Annals of Health Law

Volume 18
Issue 1 *Winter 2009*

Article 5

2009

EMR Metadata Uses and E-Discovery

Thomas R. McLean
Third Millenium Consultants, LLC

EMR Metadata Uses and E-Discovery

Thomas R. McLean, MD, JD, FACS, ESQ.[*]

In the 21st century, ninety-five percent of records are electronically created and stored.[1]

I. INTRODUCTION

Like any computer record, an electronic medical record (EMR)[2] generates metadata.[3] Metadata, commonly defined as "data about data," is an automatically generated computer record that certifies how an electronic document (e-document) has been manipulated.[4] For example, when the "track changes" feature of Microsoft Word is enabled, the application metadata associated with the e-document's use is displayed, including who

[*] tmclean@dnamail.com. CEO, Third Millennium Consultants, L.L.C., Shawnee, Kansas; Attending Surgeon, VA Eastern Kansas Health Care System, Leavenworth, Kansas; Clinical Assistant Professor of Surgery, University of Kansas. Nothing in this paper is to be construed as the U.S. Department of Veterans Affairs' policy or procedure. The author wishes to thank: (1) Edward P. Richards, Louisiana State University, Professor of Law, for his background assistance on this paper and many other papers over the past several years; and (2) the Information Technology service at the VA Eastern Kansas Health Care system for providing background knowledge in computers and software.

1. Judge Shira A. Scheindlin, *FAQ's of E-Discovery*, IN CAMERA (Fed. Judges Ass'n., Washington, D.C.), Nov. 29, 2006, http://www.fjc.gov/public/pdf.nsf/lookup/FAQEDisc.pdf/$file/FAQEDisc.pdf (last visited Jan. 25, 2009). *See* SCOTT GREIPER & MARK SAUTER, C.E. UNTERBERG, TOWBIN & CHESAPEAKE INNOVATION CTR, THE BUSINESS OF CONNECTING DOTS: THE $1 BILLION INTELLIGENCE AND SECURITY INFORMATICS/ANALYTICS MARKET 3 (2005), http://www.aatechcouncil.org/documents/ConnectingDots.pdf (last visited, Sept. 8, 2008) (noting Information Technology professionals consider data structured, when it exists in rows and columns, similar to a Microsoft Excel spreadsheet; all other electronic data (e.g., texts, images, and videos), which accounts for eighty to eighty-five percent of data, is considered to be "unstructured").

2. Provider-created EMRs can affect litigation involving physician-defendants; patient-created EMRs are becoming more prevalent. *See generally* Robert Steinbrook, *Personally Controlled Online Health Data—The Next Big Thing in Medical Care?*, 358 NEW ENG. J. MED. 1653 (2008).

3. Scheindlin, *supra* note 1, at No. 8 ("[I]t's never a question of whether there is metadata, but what kinds of metadata exist, where it resides and whether its potential relevance demands preservation and production." (quoting Craig Ball, I Never Metadata I Didn't Like (Jan. 2006) (unpublished manuscript, on file with author)).

4. CRAIG BALL, BEYOND DATA ABOUT DATA: THE LITIGATOR'S GUIDE TO METADATA 2 (2005), http://www.craigball.com/metadata.pdf.

made changes, when the changes were made, and what was changed. Thus, an EMR's metadata is tantamount to an audit trail for that e-document.[5] Recently, for example, analysis of EMR metadata allowed the University of California Los Angeles (UCLA) Medical Center to discover which of its employees were "snooping in" the medical records of Britney Spears and Farrah Fawcett.[6] The means of UCLA's discovery may have been its EMR system metadata audit trail.

More generally, metadata can be evidence of physicians and other healthcare providers' conduct and credibility. Metadata can create reasonable inferences concerning what physicians knew and when they acquired this knowledge. To illustrate, the analysis of metadata provides insight into what Merck's physicians knew about its anti-inflammatory agent Vioxx. While the medical literature contained hints that the use of Vioxx was associated with significant cardiovascular side effects as early as 2000,[7] the medical community accepted Merck's assurances that Vioxx was safe. Once the dangers of Vioxx use became common knowledge in 2004,[8] the editors of the *New England Journal of Medicine* began reviewing the metadata of submitted articles concerning Vioxx.[9] The *Journal* soon found evidence within the metadata that Merck's physicians knew about the risks of Vioxx years before this information was publicly available.[10] Furthermore, the metadata of some articles revealed that Merck's scientists may have ghostwritten articles asserting that Vioxx was safe.[11]

---

5. *See* Paul Nielson, CodeGen to Create Fixed Audit Trail Triggers, http://sqlblog.com/blogs/paul_nielsen/archive/2007/01/15/codegen-to-create-fixed-audit-trail-triggers.aspx (last visited Sept. 8, 2008); *see also* JOHN RANDALL, RANDALL CONSULTING, METADATA V. CODING IN ELECTRONIC DISCOVERY 1 (2007), http://www.rosentech.net/pdfs/ALCoder_2007_003.pdf (asserting that metadata provides no information concerning the contents of a document).

6. Charles Ornstein, *Fawcett's Cancer File Breached: The Incident Occurred Months Before UCLA Hospital Employees Were Caught Snooping in Britney Spears' Files*, L.A. TIMES, Apr. 3, 2008, at Cal. 1, *available at* http://articles.latimes.com/2008/apr/03/local/me-farrah3.

7. Thomas R. McLean, Letter to the Editor, 365 LANCET 25, 25 (2005) (criticizing how many medical journal editors engaged in hindsight bias after the side effects of Vioxx became common knowledge and exploring whether it was possible to have discovered the truth about Vioxx).

8. Peter Jüni et al., *Risk of Cardiovascular Events and Rofecoxib: Cumulative Meta-Analysis,* 364 LANCET 2021, 2021 (2004); *see also* Alex Berenson, *Analysts See Merck Victory in Vioxx Deal*, N.Y. TIMES, Nov. 10, 2007, at A1, *available at* http://www.nytimes.com/2007/11/10/business/10merck.html?_r=1&scp=1&sq=Alex%20Berenson%20Analysts%20See%20Merck%20Victory&st=cse&oref=slogin# (discussing how Merck settled the Vioxx litigation for almost five billion dollars).

9. Robert Langreth & Matthew Herper, *Merck's Deleted Data*, Forbes.com, Dec. 8, 2005, http://www.forbes.com/2005/12/08/merck-vioxx-lawsuits_cx_mh_1208vioxx.html.

10. *Id.*

11. *See* Joseph S. Ross et al., *Guest Authorship and Ghostwriting in Publications Related to Rofecoxib: A Case Study Study of Industry Documents from Rofecoxib Litigation,*

Similarly, medical malpractice litigation has used EMR metadata as a tool to measure the actual quantity and quality of physicians' clinical practices;[12] for example, EMR metadata in one particular case exposes the possible wrongdoings of an anesthesiologist.[13] The number of ways EMR metadata can be used as evidence in healthcare litigation is limited only by an attorney's imagination, subject to the limits imposed by the 2006 amended Federal Rules of Civil Procedure (FRCP)[14] and the Federal Rules of Evidence (FRE),[15] as they apply to electronically stored information (ESI).[16]

Therefore, the purpose of this article is to provide an overview of the potential uses of EMR metadata to profile physician behavior and describe how attorneys can use metadata under the new rules for electronic discovery (e-discovery).[17] Part II of this paper demonstrates how the actual work habits of physicians can be profiled by EMR metadata. Unlike the paper medical record (PMR), physician-specific EMR metadata can provide a more realistic image of how a physician practices medicine due to the absence of self-serving statements made by the physician himself. Part III of this paper provides an overview of relevant changes to the FRCP, the FRE, and the case law concerning e-discovery and metadata. When these changes are analyzed, it is possible to find support for both an expansive scope and a limited view of the amount of metadata that should be allowed in discovery. Courts that handle litigation with the potential for large-scale e-discovery (e.g., class-actions lawsuits) will probably take a narrower view

299 JAMA 1800, 1802-06 (2008); *see* Stephanie Saul, *Merck Wrote Studies for Doctors*, N.Y. TIMES, Apr. 16, 2008, at C1, *available at* http://www.nytimes.com/2008/04/16/business/16vioxx.html.

12. *See* Thomas R. McLean et al., *Electronic Medical Record Metadata: Uses and Liability*, 206 J. AM. COLL. SURG. 405, 410 (2008) [hereinafter McLean, *Metadata*]. *See generally* Thomas R. McLean et al., Presentation at 32nd Annual Meeting of the Association of VA Surgeons Meeting: Surgery Clinic: Tragedy of the Commons (May 4, 2008), [hereinafter McLean, *Tragedy*] (transcript available at the Beazley Institute for Health Law and Policy at the Loyola University Chicago School of Law).

13. Michael M. Vigoda & David A. Lubarsky, *Failure to Recognize Loss of Incoming Data in an Anesthesia Record-Keeping System May Have Increased Medical Liability*, 102 ANESTH. ANALG. 1798, 1798 (2006).

14. FED. R. CIV. P., *available at* http://www.uscourts.gov/rules/civil2007.pdf.

15. FED. R. EVID., *available at* http://www.uscourts.gov/rules/Evidence_Rules_2007.pdf.

16. FED. R. CIV. P. 34(a)(1)(A) ("[E]lectronically stored information—includ[es] writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form . . .").

17. Most litigation concerning physicians occurs in state courts. It is expected, however, that many, if not most, states will adopt the 2006 amendments to the FRCP. This paper discusses the new federal ESI discovery rules as a model for physician healthcare litigation, while it is recognized that some variation in e-discovery exists from state to state.

of how much metadata can be discovered. This view, however, may not be appropriate for healthcare litigation where the potential scale of e-discovery is much smaller.

Consequently, Part IV focuses on the use of EMR metadata in litigation involving physicians as defendants in medical malpractice actions or as respondents before a Board of Medical Examiners (BOME). Unlike class-action litigation, physician healthcare e-discovery is more circumscribed because the e-production demands are usually limited to the EMR of one or few patients. Because the EMR becomes a pivotal piece of evidence in such cases, EMR metadata is likely to become useful in two situations. First, EMR metadata may be the standard for authentication where there is a dispute over the integrity of the EMR. Second, EMR metadata may be used to challenge the veracity of EMR entries in situations where the documented care does not, or cannot, explain a particular patient's clinical outcome. Since a court order to produce EMR metadata may be issued at any time during litigation, the prudent physician-defendant should preserve a copy of the EMR with its metadata upon receiving notice of litigation to avoid sanctions.

II. USING EMR METADATA TO PROFILE PHYSICIANS' WORK HABITS

A. What is Metadata?

Metadata, defined as the "information describing the history, tracking, or management of an electronic document,"[18] comes in two forms: system and application metadata.[19] Computer networks automatically imprint system metadata, including file name, format, and date accessed, onto e-documents.[20] Because human input is not involved in the creation of system metadata, courts have viewed this form of metadata as non-hearsay evidence.[21] Under the FRE, hearsay is "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."[22] A statement is "an oral or written assertion. . . of a person,"[23] and a declarant is "a person who makes a statement."[24] Courts have held that system metadata is not considered hearsay because system

18. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005) (quoting proposed advisory committee note to FED. R. CIV. P. 26(f)).

19. THE SEDONA CONFERENCE COMMENTARY ON ESI EVIDENCE & ADMISSIBILITY 10 (2008) [hereinafter ESI EVIDENCE], http://www.thesedonaconference.org/content/miscFiles/ESI_Commentary_0308.pdf.

20. *Id.*

21. *Id.*

22. FED. R. EVID. 801(c).

23. FED. R. EVID. 801(a).

24. FED. R. EVID. 801(b).

metadata involves neither a statement nor a declarant[25] and nothing is said. In contrast, application metadata, such as the "track changes" feature of Microsoft Word, involves human input and a written statement. This suggests that courts will view application metadata as a written statement and hearsay evidence within the meaning of the FRE.

