperative note (asserting that the procedure was uncomplicated) had actually been written minutes after the operation began. Faced with an awkward situation, the anesthesiologist and the hospital entered into a confidential out-of-court settlement.

**E-DISCOVERY OF METADATA**

Discovering EMR metadata is going to become increasingly commonplace. The December 2006 modification of the Federal Rules of Civil Procedure (FRCP) and the need to authenticate EMR used in trial means discovery physician-specific metadata will become an integral component of due diligence process of litigation involving a doctor-patient relationship. (State courts, where most medical malpractice litigation occurs, are expected to similarly modify their rules of civil procedures.)

Under the new FRCP, subject to certain exceptions, all “electronically stored information” (ESI) must be turned over to the opposing party even if such information is not formally requested.\(^\text{14}\) While the new discovery rules do not define how much metadata must be produced with ESI, federal courts have held that when an electronic document is discoverable, it is to be produced “in native format…with their metadata intact.” Moreover, ESI is to be turned over to the opposing party in a “reasonably usable” form, meaning it must be readable.\(^\text{15}\) To the extent that ESI exists in an illegible or intelligible format, the party-in-possession of ESI must provide the hardware and software to “translate” the data into a readable format.

Hospitals and other organizations are under a continuous obligation to turn over to the apposing counsel newly identified relevant ESI, unless turning over such information would be unduly burdensome. Business organizations that fail to turn over ESI and/or their metadata are subject to sanctions. This rule does have an important safe harbor: ESI that is “lost as a result of the routine, good-faith operation of an electronic information system” will not subject a business organization to sanctions.\(^\text{16}\)

These new e-discovery rules are likely to impact medical malpractice litigation in two ways. First, the rules make clear that health care providers cannot stonewall plaintiffs. In the past, defense attorneys would attempt to frustrate a plaintiff’s EMR discovery by providing a paper copy of the EMR complete with all of the usually unprinted symbols (like the symbol for the return key). When an EMR is printed on paper in such a fashion, it contains sections of readable textual information interspersed with sections of incomprehensible strings of letters, numbers, and symbols. Over all, these paper print outs of EMR are unintelligible because it is unclear where, for an example, a laboratory value ends and a string of numbers that are normally non-visible begins. Such tactics by the defense, however, are headed for the history books. Under the new discovery rules, a plaintiff needs to be able to view a patient’s EMR to the same extent as the patient’s treating physician.

Second, hospitals and physician groups using EMRs must create, and comply with, a policy for ESI retention. Health care providers need clear and reasonable guidelines for how often their patients’ EMRs and related metadata will be backed up, the medium used of storage (e.g., optical disks), off-site storage, and when and how stored data will be destroyed. Moreover, the ESI retention policy must include a provision for the preservation of a particular patient’s ESI once the health care provider receives notice of impending litigation. Compliance with an ESI retention policy of course will mean that both exculpatory data must be destroyed with damming evidence. Importantly, failure to have an ESI policy or failure to comply with an ESI policy, can prove fatal to a provider’s defense in medical malpractice litigation.\(^\text{17}\)

**METADATA AND AUTHENTICATION**

The second reason EMR metadata e-discovery will become common place in physician litigation is that metadata will be needed to authenticate the EMR. Medical records—whether paper or electronic—are hearsay evidence. To be admitted at trial, medical records need to fall into one of the exceptions to hearsay. Most frequently, medical records are admitted under the business record exception (BRE) to hearsay evidence.\(^\text{18}\) According to BRE, a medical record may be admitted into evidence if:

1. It was created at the time an event occurred;
2. By a person with knowledge;
3. In the course of regular business activity; and
4. The record can be authenticated.

The first three requirements of BRE are generally not a barrier to admitting a medical record—electronic or paper—into evidence. After all, these requirements are a summary of the steps a physician goes through when entering a note into a patient’s medical record. However, the BRE’s requirement that medical records be authenticated prior to being admitted, changes the evidentiary burdens for handling paper and electronic medical records.
Satisfying the authentication requirement of the BRE is generally achieved by having someone from the medical records department testify that a patient’s record is complete, unaltered, and has remained in the position of the medical record department when not in active use by the medical staff. The authenticity of a paper medical record is corroborated by inspection of the record itself for omissions, erasures, or alterations.

Unfortunately, such testimony cannot be used to authenticate an EMR. Existing in cyberspace, an EMR cannot be considered to be in the custody and control of the medical records department when the record is not used by the medical staff. Any health care provider can access EMR and alter the document so as to reflect a certain point of view. Unlike paper records, detection of an EMR alteration by visual inspection is not possible. Rather, the only way to tell if an EMR has been altered is to use its metadata to track the changes made to the document. Metadata will tell who accessed the medical record, what information was viewed, and how and when the document was modified. Without the underlying metadata, an EMR is merely hearsay because there is no way to prove the integrity of the document.

But metadata obtained to authenticate a document can be used to undermine the credibility of physician defendants. Recall the case of the 58-year-old patient who underwent back surgery. Once the plaintiff obtained the signature-time metadata, the defendant anesthesiologist’s credibility was destroyed. More generally, e-discovery of self-serving or misleading alterations of an EMR will likely force a settlement and the reporting of the physician’s name to the National Practitioner Data Bank.

REFERENCES