The discussion regarding the hearsay distinction between system and application metadata should reach beyond the academic arena because the method of authentication for metadata depends upon how the evidence is classified. A party wishing to enter ESI metadata into evidence has the burden of establishing its accuracy.[26] Self-authentication is an unlikely way to validate either form of metadata. Furthermore, a computer printout that includes metadata will contain strange symbols that are unintelligible to most individuals without the testimony of an information technology (IT) professional.[27] Accordingly, a computer printout that includes both the source document and its metadata would not fit neatly into any of the FRE's twelve methods for self-authentication.[28]

The authentication of system metadata, like the authentication of any form of ESI, will presumably require some combination of: (1) a witness with knowledge;[29] (2) an expert witness;[30] (3) identification of distinctive characteristics;[31] or (4) evidence that the system's output is known to be reliable, such as time-stamping of a computer record.[32] In contrast, because application metadata may be deemed hearsay, its authentication is likely to require the testimony of the computer system's administrator. In particular, the computer system's administrator will probably be asked to testify that any relevant application metadata constitutes a business record within the meaning of FRE 803(6).[33]

Generally, the courts are skeptical about admitting metadata as evidence, regardless of its foundation. In part, this judicial skepticism arises from the courts' unfamiliarity with metadata. Additionally, judicial reluctance to admit metadata into evidence can be traced to the potential for selective

25. United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005).

26. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 557 (D. Md. 2007) ("The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.").

27. *See* McLean, *Metadata*, *supra* note 12, at 409.

28. *See* FED. R. EVID. 902 (Self-authentication).

29. FED. R. EVID. 901(b)(1).

30. FED. R. EVID. 901(b)(3).

31. FED. R. EVID. 901(b)(4).

32. FED. R. EVID. 901(b)(9).

33. FED. R. EVID. 902(11); *see also* Am. Express Travel Related Servs. Co. v. Vinhnee (*In re* Vinhnee), 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005) (noting that foundation and authentication for the admission of a business record generally merge under FED. R. EVID. 902(11)).

deletion or digital forgery of metadata, thereby making an e-document's metadata audit trail misleading.[34] Some commentators have speculated that the prevalence of digitally forged metadata is rising because even unsophisticated computer users can employ commercially available software products to corrupt metadata.[35]

The judicial fear of corrupted metadata misleading the courts seems unjustified. Absent an affirmative action,[36] metadata and the source e-document are recoverable to the same extent.[37] Further, any affirmative act to alter metadata will leave additional metadata indicia, which will allow an IT professional to identify the corruption. Therefore, in situations where an IT professional testifies that an individual has tampered with the metadata, it would be reasonable for the courts to presume that corruption of the metadata occurred for the benefit of the party in the custody and/or control of the e-document when the corruption occurred.[38] It appears that an e-document's metadata is no more likely to mislead a fact finder than the e-document itself.

However, an IT professional only can identify metadata corruption if the e-document and metadata are preserved. From a practical point of view, failure to preserve metadata is a more significant problem than corruption of metadata.[39] Even though storage of metadata is essential for a computer to function properly, computer systems do not necessarily store metadata indefinitely. Many computer and EMR systems intentionally were designed with limited capacity to store metadata because of the historic cost of data storage, processor speed, and the recognition that users were not interested in having long-term metadata audit trails.[40] Over the past decade, the cost of electronic storage has progressively fallen, while processor

34. *See, e.g.*, Gordon J. Calhoun & Susan F. Friedman, *Stage Is Set for More In-House Drama*, IN-HOUSE COUNSEL ONLINE, Mar. 3, 2008, http://www.law.com/jsp/ihc/PubArticleFriendlyIHC.jsp?id=1203866386498 ("Many judges and commentators have a deeply rooted suspicion of ESI.").

35. *See generally* ESI EVIDENCE, *supra* note 19, at 13 (discussing how metadata can be unreliable and subject to manipulation).

36. *See, e.g.*, Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005) (discussing how native files can be scrubbed of their metadata to produce image files and how such affirmative acts may be intentional or inadvertent).

37. Native documents, like Microsoft Word or Excel files, contain user provided content and its related metadata. In contrast, image files, like tagged image file format (TIFF) or portable document format (PDF) files, contain only user provided content. *See generally* Eric A. Taub, *Keeping Track: Deleting May Be Easy, but Your Hard Drive Still Tells All*, N.Y. TIMES, Apr. 5, 2006, at G4, *available at* http://www.nytimes.com/2006/04/05/technology/techspecial4/05forensic.html?_r=1&oref=slogin.

38. In such situations, the presumption should be rebuttable.

39. *See infra* Part III, where failure to preserve EMR metadata is discussed in more detail.

40. *See* Reed D. Gelzer, *Metadata, Law, and the Real World: Slowly, the Three Are Merging*, 79 J. AHIMA 56, 57 (2008).

speeds have substantially improved.[41] Consequently, the present market demand for metadata storage capacity seems to determine the amount of metadata a computer system stores.[42]

This trend raises several interesting legal questions. How much metadata storage capacity should a reasonable computer designer include in a system? Similarly, should society give computer designers consent to store volumes of metadata, which profiles the computer user's habits? Alternatively, should society give computer designers the right to destroy metadata when it is no longer needed for the system to function properly? Because failure to store metadata arguably could be construed as tantamount to the spoilage of evidence, [43] these questions are fundamental to the e-discovery process and, ultimately, to those who win or lose during litigation.

B. Metadata Search Issues

E-document discovery, with or without metadata, can generate millions of pages of ESI.[44] Such voluminous document production raises an important logistical question: how can a file of one million pages, which contains approximately 500 words per page, be reviewed efficiently? Assuming the average attorney reads 500 words per minute,[45] it would take a single attorney almost two years of non-stop reading to digest a million-page file. Therefore, multiple individuals must be employed to review documents of this magnitude efficiently.

Perhaps the most important reason for the employment of a phalanx of associates at large law firms is the efficient review of voluminous documents. On the other hand, as e-document production grows exponentially,[46] commentators postulate that there are insufficient financial and staffing resources within the legal community to continue document review as done previously.[47] Accordingly, it is anticipated that search

41. *Id.*

42. E-mail from Reed D. Gelzer, Chief Operating Officer, Advocates for Documentation Integrity & Compliance, to author (Mar. 17, 2008) (on file with Beazley Institute for Health Law and Policy at the Loyola University Chicago School of Law).

43. BALL, *supra* note 4, at 9.

44. *See* Qualcomm Inc. v. Broadcom Corp., No. 05cv1958-B (BLM), 2008 U.S. Dist. LEXIS 911, at *31 (S.D. Cal. Jan. 7, 2008), *vacated in part*, 2008 U.S. Dist. LEXIS 16897 (S.D. Cal. Mar. 5, 2008) (discussing the production of 1.2 million pages of "marginally relevant documents").

45. *See generally* TurboRead, How Does Your Light Reading Speed Compare Below?, http://www.turboread.com/interpretation.htm (last visited Sept. 5, 2008) (indicating that 500-800 words per minute is a comfortable reading speed for office purposes).

46. *See* Scheindlin, *supra* note 1.

47. *See, e.g.*, The Sedona Conference Working Group on Best Practices for Document Retention and Production (WG1), *The Sedona Conference Best Practices Commentary on*

strategies will soon drive e-discovery.[48] Commercial software vendors already sell search algorithms to attorneys to facilitate large-scale e-document reviews.[49] These software products facilitate e-discovery by (1) making maximal use of e-filing strategies;[50] (2) identifying the relevant e-documents that must be disclosed to the opposition;[51] and (3) identifying which e-documents do not require review because they contain no relevant information.[52] Metadata also is searchable; thus, search strategies that facilitate source document review could be used to search metadata.[53] This observation suggests that, even if metadata production doubles or triples, the total volume of ESI generated via an e-discovery process would not be more burdensome than traditional discovery because a search-directed review of the ESI would relieve humans from reviewing every word. Thus far, the discussion regarding search-driven e-discovery has focused on how a search strategy facilitates discovery. Few commentators appreciate that search-driven metadata review may fundamentally change the nature of the discovery process. In business, documents often are created in a self-serving fashion, such that the documents detail what a business organization should have done rather than indicating what actually happened.[54]

---

the Use of Search and Information Retrieval Methods in E-Discovery, 8 SEDONA CONF. J. 189, 192 (2007) [hereinafter *Best Practices*]; *see also* BUILDING AN ELECTRONIC RECORDS ARCHIVE AT THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION: RECOMMENDATIONS FOR A LONG-TERM STRATEGY 5 (Robert F. Sproull & Jon Eisenberg eds., Nat'l Acad. Press 2005), *available at* http://books.nap.edu/catalog.php?record_id=11332.

48. As the legal profession becomes more comfortable with search-directed discovery, it is questionable whether there will still be demand at large law firms for associates to perform as much document review work. *See Best Practices*, *supra* note 47, at 194; BUILDING AN ELECTRONIC RECORDS ARCHIVE AT THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION: RECOMMENDATIONS FOR A LONG-TERM STRATEGY, *supra* note 47.

49. Zantaz: End the Guesswork. Automate eDiscovery, FORBES, Mar. 31, 2008 at 39 [advertisement]; *see also* Posting of Robert Hundock, *Data Culling Strategies for Electronic Stored Information (ESI)* to E-DISCOVERY LEGAL AND TECHNOLOGY UPDATES, http://ediscoverylaw.us/2008/02/20/data-culling-strategies.aspx (Feb. 20, 2008, 1:06 AM).

50. *See* Gen. Elec. v. Lear Corp., 215 F.R.D. 637, 640 (D. Kan. 2003); McPeek v. Ashcroft, 202 F.R.D. 31, 32-33 (D.D.C. 2001).

51. *See* Treppel v. Biovail Corp, 233 F.R.D. 363, 374 (S.D.N.Y. 2006).

52. *See* Wood v. Sempra Energy Trading Corp., No. 3:03-CV-986 (JCH), 2005 WL 3465845, at *4-6 (D. Conn. Dec. 9, 2005); United States v. Amerigroup Ill. Inc., No. 02 C 6074, 2005 WL 3111972, at *2-3 (N.D. Ill. Oct. 21, 2005); *In re* Ford Motor Co., 345 F.3d 1315, 1316-17 (11th Cir. 2003); *McPeek*, 202 F.R.D. at 34; *see also* THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 34-35 (Jonathan M. Redgrave et al. eds., 2003).

53. *See* JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE 22-23, 263-66 (Portfolio 2005).

54. *See Review Prompts Restatement of Earnings at GE*, BUS. REV. (Albany), May 6, 2005, http://www.bizjournals.com/albany/stories/2005/05/02/daily44.html. When a company restates its earnings, it is tacitly acknowledging that the previously published earning statement reflected what the company should have or wanted to achieve, and not what the business had actually achieved. *See id.* Misleading statements of this nature are

Metadata, on the other hand, frequently reflects real occurrences and essentially creates an audit trail that can be used to test the veracity of assertions made in a business record. For example, systems metadata can reveal which documents an individual actually reviewed, while application metadata may suggest what information has been withheld. In short, it is possible to profile the person who created and used e-documents by searching and analyzing ESI metadata.

C. Profiling Physicians

Historically, the medical community has opposed attempts to profile physicians. These profiles, often constructed from crude administrative data (e.g., billing data), were considered a travesty by the medical community. These profiles were considered misleading because they did not necessarily reflect actual patient care, were based on non-standardized terminology, and frequently contained misclassified information.[55]

In today's healthcare market, however, a growing demand exists for accurate physician profiles. Consumer advocates want "a national set of principles to guide measuring and reporting to consumers about doctors' performance."[56] Physician profiling, including the public reporting of physician-specific data, is also an integral component of reputational incentives. As employers, healthcare payors, and labor organizations insist physicians should be held more accountable, the demand for physician profiling will increase regardless of the medical community's objections.[57] To help meet the increased demand for physician profiles, companies such as HealthGrades[58] have entered the market. Unfortunately, even if existing physician profiles were based on standard definitions and misclassifications

---

common in the healthcare field as doctors often describe in the medical record the care they should have given, rather than the care they actually gave. *See infra* Part IV.

55. McLean, *Metadata*, *supra* note 12, at 405 (citing David M. Shahian et al., *Comparison of Clinical and Administrative Data Sources for Hospital Coronary Artery Bypass Graft Surgery Report Cards*, 115 CIRCULATION 1518, 1523-25 (2007)). *See also* Rebecca D. Kush et al., *Electronic Health Records, Medical Research, and the Tower of Babel*, 358 NEW ENG. J. MED. 1738, 1738 (2008) ("Without the use of common vocabularies, it is impossible not only for a given hospital's computer system to understand a patient record from another hospital, but also for researchers to compare data across organizations or to collect sufficient data to make informed decisions.").

56. CONSUMER-PURCHASER DISCLOSURE PROJECT, CONSUMERS, HEALTH CARE PURCHASERS, PHYSICIANS, AND HEALTH INSURERS ANNOUNCE AGREEMENT ON PRINCIPLES TO GUIDE PHYSICIAN PERFORMANCE REPORTING 1 (2008), http://healthcaredisclosure.org/docs/files/PatientCharterDisclosureRelease040108.pdf.

57. *See* CONSUMER-PURCHASER DISCLOSURE PROJECT, *supra* note 56, at 2.

58. HealthGrades, http://www.healthgrades.com (last visited Sept. 9, 2008) (selling "report cards" that detail physicians' training, experience, and discipline).

were eliminated,[59] profiles such as those obtained from HealthGrades, would still not necessarily reflect actual patient care.[60]

Alternatively, rather than using administrative data or performance measures[61] to profile physicians, EMR metadata physician profiles would reflect the actual care given by a doctor.[62] Entrepreneurial software vendors are positioning themselves to gain control of this market.[63] Because the technology to create EMR metadata physician profiles already exists, the greatest barrier to using metadata physician profiles may be the slow diffusion of EMRs into clinical practice.[64]

Even though the widespread use of EMR metadata physician profiles remains several years in the future,[65] the American Medical Association (AMA) already is expressing its concerns. According to the AMA, third parties should only have access to EMR metadata to obtain "clinical data"

---

59. This assumption is often not true. *See* Hui Zheng et al., *Profiling Providers on Use of Adjuvant Chemotherapy by Combining Cancer Registry and Medical Record Data*, 44 MED. CARE 1, 1-7 (2006) (noting that registrar data is often not collected or analyzed in a systematic manner).

60. *Cf.* Samuel Cykert, Grace Kissling, & Charles J. Hansen, *Patient Preferences Regarding Possible Outcomes of Lung Resection: What Outcomes Should Preoperative Evaluations Target?*, 117 CHEST 1551, 1551 (2000) ("Whether patients suffer from chronic lung disease or not, they do not regard the postoperative outcomes reported in the lung surgery literature as sufficiently [ominous] to forego important surgery. However, [patients perceive] physical debility . . . as extremely undesirable, and anticipation of its occurrence could deter surgery.").

61. Performance measures, including antibiotic usage, are increasingly being used to assess a physician's quality of care. *See, e.g.*, Timothy Bhattacharyya & David C. Hooper, *Antibiotic Dosing Before Primary Hip and Knee Replacement as a Pay-for-Performance Measure*, 89-A J. BONE & JOINT SURGERY 287, 287-91 (2007). Few physicians believe that performance measures, either alone or in combination with other performance measures and/or mortality data, reflect actual patient care. On the contrary, physicians view performance measures as merely a manifestation of the Hawthorn effect. *See* Robin Upton's Research, *Some Problems of Thinking by the Numbers*, Mar. 7, 2003, http://www.robinupton.com/research/publications/some_problems_of_thinking_by_numbers.html (last visited Jan. 25, 2009).

62. *Cf.* NAT'L INST. OF HEALTH, NIH ROADMAP PROGRAM RE-ENGINEERING THE CLINICAL RESEARCH ENTERPRISE: SUMMARY OF NIH ROADMAP NETWORK INVESTIGATOR MEETING (2006), http://rd100.cceb.med.upenn.edu/crcu_html/roadmap/mtgs/may_special_2006/NCRR_SummaryFinal_20060530.pdf.

63. *See* Press Release, ThomasNet.com, AccuStudy(TM); Revolutionizing Time-and-Motion Studies (Jan. 10, 2002), http://news.thomasnet.com/fullstory/6070 (discussing a commercial software product that uses metadata to perform a time-and-motion study).

64. The market penetration of the EMR is far from ubiquitous. *See* Catherine M. DesRoches et al., *Electronic Health Records in Ambulatory Care – A National Survey of Physicians*, 359 NEW ENG. J. MED. 50, 56 (2008) (indicating that only seventeen percent of physicians' practices have basic EMR technology); *see also Hospital EMR Use Not Yet Widespread*, AMNEWS, Mar. 19, 2007, http//www.ama-assn.org/amednews/2007/03/19/bicb0319.htm [hereinafter *Hospital EMR*] (observing that only eleven percent of community hospitals have completely converted from paper records to EMRs).

65. *See Hospital EMR*, *supra* note 64.

needed for "payment and [health care] operations."[66] Moreover, the AMA believes that physicians should be notified "on a case-by-case basis of any EMR metadata analysis undertaken."[67] Such statements imply that if the AMA's position prevails, third parties would be barred from constructing EMR metadata profiles of physicians. Why does the AMA take such a strong stance against access to EMR metadata? A possible answer is that EMR metadata could contain unfavorable information about physicians.

However, the AMA is unlikely to prevent the use of EMR metadata in the long run. Two recent studies that used actual patient care information demonstrated that EMR metadata could objectively measure the quality of care given by a physician (how assiduously the physician analyzes a patient's condition)[68] and how efficiently a physician provides patient care (time-and-motion study).[69] Both of these studies examined the metadata audit trail left by a physician every time he or she logged into an EMR by tracking the doctor's Unique Physician Identification Number (UPIN).[70] The UPIN is similar to a digital fingerprint left on e-documents handled by a computer user.[71] Thus, an individual only needs to search the EMR for the physician's UPIN to discover which EMR documents a physician has reviewed.[72] If one uses the EMR as a starting point, one can discover who has viewed a particular record by searching that record's metadata for the UPINs attached to the file.[73]

The first study of EMR metadata focused on the radiographic viewing habits of physicians-in-training.[74] During a five-month period, the study retrospectively reviewed the EMR metadata for all radiographic images viewed by the medical students and general-surgery residents on a single surgery service.[75] The study found that the number of images viewed by physicians-in-training increased with increasing years of professional

66. Kevin B. O'Reilly, *AMA Wants Limits on Insurers' Use of EMR, Claims Data*, AMA NEWS, Dec. 4, 2006, http://www.ama-assn.org/amednews/2006/12/04/bisc1204.htm.

67. *Id.*

68. McLean, *Metadata*, *supra* note 12, at 408.

69. McLean, *Tragedy*, *supra* note 12.

70. McLean, *Metadata*, *supra* note 12, at 406; *see also* McLean, *Tragedy*, *supra* note 12.

71. *See* McLean, *Metadata*, *supra* note 12, at 406; *see also* McLean, *Tragedy*, *supra* note 12.

72. *See* McLean, *Metadata*, *supra* note 12, at 406; *see also* McLean, *Tragedy*, *supra* note 12.

73. *See, e.g.*, AM. COLL. OF RADIOLOGY, PRACTICE GUIDELINE FOR DETERMINANTS OF IMAGE QUALITY IN DIGITAL MAMMOGRAPHY IN: PRACTICE GUIDELINES AND TECHNICAL STANDARDS 535-559 (2007), *available at* http://www.acr.org/SecondaryMainMenu Categories/quality_safety/guidelines/breast/image_quality_digital_mammo.aspx. The UCLA Medical Center almost certainly used EMR metadata in this way, as a "digital fingerprint" to determine who had been looking in the medical records of celebrities.

74. McLean, *Metadata*, *supra* note 12, at 406.

75. *Id.*

experience.[76] This was an expected result of the study.[77] On the other hand, an unexpected finding was that regardless of the number of years of professional experience, physicians-in-training almost never viewed routine admission chest x-rays.[78] Since few physicians, other than radiologists, review routinely-ordered radiographic examinations, this finding suggests a reason why patients with abnormal admission chest x-rays tend to file medical malpractice lawsuits against radiologists.[79]

The study of the radiographic viewing habits of physicians-in-training demonstrated how EMR metadata can be used as "digital fingerprint" evidence. To illustrate, consider a situation where the EMR contains a physician's statement that he or she had personally reviewed a particular radiographic study and found the study to be "within normal limits" (WNL).[80] Not infrequently, WNL impressions are wrong. When utilizing PMRs, physicians could rationalize their erroneous impression by indicating they had made an honest mistake rather than admitting that they had never reviewed the x-ray image or the radiologist's report.[81] Such rationalizations often were accepted because the only record of care given to patients was the doctor's own notes.

However, with the use of EMRs, the EMR metadata functions as an independent record that can challenge a physician's credibility. If a physician never views a radiographic image, the physician's UPIN will never attach to that file. Moreover, physicians who look only at one image of a computed tomography (CT) scan will no longer be able to assert that they reviewed the whole set of images, because a physician's UPIN digital fingerprint is left on each individual image. Based on this information, a jury reasonably could conclude that a physician provided suboptimal care if the physician reviewed only one CT scan image out of several hundred images.

The second study demonstrating how EMR metadata could be used to profile physicians' actual work habits utilized a time-and-motion

76. *Id.* at 406-08.

77. *Id.*

78. *Id.* at 408.

79. When patients with lung cancer sue their physicians, the two most common reasons for the lawsuit are: (1) the radiologist failed to perceive an abnormality and (2) the treating physician failed to notice an abnormal chest x-ray report in the patient's medical record. The problem is that no one checks the behavior of the radiologist or the primary care providers on a regular basis. Thomas R. McLean, *Why Do Physicians Who Treat Lung Cancer Get Sued?*, 126 CHEST 1672, 1678 (2004).

80. *See* Michael D. Freeman & Christopher Centeno, *A Fatal Case of Secondary Gain: A Cautionary Tale*, 9 AM. J. CASE REP. 97, 98 (2008) (referring to the adage that when physicians write "WNL" they actually mean "we never looked").

81. McLean, *Why Do Physicians Who Treat Lung Cancer Get Sued?*, *supra* note 79, at 1677.

technique.[82] Rather than timing the residents with a stopwatch, the study used time-signature metadata to estimate how much time surgery residents spent evaluating each clinic patient.[83] During the study period, residents received incentives to motivate them to see patients more efficiently.[84] This metadata time-and-motion study demonstrated that the incentive package resulted in a statistically significant reduction in clinic time compared to historic controls.[85] Accordingly, attorneys should realize that time-signature metadata could also be valuable evidence in healthcare fraud litigation.

For example, consider a situation where a physician has engaged in upcoding.[86] Upcoding occurs when a physician bills for a higher level of services than the he or she truly provided.[87] If a physician's records do not contain the documentation necessary to support the care level that was billed, the physician has engaged in upcoding.[88] In actual practice, the EMR facilitates upcoding because physicians can "cut-and-paste" information found elsewhere in the record into a current entry to obviate the

82. Classically, a time-and-motion study was labor-intensive because it required an observer with a stop watch to follow a worker throughout the course of a workday. Samuel B. Welch & Lawrence T. Kim, Presentation at 31st Annual Meeting of the Association of VA Surgeons Meeting, Effect of Electronic Workload on Physician-Patient Interaction Time (May 12, 2007). One of the key advantages of using metadata to perform time-and-motion studies is that it is not labor intense and with the right software can now be performed automatically.

83. McLean, *Tragedy*, *supra* note 12. Time-signature metadata is the metadata produced when a physician signs an e-note in the EMR.

84. *Id.* Residents were instructed to limit their notes to less than 500 words, and they were required to evaluate a specific number of patients before they could leave clinic.

85. *Id.*

86. Upcoding is a particular type of healthcare fraud. It can be prosecuted under a number of legal theories, including the False Claims Act, when the claim is submitted to the federal government, or the Health Insurance Portability and Accountability Act, if the claim is submitted to a private insurer. False Claims Act, 31 U.S.C. §§ 3729-3733 (2000); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 2016 (1996).

87. In general, as the level of care given increases (from level 1 to level 5), a physician has to spend more time with a particular patient to gather the information necessary to meet the heightened documentation requirements of the higher level of care. On the other hand, if the physician bills for a higher level of care, the physician will be paid more. *See* E/M University Level 1 Office Consult, http://emuniversity.com/Level1OfficeConsult.html (last visited Sept. 17, 2008) (requiring about fifteen minutes of face time between the patient and physician for a level 1 consult); *see also* E/M University Level 5 Office Consult, http://emuniversity.com/Level5OfficeConsult.html (last visited Sept 17, 2008) (requiring about sixty minutes of face time between the patient and physician for a level 5 consult).

88. *See* AM. MED. ASS'N, EVALUATION AND MANAGEMENT SERVICES GUIDE 7 (2008), http://www.cms.hhs.gov/mlnproducts/downloads/eval_mgmt_serv_guide.pdf; *see also* David Hellerstein, *HIPPA's Impact*, HEALTH MGMT. TECH., Apr. 1999, at 10, *available at* http://archive.healthmgttech.com/archives/bus0499.html.

need to spend time with the patients.[89] Auditing a physician's medical records and billing practice can prove that a physician engaged in upcoding, but doing so is labor intensive. Moreover, payors would prefer to validate and deny claims that are initially suspicious for upcoding rather than paying doctors upon receipt of a claim and pursuing fraudulent behavior later.[90]

Alternatively, screening for upcoding with an EMR metadata time-and-motion study would be simpler, and it also would provide payors with a method to validate and deny suspicious claims. The time-and-motion study indicated that time-signature metadata provides an estimate of how much time a physician spends with a patient.[91] This time estimate can be compared to standard time estimates to calculate how long a patient's encounter with a physician should last.[92] For example, if a provider submitted a bill for a level of care that was inconsistent with the metadata estimated time for the patient encounter, the bill could be flagged for further investigation, and payment on the claim could be suspended.[93] Furthermore, if the doctor engaged in a pattern of billing behavior where a substantial number of claims were suspended, a more formal audit of the doctor's billing practice may be in order.

Given the power of EMR metadata to screen for physician billing fraud, it is not surprising that the AMA is seeking to limit access to EMR metadata.[94] In addition, the AMA may wish to limit access to EMR metadata for reputational incentives such as the public reporting of physician-specific clinical data.[95] Reputational incentives may be used to remove physicians from the market who consistently fail to practice evidence-based medicine.[96] Once considered an ineffective tool for modifying physicians' behavior, reputational incentives are increasingly

89. Conversely, "cutting and pasting" may provide a clue that upcoding has occurred. For example, the presence of a different "voice" in the cut and pasted segment may suggest that it was not written by the same author. *See* Selena Chavis, *Detouring Deception: New Antifraud Requirements for Electronic Health Records are Designed to Head Off Potential Problems*, FOR THE REC., Aug. 20, 2007, at 21, *available at* http://www.fortherecordmag.com/archives/ftr_08202007p18.shtml.

90. AM. MED. ASS'N, *supra* note 88.

91. Welch & Kim, *supra* note 82.

92. *See* E/M University Level 1 Office Consult, *supra* note 87; *see also* E/M University Level 5 Office Consult, *supra* note 87.

93. Presumably, payors will have a policy in place to resolve sporadic billing inconsistencies.

94. *See* O'Reilly, *supra* note 66.

95. Thomas R. McLean, *Will Reputational Incentives Stimulate a Reversal of the Physician Brain Drain?*, 13 J. HEALTH SERVS. RES. & POL'Y 50, 50–52 (2008).

96. *See generally* INST. OF MED. OF THE NAT'L ACAD., REWARDING PROVIDER PERFORMANCE: ALIGNING INCENTIVES IN MEDICARE 2 (Nat'l Acad. Press 2007) (indicating that performance reporting can motivate providers to improve); Thomas R. McLean, *Application of Administrative Law to Health Care Reform: The Real Politik of Crossing the Quality Chasm.* 16 J.L. & HEALTH 65, 69-70 (2001-2002).

recognized as a reliable method for securing physicians' compliance with evidenced-based practice patterns.[97]

For example, in the Jha and Epstein study, a review of surgeons' logs on performing coronary artery bypass graft (CABG) operations in New York State demonstrated a correlation between the use of reputational incentives and surgeons' activity levels.[98] The study demonstrated that surgeons with the highest mortality rates disproportionately exited the market.[99] A second study by McLean examined the impact of reputational incentives on surgeons' willingness to perform risky CABG operations.[100] This study found that surgeons in markets that employed reputational incentives performed fewer CABG operations per capita and selected less risky cases to perform than surgeons who operated in markets that did not employ reputational incentives.[101]

Thus, evidence is accumulating that reputational incentives force physicians from the market who are non-compliant with evidence-based practice of medicine. At first glance, the notion of forcing physicians out of any market in the United States may seem peculiar, especially in light of the popular myth that the United States has a shortage of physicians. After all, for many years, the AMA and other institutions with a business interest in training physicians have published data suggesting that the United States has, or will have, a shortage of physicians.[102]

Yet, recent analysis of both Medicare data and market dynamics suggests the opposite. Analysis of Medicare data demonstrates that

> [the] current delivery and payment systems often make it more "efficient" for primary care physicians to see patients they already know (diminishing others' access to primary care) and for all physicians to narrow their scope of practice (increasing referrals to specialists) and to admit patients to the hospital (where hospitalists manage their care).[103]

---

97. *See generally* INST. OF MED. OF THE NAT'L ACAD., *supra* note 96, at 1-31.

98. Ashish K. Jha & Arnold M. Epstein, *The Predictive Accuracy of the New York State Coronary Artery Bypass Surgery Report-Card System*, 25 HEALTH AFF. 844, 844 (2006).

99. *Id.* at 854.

100. Thomas R. McLean, *In New York State, Do More Percutaneous Coronary Interventions Mean Fewer or More Complex Referrals to Cardiac Surgeons?*, 6 AM. HEART HOSP. J. 30, 35 (2008).

101. *Id.*

102. *See* John K. Iglehart, *Grassroots Activism and the Pursuit of an Expanded Physician Supply*, 358 NEW ENG. J. MED. 1741, 1743 (2008) ("In general, the methods that have been used to determine future demand involve assessing current levels of physician service, measuring the effect of changing demographics and other forces that will impinge on the supply of doctors, and then projecting these items forward to arrive at a conclusion. The reports in general assume that the current patterns of new graduates, specialty choice, and practice behavior will continue with little or no change.").

103. David C. Goodman & Elliot S. Fisher, *Physician Workforce Crisis? Wrong*

This observation helps to explain why Medicare patients and those patients with private insurance have little trouble evaluating a physician.[104] Further, the nature of physician-service contracts indicates that a surplus of physicians exists.[105] Today, almost all employment contracts offered to physicians are adhesion contracts. If there was a shortage of physicians, the medical community would have more negotiating power to obtain better terms for employment and adhesion contracts.[106] Further, if a higher demand for physicians' services existed in the marketplace, physicians would be able to garner higher reimbursements based on basic supply and demand principles.

The perception that the United States has a shortage of physicians also is inconsistent with America's consumption of healthcare services. "American women undergo twice as many hysterectomies per capita as British women and four times as many as Swedish women."[107] Such demographic data, similarly found with many other surgical procedures, may indicate that gynecologists in the United States are over prescribing hysterectomies for their own benefit. Not surprisingly, many "insurance executives look at physician-supply estimates with a skeptical eye because they believe physicians are able to create their own demand."[108]

The utility of reputational incentives can be seen when viewed against the backdrop of an oversupply of physicians who over prescribe expensive treatment. By using reputational incentives, healthcare payors intend to provide impetus for physicians to comply with evidence-based medical practices and remain practicing in the marketplace. Given the ability of EMR metadata to create unflattering physician-specific profiles, reputational incentives based on those profiles may force providers out of the market. Thus, the position of the AMA and many physicians limiting access to EMR becomes clearer.

Containment of EMR metadata usage for much longer seems unlikely. First, economic concerns drive healthcare delivery. Evidence-based medical practices are cost effective.[109] For example, the cost of managing a well-controlled diabetic, one that follows evidence-based treatments, is

---

Diagnosis, Wrong Prescription, 358 NEW ENG. J. MED. 1658, 1660 (2008).

104. *See generally* Iglehart, *supra* note 102, at 1746-47.

105. Personal observation.

106. As a principle of economics, if consumers believe that a shortage of physicians exists, then physicians would be able to demand higher levels of reimbursements.

107. Curt Pesmen, *5 Operations You Don't Want to Get — and What to Do Instead*, CNN.com, June 27, 2007, http://www.cnn.com/2007/HEALTH/07/27/healthmag.surgery/index.html.

108. Iglehart, *supra* note 102, at 1747.

109. *See* Thomas R. McLean, *Crossing the Quality Chasm: Autonomous Physician Extenders Will Necessitate a Shift to Enterprise Liability Coverage for Health Care Delivery*, 12 HEALTH MATRIX 239, 253-54 (2002).

$5,000 per year; this compares favorably with the cost of managing a poorly controlled diabetic at $45,000 per year.[110] Well-controlled diabetics achieve these cost savings because they consume fewer emergency room services.[111] While the compliance with evidence-based medicine practices needed to achieve a well-controlled diabetic state is a complex subject,[112] clearly healthcare payors want to improve compliance with these evidence-based practices since payors institute reputational incentives and give physicians pay-for-performance bonuses.[113] To achieve such compliance, notwithstanding the AMA's wishes, it seems likely that healthcare payors will use EMR metadata profiles and reputational incentives to select guideline-compliant physicians.[114]

Second, litigation will likely promote third-party access to EMR metadata despite the AMA's view. As the study concerning the radiology viewing habits of physicians-in-training demonstrates, EMR metadata provides an inference concerning the actual care given by a physician, rather than the description of the care found in the EMR that may not be accurate due to the subjective nature of the entry.[115] Depending on one's point of view, EMR metadata may be unfavorable or exculpatory to the physician-defendant. Accordingly, parties in healthcare litigation will want access to EMR metadata to support their versions of medical reality. Certainly, in a court of law, the AMA does not determine the information admitted into evidence. To the contrary, the rules of civil procedure and evidence will determine whether EMR metadata is admitted as evidence.

---

110. *See* HealthPartners: Beyond Benefits, http://www.healthpartners.com:747/media/beyondbenefits/BB0106_br.htm (last visited Jan. 25, 2009). *See generally* INST. OF MED. OF THE NAT'L ACAD., PERFORMANCE MEASUREMENT: ACCELERATING IMPROVEMENT (Nat'l Acad. Press 2006).

111. *See generally* DAVID C. WARNER, GENIE NYER & LISA KERBER, CARE THAT PAYS FOR ITSELF?: COMMUNITY INITIATIVES TO REDUCE THE COST OF UNCOMPENSATED HEALTH CARE (Lyndon B. Johnson Sch. of Pub. Affairs 2006), *available at* http://www.stdavidsfoundation.org/downloads/collaborations_lbj_prp.pdf (discussing various community initiatives to educate and follow up with diabetic patients to reduce the amount of time spent in the hospital and the number of emergency room visits).

112. Non-compliance with evidence-based medicine is caused by both patient and physician factors.

113. *See* INST. OF MED., LEADERSHIP BY EXAMPLE: COORDINATING GOVERNMENT ROLES IN IMPROVING HEALTH CARE QUALITY, 45-46 (Janet M. Corrigan et al. eds., Nat'l Acad. Press 2003). *See generally* Thomas R. McLean, *Medical Rationing: The Implicit Result of Leadership by Example*, 36 J. Health L. 325 (2003).

114. Press Release, Bus. Wire, Quantros Launches New Software for Managing Disruptive Events in Healthcare Facilities (Apr. 15, 2008), http://www.pr-inside.com/quantros-launches-new-software-for-managing-r539201.htm.

115. McLean, *Metadata*, *supra* note 12, at 410.

III. E-DISCOVERY AND EMR METADATA

A. History of E-Discovery

Before 2006, e-documents were discoverable if they were: (1) "relevant to any party's claim or defense"; (2) "reasonably calculated to lead to the discovery of admissible evidence"; and (3) not subject to privilege.[116] If the producing party objected to a request for production, "the burden shift[ed] to the party seeking the information to demonstrate that the requests [were] relevant to the subject matter involved in the pending action."[117] Therefore, in the pre-amendment era, the question of whether metadata was relevant and/or needed to be produced did not have a clear answer.[118]

In pre-amendment cases, the courts tended to view metadata as if it was virtually all system metadata. Courts frequently have quoted the view put forth in *Williams* that most metadata "has no evidentiary value, and . . . reviewing it is a waste of resources."[119] Accordingly, the "emerging standards of electronic discovery appear to articulate a general presumption against the production of metadata."[120] Indeed, before 2006, unless specifically requested, the production of portable document format (PDF) or tagged image file format (TIFF) image file, which are free of metadata,[121] was legally sufficient to meet the discovery requirements under FRCP Rule 34.[122]

---

116. FED. R. CIV. P. 26(b)(1); Ky. Speedway, L.L.C. v. NASCAR, No. 05-138-WOB, 2006 U.S. Dist. LEXIS 92028, at *11-12 (E.D. Ky. Dec. 18, 2006) (citing Lewis v. ACB Bus. Servs., Inc., 135 F.3d 389, 402 (6th Cir. 1998)).

117. *Ky. Speedway, L.L.C.*, 2006 U.S. Dist. LEXIS 92028, at *12 (citing Allen v. Howmedica Leibinger, GmhH, 190 F.R.D. 518, 522 (W.D. Tenn. 1999)).

118. *See* Joseph Poluka & Inbal Paz, *Mining Buried Electronic Data: Increasing Criminal and Civil Case Concerns*, MONDAQ, Mar. 5, 2008, http://www.mondaq.com/article.asp?article_id=57926&1k=1.

119. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 651 (D. Kan. 2005) (quoting THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 46 cmt. 12.a (Jonathan M. Redgrave et al. eds., 2005)).

120. *Id.* at 652.

121. *See supra* note 37.

122. Pace v. Int'l Mill Serv., Inc., No. 2:05CV69, 2007 U.S. Dist. LEXIS 34104, at *3 (N.D. Ind. May 7, 2007); *Williams*, 230 F.R.D at 652 ("[U]nless 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."); Wyeth v. Impax Lab., Inc., 248 F.R.D. 169, 171 (D. Del. 2006) ("[I]f the requesting party can demonstrate a particularized need for the native format of an electronic document, a court may order it produced.") (citing Ad Hoc Committee for Electronic Discovery of the U.S. District Court for the District of Delaware, "Default Standard For Discovery of Electronic Documents ("E-Discovery") Rule 6, *available at* http://www.ded.uscourts.gov/Announce/Policies/Policy01.htm); *Ky. Speedway, L.L.C.*, 2006 U.S. Dist. LEXIS 92028, at *21 ("Rule 34 specifically includes the term 'data compilations' as documents that must be produced, but does not define that term to

When the *Williams* court addressed "emerging standards," it referred to the Sedona Principles,[123] articulated by the Sedona Conference in 2005.[124] These principles were highly influential in shaping the scope of e-discovery before the 2006 amendments to the FRCP. The Sedona Conference has great influence because its members are well-connected attorneys, judges, and law professors.[125] However, the conspicuous absence of significant numbers of plaintiffs' attorneys and consumer advocates from the Conference's attendance list may account for the anti-e-discovery tone of the Sedona Principles.[126] For example, Principle 9 observes that "[a]bsent a showing of special need," the producing party "should not be required to *preserve*, review, or produce deleted, shadowed, fragmented, or residual data or documents."[127] Similarly, Principle 12 states that "[u]nless it is material to resolving the dispute, there is no obligation to *preserve* and produce metadata absent agreement of the parties or order of the court."[128]

Economic principles best explain the Sedona Conference's views on ESI preservation. Compared to traditional discovery of paper documents, ESI discovery substantially increases both the cost of reviewing documents for privileged information[129] and the potential for the inadvertent release of privileged documents.[130] The Sedona Principles attempt to offset these

---

necessarily include metadata.").

123. *Williams*, 230 F.R.D. at 648. *See generally* THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (Jonathan M. Redgrave et al. eds., 2005), http://www.thesedonaconference.org/content/miscFiles/7_05TSP.pdf.

124. The Sedona Conference is a "501(c)(3) research and educational institute dedicated to the advancement of law and policy in the areas of antitrust law, complex litigation and intellectual property rights. It is supported by registrations, meeting fees, sponsorships and donations." The Sedona Conference Frequently Asked Questions, http://www.thesedona conference.org/content/faq (last visited Oct. 1, 2008).

125. *See, e.g.*, The Sedona Conference, Complex Litigation V, http://www.thesedona conference.org/conferences/20030424 (last visited Oct. 1, 2008).

126. *See* Hopson v. Mayor of Baltimore, 232 F.R.D. 228, 245 (D. Md. 2005) ("In many cases, such as employment discrimination cases or civil rights cases, electronic discovery is not played on a level field. The plaintiff typically has relatively few electronically stored records, while the defendant often has an immense volume of it. In such cases, it is incumbent upon the plaintiff to have reasonable expectations as to what should be produced by the defendant.").

127. SEDONA PRINCIPLES, *supra* note 52, at 10 (emphasis added).

128. *Id.* (emphasis added because the ability to preserve metadata is time dependant). *See infra* Parts III-IV for discussion of failure to preserve metadata as grounds for the imposition of sanctions.

129. This statement assumes that an electronic search (e-search) strategy was not employed. *See* Ky. Speedway, L.L.C. v. NASCAR, No. 05-138-WOB, 2006 U.S. Dist. LEXIS 92028, at *14-15, 26 (E.D. Ky. Dec. 18, 2006) (ordering defendant to produce even more documents, after the defendant spent more than $3 million dollars on document production without employing an e-search strategy). *See supra* Part II.

130. *See* Lava Trading, Inc. v. Hartford Fire Ins. Co., No. 03 Civ. 7037 PKC MHD, 2005 WL 66892, at *2 (S.D.N.Y. Jan. 11, 2005) (stating that inadvertent document

liabilities in a number of ways. For example, the Principles attempt to minimize the potential liability associated with the inadvertent release of privileged information found within application metadata by recommending that "[a]bsent specific objection, agreement of the parties, or order of the court, producing electronic data in a commonly accepted image format (paper, PDF, or TIF[F]) should be sufficient in most cases."[131] The Sedona Principles also attempt to limit the liabilities associated with ESI discovery through a "clawback" provision.[132] Under this provision, "if the requesting party finds a document that appears to be privileged, the producing party can 'claw back' the document without having waived any privilege."[133] Of course, nothing in the Sedona Principles prevents the opposing party from reading an inadvertently disclosed privileged document.

While courts may have considered image file production to be legally sufficient for discovery, the courts inconsistently have applied discovery rules to the underlying metadata in these files. On one hand, the courts recognized that metadata should be preserved.[134] On the other hand, even if metadata was preserved, courts often were unwilling to issue an order for the production of metadata.[135] In 2008, the Sedona Conference expressed

---

production, in certain circumstances, does not waive the attorney-client privilege); *see also* SEC v. Cassano, 189 F.R.D. 83, 85 (S.D.N.Y. 1999) (confirming that inadvertent production of privileged document does not waive privilege unless the party's conduct suggests that it was not concerned with the protection of the privilege); *cf.* Scott v. Beth Israel Med. Ctr., 847 N.Y.S.2d 436, 439-40 (N.Y. Sup. Ct. 2007) (determining that communication over a company's e-mail system waives attorney-client privilege when the company's e-mail policy states that employee should not consider their e-mail communications as private); *see also In re* Asia Global Crossing, Ltd., 322 B.R. 247, 256-59 (Bankr. S.D.N.Y. 2005) (stating that attorney-client privilege for e-mail communication depends upon company's e-mail policies regarding use and monitoring, company access to e-mail system, and employee notification of policy); *see also* Long v. Marubeni Am. Corp., No. 05 Civ. 639 (GEL)(KNF), 2006 U.S. Dist. LEXIS 76594, at *9-12 (S.D.N.Y. Oct. 19, 2006) (holding that plaintiff did not waive attorney-client privilege by using company owned computer for personal use, regardless of company's computer usage policy). *But see* Curto v. Med. World Commc'ns Inc., 99 Fair Empl. Prac. Cas. (BNA) 298, 300-02, 305 (E.D.N.Y. 2006) (affirming that employee did not waive attorney-client privilege by using company owned computer for personal use, regardless of company's computer usage policy).

131. SEDONA PRINCIPLES, *supra* note 52, at 42 cmt. 12.c.

132. *Id.* at 37 cmt. 10.d.

133. *Id.*

134. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 647 (D. Kan. 2005); *see also In re* Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 90-91 (D. Conn. 2005) (allowing defendant to produce e-documents as TIFF files, but instructing the defendant to preserve the native file with its metadata).

135. *See* Hopson v. Mayor of Baltimore, 232 F.R.D. 228, 245 (D. Md. 2005) (stating that the days when a party could expect to get every document requested are long gone); *see also* Williams v. Sprint/United Mgmt. Co. (Williams II), 99 Fair Empl. Prac. Cas. (BNA) 1502, 1508 (D. Kan. 2006) (taking the view that after a party had accepted paper discovery, a second round of ESI discovery was overly burdensome).

its own views regarding the controversy of metadata preservation.[136] According to the Conference, metadata preservation unnecessarily complicates ESI discovery because it could be intentionally or inadvertently corrupted[137] and preservation of metadata evidence for appeal requires special resources.[138] Further, to the extent that metadata has value in the authentication of an e-document, the Sedona Conference suggested that "many of the hurdles to authentication and admissibility of evidence can be overcome through agreement and stipulation. And even in those cases where authenticity is a legitimate concern, the parties should seek to discuss and perhaps narrow the scope of the dispute over ESI [metadata] in good faith."[139]

If the parties to litigation agree that an image file is a true and accurate reproduction of an original e-document, the value of metadata as evidence is substantially diminished; the only other likely use for metadata would be as an impeachment tool.[140] The Conference's 2008 assertions concerning metadata preservation do not appear to properly address the issues related to metadata and ESI discovery.

First, while it is true that commercial software products facilitate metadata corruption,[141] examination of the metadata is likely to reveal evidence of digital forgery.[142] Alternatively, metadata destruction may occur intentionally as part of a record destruction policy. A more rational approach to handling corrupt metadata would be to use a burden-shifting presumption. In situations where the court finds metadata to be corrupted, it should be presumed that the corruption occurred for the benefit of the producing party. The burden would then shift to the producing party to explain the metadata anomalies (*e.g.*, routine operations of the computer system or corruption due to a records retention policy).

---

136. ESI EVIDENCE, *supra* note 19, at 13.

137. *Id.*

138. *Id.* at 18.

139. *Id.* at 19.

140. For example, even if an image file is deemed legally sufficient for the production of ESI, metadata demonstrating a physician never viewed a radiographic image could be used to impeach a witness who testified to the contrary.

141. The simplest example of metadata corruption is a software program that takes a native e-document and converts it into an image file devoid of metadata. *See* ARCHITECTURES & APPLICATIONS DIV. OF THE SYS. & NETWORK ATTACK CTR. (SNAC), NSA, REDACTING WITH CONFIDENCE: HOW TO SAFELY PUBLISH SANITIZED REPORTS CONVERTED FROM WORD TO PDF 3-4 (2005), *available at* http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf.

142. *See* Chris Gaylord, *Digital Detectives Nab Photoshop Frauds: New Software Combs for Clues in Al Qaeda Tapes, Harry Potter Pages, and Celebrity Waistlines*, CHRISTIAN SCI. MONITOR (Boston), Aug. 29, 2007, § 2, at 13, *available at* http://www.csmonitor.com/2007/0829/p13s02-stct.html (discussing how missing metadata in a digital image was used as evidence that the photograph was a forgery).

Second, the Sedona Conference's belief that metadata has limited evidentiary value is predicated on the notion that a discovery agreement cannot be altered. At the beginning of the discovery process, parties to litigation may agree that metadata is not necessary. However, the parties have the ability to modify these agreements. If subsequent discovery suggests e-document corruption, the opposing party may file a motion for metadata production to determine the authenticity of the e-document. Therefore, a party that failed to preserve metadata based on any early e-discovery agreement may face sanctions for the spoilage of evidence in the future.[143]

Finally, the Sedona Conference's views on metadata production are impractical because of the Conference's belief that hash values can be virtually and universally substituted for metadata.[144] A hash value from an online calculator[145] is obtained by running ESI through a hashing algorithm.[146] The output of this algorithm is a unique identifier applicable to a specific ESI file. Because a hash value is based upon the entire e-document, including metadata,[147] changing a single bit of data in a multi-gigabyte native e-document completely changes the document's hash value.[148] Even the act of opening an e-document can change the e-document's hash value because it will add a piece of time-signature metadata to the file.[149]

The Sedona Conference views hash values, a sensitive indicator of e-document alteration, as a valuable screening tool for ESI corruption. Beyond screening for alterations, the actual application of hash-value analysis to ESI discovery and authentication has several limitations. The

143. *See infra* Part III.B.

144. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 547 (D. Md. 2007) ("Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4).)"; *see also, e.g.*, *Id.* at n.24 (citing United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information 20, http://www. mdd. uscourts. gov/ news/ news/ ESIProtocol. pdf (last visited April 10, 2007)).

145. FileFormat.info, Hash Functions, http://www.fileformat.info/tool/hash.htm (last visited Oct. 3, 2008).

146. Ralph C. Losey, *Hash: The New Bates Stamp*, 12 J. TECH. L. & POL'Y 1, 2 (2007).

147. Letter from Chylton Miller, Veterans Affairs IT specialist, to author (Mar. 25, 2008) (on file with the Beazley Institute for Health Law and Policy at the Loyola University Chicago School of Law).

148. *See* Losey, *supra* note 146, at 2. A hash value is not a single number, but is more akin to a matrix of information. *See* FileFormat.info, *supra* note 145.

149. This fact can frustrate the use of hash values as an authentication tool. Even if an e-document has otherwise been unaltered, a producing party will need to provide testimony and/or documentation that there has been no unauthorized viewing of the e-document in question. *See* Surety: The Power of Proof, Sedona Conference Commentary on ESI Evidence & Admissibility, http://www.surety.com/news/article/sedona_conference_commentary_on_esi_evidence_admissibility/ (last visited Oct. 3, 2008).

first consideration is determining the standard of comparison that should be used for a particular hash value. Unless the producing party provides access to its computer system, the hash value associated with a produced e-document cannot be verified as identical to the hash value of the e-document in the producing party's computer.[150] To avoid giving access to its computer system, the producing party will likely have one of its IT agents testify that the hash value of the produced e-document is identical to the hash value of the e-document within the computer system. Some courts have adopted elaborate e-foundation requirements for the authentication of ESI due to reliability concerns in connection with such self-serving testimony.[151]

Second, the sensitivity of hash values limits the utility of using this type of screening for ESI corruption. In any computer system, an e-document may exist in multiple copies.[152] If merely opening an e-document can change its hash value, determining which copy of an e-document in a computer system has the "true" hash value can prove difficult. This is the fundamental problem with using hash values for authenticating ESI. "All the evidence [within the] metadata components; [sic] including the 'what,' 'who' and 'when' [the document was manipulated] are hash

150. *See* Michael Cherry & Edward J. Imwinkelried, *The Danger of Exposure to the Internet*, CHAMPION, Dec. 2007, at 38, 41, *available at* http://www.nacdl.org/public.nsf/01c1e7698280d20385256d0b00789923/f4ee49d3875d5446052573ed0056ffa4?OpenDocument; *see also* LEXISNEXIS, ELECTRONIC DISCOVERY BEST PRACTICES 5 (2007), http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_ImplementEDiscBestPractices.pdf [hereinafter ELECTRONIC DISCOVERY BEST PRACTICES]; Eric Schwarz & Vincent Walden, *Attorneys Should Never Forget Who Is Responsible: Vendors Can Take the Anxiety out of Discovery, but Need Supervision*, NAT'L L.J. Aug. 20, 2007, S2, *available at* www.mondaq.com/article.asp?articleid=55666. It is worth noting that metadata can be used to establish a chain of custody and control.

151. *See* Am. Express Travel Related Servs. Co., Inc. v. Vinhnee (*In re* Vinhnee), 336 B.R. 437, 442-46 (B.A.P. 9th Cir. 2005) (refusing to admit ESI that did not satisfy the eleven-step process outlined by Imwinkelried); *see also* EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03[2] 62 (LexisNexis 7th ed. 2008); *cf.* United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001) ("Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility." (quoting United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988)). *But see* Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740, at *6-7 (N.D. Ill. Oct. 15, 2004) (noting that a third-party, archiving company can authenticate hardcopy printouts of ESI by affidavit); *see also* Sea-Land Serv., Inc. v. Lozen Int'l, L.L.C., 285 F.3d 808, 821-22 (9th Cir. 2002) (determining that the admissibility of evidence turns on testimony of the record custodian and errors created by printing an e-document concern its reliability, not its admissibility).

152. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 547 (D. Md. 2007) ("Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the 'final' or legally operative version.").

together . . . ."[153] If two seemingly identical documents are not accessed the same number of times, the documents will have different hash values, suggesting that one document has been altered. Unfortunately, absent the metadata analysis, hash values by themselves cannot explain how the documents differ.

The legal consequences of how two documents with different hash values are treated can be significant. For example, if one version of an e-document was merely viewed one more time than another copy, it may not be considered an original. If a court finds that it is unable to distinguish an original e-document from another version or from a forgery, the court may find it necessary to inquire whether evidence spoilage or fraud exists. In situations where an e-document's metadata has been forged to the point where it is not possible to reproduce the original source document, it could and should be presumed that the reason the metadata was corrupted was to obscure information that was adverse to the producing party. On the other hand, the audit trail found in the metadata that concerned who, what, where, and how an e-document was altered would more easily differentiate the original source document from later and corrupt versions.[154] In short, given a choice between hash-value authentication and metadata authentication, metadata authentication seems superior.[155]

This does not mean that hash values have no value in litigation.[156] The Sedona Conference may be correct that hash-value screening is more cost effective in large-scale ESI production, such as in class-action securities litigation. However, the cost benefits of hash-value analysis compared to having access to an e-document's metadata are likely to be less apparent in small-scale ESI production, such as in healthcare litigation. With far fewer documents being admitted into evidence, laying a foundation for an EMR would not be substantially simpler if it were laid by hash-value analysis rather than by metadata.[157] Additionally, in any healthcare litigation, one party or the other may want to have EMR metadata admitted. In cases

153. Evident Technologies Frequently Asked Questions General Principles, http://evident-technologies.net/Seals_Tech_Summary/FAQ/FAQ.php (last visited Oct. 2, 2008).

154. *See supra* notes 141-145.

155. Detection of a specific alteration in an e-document is more readily apparent with metadata than with hash values. For example, the MD5 hash value for "I manipulated this sentence" is 3086e401cae727bc9536d64e32a6903e, while the MD5 hash value for "I did not manipulate this sentence" is 3086e401cae727bc9536d64e32a6903e. *See* FileFormat.Info, *supra*, note 145.

156. Given the nascent nature of the law concerning e-discovery, it cannot be definitively determined which method of authentication, metadata or hash value, is superior. *See Lorraine*, 241 F.R.D. at 537-8 ("Very little has been written, however, about what is required to insure that ESI obtained during discovery is admissible into evidence at trial, or whether it constitutes 'such facts as would be admissible in evidence' for use in summary judgment practice." (citing FED. R. CIV. P. 56(e)).

157. *See infra* Part III.C.

where the doctor has made a mistake, a plaintiff or BOME will want to have the EMR metadata admitted into evidence to demonstrate the doctor's wrongdoing. Conversely, in cases where a doctor truly is innocent, the doctor likely will move to have the EMR metadata admitted to corroborate his or her version of the facts, or alternatively, to show why the plaintiff's expert's theory does not fit the facts in the case.

B. Impact of 2006 E-Discovery Amendments

Against this backdrop, the 2006 amendments to the FRCP were introduced to facilitate ESI discovery.[158] Interestingly, the new rules define neither "ESI" nor "metadata."[159] Given the judicial system's pre-2006 struggles with the scope of e-discovery, the omission of a definition for ESI should be viewed as intentional. Rather, the amended FRCP elected to identify ESI expansively to include "writings, drawings, graphs, charts, photographs, sound recordings, images, and *other data or data compilations*—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."[160]

The new e-discovery rules modify the traditional e-discovery rules in five discrete ways: (1) encouraging that ESI discovery be addressed early in litigation; (2) addressing the forms of ESI to be produced; (3) handling discovery situations where ESI is not reasonably accessible; (4) providing a procedure for privilege as a post-production safe harbor for sheltering ESI; and (5) tailoring sanctions for non-compliance with ESI discovery. [161] However, it would be appropriate to review the application of these rules to e-documents in general before applying these rules to EMR metadata.

The potential reach of e-discovery is broad, as it extends to any relevant matter related to a party's claim or defense.[162] To narrow the scope of e-discovery, the parties must hold a Rule 26 conference "as soon as practicable—and in any event at least 21 days before a scheduling

158. *See generally* Rick Wolf, Lexakos, L.L.C., The New Federal Rules of Civil Procedure: E-Discovery and Record Management, http://www.lexakos.com/Upload/Compliance%20Week%20Deck.pdf (last visited Oct. 4, 2008).

159. FED. R. CIV. P. 34(a)(1)(A).

160. FED. R. CIV. P. 34(a)(1)(A) (emphasis added). While no court has explicitly ruled on the meaning of "other data or data compilations," depending on the definition of metadata used, it is either ESI "other data" or a "data compilation" of ESI.

161. Conor R. Crowley, *E-Discovery: Proposed Changes to the Federal Rules of Civil Procedure*, LEAD COUNS., Summer 2006, at 7, http://www.labaton.com/_cs_upload/en/about/published/4314_1.pdf.

162. FED. R. CIV. P. 26(b)(1); *see also* FED. R. CIV. P. 16(c)(2)(D) (stating that one purpose of a pre-trial conference is to avoid "unnecessary proof and cumulative evidence, and limiting the use of testimony under Federal Rule of Evidence 702").

conference is to be held."[163] Afterwards, the parties have only 14 days to make their initial disclosures.[164] Parties charged with ESI production have only "14 days to object to the admissibility of an opponent's proposed documents [for] trial exhibits, and the failure to do so results in a waiver."[165]

Consequently, upon notice of litigation, the parties must automatically disclose "a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses."[166] Courts have interpreted this disclosure requirement to mean that the parties have an affirmative duty to search their records in good faith for relevant e-documents.[167] This duty is "heightened in this age of electronic discovery when attorneys [and their clients] may not [be able to] physically touch and read every document within the client's custody and control."[168] Existing case law makes it clear that attorneys also have an affirmative duty to communicate to their clients that they must identify, disclose, and potentially make available all relevant ESI to the court.[169] Should a client decline to turn over relevant ESI, the *Qualcomm* court held that the attorneys involved risk having personal sanctions imposed.[170]

Rule 34 reinforces Rule 26's admonition for liberal discovery. Under Rule 34, a party may request any relevant ESI that is in the custody or

163. FED. R. CIV. P. 26(f).

164. FED. R. CIV. P. 26(a)(1)(C) (stating that this default rule may be modified by agreement or by court order). However, judicial involvement in the e-discovery process is discouraged. Under the new rules, "primary responsibility for conducting discovery is to continue to rest with the litigants," and motions for production are to be limited to situations were there is a dispute. Qualcomm Inc. v. Broadcom Corp., No. 05cv1958-B (BLM), 2008 U.S. Dist. LEXIS 911, at *30-31 (S.D. Cal. Jan. 7, 2008), *vacated in part*, 2008 U.S. Dist. LEXIS 16897 (S.D. Cal. Mar. 5, 2008) (citing FED. R. CIV. P. 26(g) advisory committee's notes (1983 Amendment)). To the extent there is a dispute, the parties are to file Form 35. *See* Carol René Brophy, Supreme Court Approves Rules Governing the Discovery of "Electronically Stored Information," Nossaman Litigation E-Alert Bulletin, http://www.envoynews.com/nossaman/e_article000636703.cfm (last visited Oct.4, 2008).

165. ESI EVIDENCE, *supra* note 19, at 2 (citing FED. R. CIV. P. 26(a)(3)).

166. FED. R. CIV. P. 26(a)(1)(A)(ii).

167. *See Qualcomm, Inc.*, 2008 U.S. Dist. LEXIS 911, at *31 (concluding that the production of 1.2 million pages of marginally relevant documents, while concealing 46,000 critically important pages does not constitute good faith); *see also* Treppel v. Biovail Corp., 233 F.R.D. 363, 374 (S.D.N.Y. 2006) (stating that a "diligent search" involves a "reasonably comprehensive search strategy").

168. *Qualcomm, Inc.*, 2008 U.S. Dist. LEXIS 911, at *30-31 (noting under the new rules, "primary responsibility for conducting discovery is to continue to rest with the litigants" (citing FED. R. CIV. P. 26(g) advisory committee's notes (1983 Amendment)).

169. *See Qualcomm, Inc.*, 2008 U.S. Dist. LEXIS 911, at *45; *see also* Zubulake v. UBS Warburg L.L.C., 229 F.R.D. 422, 432 (S.D.N.Y. 2004).

170. *See Qualcomm, Inc.*, 2008 U.S. Dist. LEXIS 911, at *45; *see also* Calhoun & Friedman, *supra* note 34.

control of the opposing party.[171] Conceptually, Rule 34 provides that the scope of e-discovery requested extends to any ESI, regardless of how it is stored.[172] However, while all relevant ESI must be disclosed, not all requested ESI must be produced.[173] Absent a court order, a party needs only to produce ESI as it exists in the "usual course of business."[174]

ESI production is further limited by the imposition of a cost-benefit analysis. Under Rule 26, "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issue at stake in the litigation, and the importance of the proposed discovery in resolving the issues," the courts must limit the frequency or extent of discovery.[175] The courts have already used Rule 26's cost-benefit analysis to limit ESI discovery. For example, Judge Grimm opined that "it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted."[176]

Rule 26's cost-benefit analysis sets the stage for the amended FRCP to create one of the two safe harbors for sheltering ESI from discovery. In addition to the safe harbor of privilege, ESI is not discoverable if its production would be overly burdensome.[177] Because parties must pay for their own discovery costs,[178] the "burden" contemplated by Rule 26's safe harbor refers to the degree a producing party's operations would be disrupted by the process of identifying and collecting ESI located in an off-site computer or in a legacy system (*i.e.*, in a computer system that is no longer in use).[179] The logistics of collecting ESI from either off-site

171. FED. R. CIV. P. 34(a)(1).

172. FED. R. CIV. P. 34(a)(1)(A).

173. FED. R. CIV. P. 34(b)(2).

174. FED. R. CIV. P. 34(b)(2)(E) ("If a request does not specify a form . . . a [responding] party must produce [the information] in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms . . . ."). *But see In re* Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., No. MD-05-1720(JG)(JO), 2007 WL 121426, at *4 (E.D.N.Y. Jan. 12, 2007) (noting that when a party chooses to produce a "reasonably usable form" of data that is ordinarily in an electronically searchable form, it should not produce it in a form that significantly reduces or removes the searching feature (citing FED. R. CIV. P. 34(b), advisory committee's notes (2006 Amendment))).

175. FED. R. CIV. P. 26(b)(2)(C). This rule is enforced during pretrial conferences. FED. R. CIV. P. 16(c)(2).

176. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007).

177. *See* FED. R. CIV. P. 26(b)(2)(B).

178. Cozen O'Connor, Electronic Discovery Disputes: E-Discovery Frequently Asked Questions, http://cozen.com/practice_area_detail.asp?d=1&paid=212&m=99&spid=60 (last visited Oct. 2, 2008).

179. *See* ELECTRONIC DISCOVERY BEST PRACTICES, *supra* note 150, at 5.

locations or legacy systems is potentially onerous because off-site computer data frequently is not systematically catalogued and IT personnel knowledgeable in the legacy system's software may not be readily available. Therefore, absent a good cause, ESI in an off-site or legacy system is presumptively non-discoverable.[180] This general rule is essentially a restatement of the rule that ESI production is limited to the format that exists in the ordinary course of business.[181]

When all businesses are considered, the off-site/legacy system rule creates a significant loophole for sheltering ESI from e-discovery. This loophole is large because many business organizations rarely store ESI in their active computer networks.[182] Accordingly, parties requesting production must become familiar with how their opponents archive their e-documents. Early in the discovery process, a party requesting document production should conduct interviews with the opposing party's employees and IT professionals to identify when, how, and where ESI is stored.[183] Requesting parties can then use this knowledge to specifically request which off-site and/or legacy systems are to be searched to minimize the burden of document production.

As a corollary, parties requesting production need a firm understanding of their opponent's e-document retention and destruction policy.[184] Knowledge of an opponent's ESI retention and destruction policy provides insight into what ESI is available in off-site/legacy systems. Moreover, such knowledge may become important if sanctions are imposed for non-production. Under the new rules, although e-documents destroyed in the ordinary course of business do not need to be produced,[185] document

180. *See* FED. R. CIV. P. 26(b)(2)(B); *see also* Phoenix Four, Inc. v. Strategic Res. Corp., No. 05 CIV. 4837 (HB), 2006 U.S. Dist. LEXIS 32211, at *19 (S.D.N.Y. May 23, 2006); Anthony Schoenberg, *New Discovery Rules: Avoid Costly Consequences by Understanding What the Amendments Allow and Require*, MONDAQ, June 28, 2007, http://www.mondaq.com/article.asp?articleid=49618.

181. *See* ELECTRONIC DISCOVERY BEST PRACTICES, *supra* note 150, at 6.

182. *See* John J. Coughlin, Electronic Discovery: Know What You Have Before Your Adversary Does, Duane Morris L.L.P. Alert (Mar. 6, 2007), http://www.duanemorris.com/alerts/alert2442.html.

183. *See* Treppel v. Biovail Corp., 233 F.R.D. 363, 373-74 (S.D.N.Y. 2006) (instructing a party to submit interrogatories to obtain basic information about its opponent's electronic document systems before conducting depositions).

184. In e-discovery, "saved" and "preserved" have different meanings. Data is "saved" when it is automatically updated. When data is "preserved," it and its metadata are fixed for all time. "Preservation," unlike saving an e-document, generally requires the assistance of an IT professional. *See* Coughlin, *supra* note 182.

185. FED. R. CIV. P. 37(e). Document destruction is essentially a form of off-site storage.

destruction that occurs outside of the policy may be grounds for the imposition of sanctions.[186]

The 2006 amendments to the FRCP heighten the risks associated with the operation of a record destruction policy.[187] Unlike a paper document destruction policy, where all documents older than a certain date are destroyed, e-document destruction policies are more complex due to the volume, diversity, and dispersion of ESI. Business organizations, for example, may want to retain the final version of contracts in a PDF file longer than the counterpart Word documents. Businesses also may wish to retain e-mail documents for a shorter amount of time than Word documents. Such selective e-document destruction policies add complexity to the process and carry with it a significant burden. Under the new rules, a party "must be able to account for [one-hundred percent] 100% of the data collected, including explanations of all assumptions used in de-duplicating, filtering, rendering, displaying and exporting the data."[188] This task becomes complicated when a business organization's ESI is hundreds of millions of pages and may exist in multiple formats and versions.[189]

ESI diversity also affects the ability to use privilege to shelter e-documents from discovery. Under the 2006 amendments, privileged e-documents are not discoverable.[190] When the legal literature discusses the topic of privilege during e-discovery, it is often in the context of how a lawyer's careless handling of metadata resulted in the waiver of the attorney-client privilege.[191] Less appreciated is the fact that ESI diversity frequently creates a false sense of privacy, and hence does not provide for the confidential communication necessary to create the attorney-client privilege. For example, in *Scott v. Beth Israel Hospital Medical Center, Inc.*, the court ruled that when a surgeon sent an e-mail from his employer's

186. *See e.g.*, FED. R. CIV. P. 37(f); *see* Broccoli v. Echostar Commc'ns, Corp., 229 F.R.D. 506, 510 (D. Md. 2005); *see also* Calhoun & Friedman, *supra* note 34.

187. *See* Jon Neiditz & Aimee Siliato, *What the E-Discovery Amendments to the Federal Rules of Civil Procedure Mean to You*, TDAN.COM, Feb. 1, 2007, http://www.tdan.com/view-special-features/5353.

188. Schwarz & Walden, *supra* note 150.

189. *See* Scheindlin, *supra* note 1, at No. 8. The volume of information in business is now so substantial that it is impairing productivity. *See generally* Matt Richtel, *Lost In E-mail, Tech Firms Face Self-Made Beast*, N.Y. TIMES, June 14, 2008, at A1, *available at* http://www.nytimes.com/2008/06/14/technology/14email.html.

190. FED. R. CIV. P. 26(b)(1).

191. *See* Elliot Paul Anderson, *What Lies Beneath: Native Format Production and Discovery of Metadata in Federal Court*, 78 OKLA. B.J. 999, 999 (2007), *available at* http://www.okbar.org/obj/articles07/041407anderson.htm (observing that it is difficult, if not impossible, to redact the metadata from a native document); *see also* Williams v. Sprint/United Mgmt. Co., No. 03-2200-JWL, 2007 WL 38397, at *5 (D. Kan. Jan. 5, 2007) (finding that an attorney's voluntary and intentional disclosure of metadata is a waiver of privilege).

computer to his attorney, attorney-client privilege was waived.[192] The precise reason for the waiver was that the hospital where Dr. Scott was employed had a policy stating that employees had no privacy expectations for e-mails sent over the hospital's computer system.[193] A confidential communication between the doctor and his attorney did not occur.[194]

ESI diversity, which often obscures the relationship of one computer program to another, can negatively affect confidential communications in other ways. Consider the collateral consequences of using an application program for social networking (*e.g.,* Myspace.com or Facebook.com). During the registration phase of a social networking program, the program's developer often requires the user to grant access to all personal information that is placed on that site.[195] After the program is installed, any material that passes through this website may no longer be considered confidential because of the grant of information access that was given to the site owner. Accordingly, social network websites may be able to sufficiently destroy any notion of a confidential communication. Similarly, after *Scott*, it is possible that either the presence of spyware or a Trojan horse program on an attorney's or a client's computer may be sufficient to destroy the confidentiality of any electronic communication sent from that computer.[196] This is a particularly frightening situation because the computer user is often unaware that these programs transmit personal and/or confidential information.

While the 2006 amendments to the FRCP make it clear that privileged information is sheltered from production, the amended FRCP does not create any new privileges.[197] What is new, however, is the creation of a clawback provision. Similar to the Sedona Conference's clawback

192. Scott v. Beth Israel Med. Ctr., Inc., 847 N.Y.S.2d 436, 440 (N.Y. Sup. Ct. 2007). *But see* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 910 (9th Cir. 2008) (holding that the Fourth Amendment and state constitutional privacy rights protected employees' text message content).

193. *Scott*, 847 N.Y.S.2d at 440.

194. *Id.*

195. See Martha Irvine, *Social Networking Applications Can Pose Security Risks*, Pantagraph.com, Apr. 27, 2008, http://www.pantagraph.com/articles/2008/04/27/news/doc48120a3d97c75432641888.txt (noting that an application program on Facebook can only be "downloaded if a user checks a box allowing its developers to 'know who I am and access my information'").

196. *See* Merriam-Webster Online, Spyware, http://www.merriam-webster.com/dictionary/spyware; *see also* Mark. G. Milone, *Hacktivism: Securing the National Infrastructure*, 58 BUS. LAW. 383 n.21 (2002). Spyware and Trojan horse programs differ in the degree to which they send information from the user's computer to remote locations. Spyware sends only limited information, such those websites to which the computer has been logged in, to a remote location. A good Trojan horse program will literally send every key stroke entered into the computer to a remote location.

197. FED. R. CIV. P. 26(b)(1).

procedure, the amended rules have created a clawback procedure for handling the inadvertent release of privileged ESI.[198] Under the new rules, when a party recognizes that an e-document may be subject to a claim of privilege, that party must: (1) destroy, return, or sequester the material or (2) present the material to the court for a ruling on the privilege.[199]

Interestingly, the American Bar Association (ABA) rules set a lower ethical standard for handling the inadvertent release of privileged ESI. According to the new ABA rules, when an attorney recognizes that he or she has received ESI that may be subject to a claim of privilege, the attorney need only notify the producing parties.[200] Similar to the FRCP's clawback provision, the ABA's new ethics rules do not prohibit attorneys who have received ESI that may be subject to a claim of privilege from reading and profiting from the e-document.[201] Nor do the ABA rules require attorneys to abstain from mining metadata within the e-document.[202] To the contrary, one could argue that if an attorney receives privileged ESI from an opponent, he or she should read the document and *mine the metadata* to represent his or her client with zeal.[203]

C. Sanctions and E-Discovery

Finally, the amended FRCP creates sanctions for non-compliance with the new e-discovery rules. When relevant ESI is not produced, the courts have been granted wide discretion to determine whether the non-production is justified.[204] If the non-production is unjustified, the courts may impose sanctions on the non-compliant party.[205] When sanctions are imposed, courts are to consider whether a motion to produce the ESI was filed[206] and the harm done during the discovery process due to non-production.[207]

198. *See* Schoenberg, *supra* note 180.

199. FED. R. CIV. P. 26(b)(5)(B); *see also* Schoenberg, *supra* note 180.

200. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006).

201. *Id.*

202. Poluka & Paz, *supra* note 118.

203. ABA MODEL RULES OF PROF'L CONDUCT R. 1.3 cmt. 1 (2002) ("A lawyer must also act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf.").

204. FED. R. CIV. P. 37(a)(3)(A) ("If a party fails to make a disclosure required by Rule 26(a), any other party may move to compel disclosure and for appropriate sanctions."); *see* Qualcomm Inc. v. Broadcom Corp., No. 05cv1958-B (BLM), 2008 U.S. Dist. LEXIS 911, at *28-31 (S.D. Cal. Jan. 7, 2008), *vacated in part*, 2008 U.S. Dist. LEXIS 16897 (S.D. Cal. Mar. 5, 2008) (discussing the requirement for a formal motion for document production in order to obtain sanctions against individual attorneys for failing to produce ESI, which demonstrated that the attorneys were obligated to produce specific ESI and by withholding the ESI, the attorneys acted with requisite culpable intent).

205. *See* FED. R. CIV. P. 37(e).

206. *See Qualcomm Inc.*, 2008 U.S. Dist. LEXIS 911, at *29.

207. *See* Chambers v. NASCO, Inc., 501 U.S. 32, 55 (1991); *see also* FED. R. CIV. P.

Accordingly, an e-document of minor relevance that is "lost as a result of the routine, good-faith operation of an electronic information system" may not result in the imposition of sanctions.[208] On the other hand, even the venial loss of ESI may result in the imposition of significant sanctions in order to deter the parties from engaging in spoliation.[209] Sanctions also place the "risk of an erroneous judgment on the party who wrongfully created the risk" or restore "the prejudiced party to the position it would have been in had the misconduct not occurred."[210]

More generally, the sanctions available under the amended FRCP are designed to limit spoilage of ESI. Spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."[211] Because parties to litigation must be able to account for, and therefore potentially produce, one-hundred percent of relevant ESI, spoilage is expected to be a greater problem in the electronic era than it was when all documents were paper.[212]

Consequently, the framers of the amended FRCP have created significant sanctions to deter spoilage.[213] Sanctions to deter spoilage are appropriately imposed when: (1) the party with custody or control of an e-document has an obligation to produce that document; (2) the concealed information was "relevant" to the requesting party's claim or defense; and (3) the party had a "culpable state of mind" at the time of non-production of an e-document.[214] Demonstration of a "culpable state of mind" does not require a "smoking gun memo," rather a party may demonstrate a "culpable state of mind" during e-discovery by a party's pattern of non-cooperation with production requests.[215]

26(g)(3).

208. FED. R. CIV. P. 37(e).

209. *See* Phoenix Four, Inc. v. Strategic Res. Corp., No. 05 CIV. 4837 (HB), 2006 U.S. Dist. LEXIS 32211, at *10 (S.D.N.Y. May 23, 2006).

210. *Id.* at *11 (citing West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999)); *see also* FED. R. CIV. P. 37(c)(1).

211. *West*, 167 F.3d at 779 (citing BLACK'S LAW DICTIONARY 1401 (6th ed. 1990)).

212. *See* Schwarz & Walden, *supra* note 150 ("[P]roducing parties must be able to account for [one-hundred percent] of the data collected, including explanations of all assumptions used in de-duplicating, filtering, rendering, displaying and exporting data.").

213. *See* Schoenberg, *supra* note 180 (noting the size of this verdict was in part due to Morgan Stanley's destruction of evidence after it received notice of litigation); *see also* Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., No. CA 03-5045 AI, 2005 EXTRA LEXIS 94, at *30-31 (Fla. Palm Beach County Ct. Mar. 23, 2005), *rev'd*, 955 So.2d 1124 (Fla. Dist. Ct. App. 2007) (reversing the compensatory and punitive damages awards).

214. *Phoenix Four, Inc.*, 2006 U.S. Dist. LEXIS 32211, at *11-12 (citing Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107 (2d Cir. 2002); Zubulake v. UBS Warburg L.L.C., 220 F.R.D. 212, 220 (S.D.N.Y. 2003) (*Zubulake IV*)).

215. *See* Treppel v. Biovail Corp., 233 F.R.D. 363, 371-72 (S.D.N.Y. 2006) (stating that culpability is "often met by demonstrating that the opposing party has lost or destroyed

To avoid sanctions for ESI spoilage, a party should create a litigation hold to preserve relevant ESI as soon as notice of impending litigation is received.[216] Once a party receives a notice of litigation, the party "must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."[217] A litigation hold is created by three affirmative actions: (1) identifying and preserving relevant information; (2) issuing a written notice clearly defining the ESI to be preserved; and (3) compliance monitoring.[218] If these steps are followed properly, the litigation hold appropriately preserves the relevant ESI as it exists in the "ordinary course of business," which is the standard by which the courts measure the quality of preservation.[219] As a corollary, documentation of the steps followed to create the litigation hold will help to establish a chain of custody and control that may be needed for authentication of the ESI.[220]

Unlike traditional litigation holds, ESI litigation holds should not be created in a perfunctory manner. Depending on the complexity of the computer network, a certain degree of due diligence must be used to affirmatively search and catalogue relevant ESI in both the current memory

---

evidence in the past or has inadequate retention procedures in place" (citing Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 138 (2004)); *see also* Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 437 (W.D. Pa.2004) ("Had there been evidence of attempted damage or destruction of the report or the data compilations used to produce it, the Court's level of concern for the protection of the integrity and existence of the evidence would be different.").

216. *See Treppel*, 233 F.R.D. at 371 (citing Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998)); *Zubulake IV*, 220 F.R.D. at 216 (citing Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001)); *see also* Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1987).

217. ELECTRONIC DISCOVERY BEST PRACTICES, *supra* note 150, at 8.

218. Scheindlin, *supra* note 1, at No. 3.

219. *See Zubulake IV*, 220 F.R.D. at 216 ("Identifying the boundaries of the duty to preserve involves two related inquiries: *when* does the duty to preserve attach, and *what* evidence must be preserved?"); *see also* Linnen v A.H. Robins Co., No. 97-2307, 1999 Mass. Super. LEXIS 240, at *3, 29-30 (Super. Ct. Mass. June 16, 1999); Procter & Gamble Co. v. Haugen, 179 F.R.D. 622, 631-32 (D. Utah 1998); *In re* Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 615 (D.N.J. 1997); Applied Telematics, Inc. v. Sprint Commc'ns Co., No. 94-4603, 1996 U.S. Dist. LEXIS 14053, at *8-11 (E.D. Pa. Sept. 18, 1996).

220. *See* Schwarz & Walden, *supra* note 150; THE SEDONA CONFERENCE WORKING GROUP ON BEST PRACTICES FOR ELEC. DOCUMENT RETENTION & PROD., THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE 80 (Charles R. Ragan et al. eds., 2005), http://www.thesedonaconference.org/content/miscFiles/TSG9_05.pdf ("Metadata allows organizations to track the many layers of rights and reproduction information that exist for records and their multiple versions. Metadata may also document other legal or security requirements that have been imposed on records; for example, privacy concerns, privileged communications or work product, or proprietary interests.").

and in off-site or legacy systems.[221] When a client fails to exercise the necessary degree of due diligence to search for relevant ESI, the courts have used FRCP Rule 37's authority to impose sanctions for both negligent searches[222] and willful non-compliance with the discovery process.[223] These sanctions even have included orders authorizing the opponent's computer expert to search the non-producing party's computers when the courts have concluded that a party's non-production was unjustified.[224]

In extreme cases, sanctions for violations of the new e-discovery rules have been imposed personally on attorneys.[225] In *Qualcomm*, a well-known telephone manufacturer asserted that it had turned over all of the relevant ESI.[226] The falsity of this statement was revealed during the trial when a Qualcomm witness testified to the existence of previously undisclosed e-mail documents.[227] Subsequently, the court discovered that both in-house and outside attorneys had been complacent with their client's non-disclosure of ESI, a specific violation of the amended FRCP rules.[228]

---

221. *See* Qualcomm Inc. v. Broadcom Corp., No. 05cv1958-B (BLM), 2008 U.S. Dist. LEXIS 911, at *31, 36-38, 71 (S.D. Cal. Jan. 7, 2008) *vacated in part*, 2008 U.S. Dist. LEXIS 16897 (S.D. Cal. Mar. 5, 2008).

222. *See, e.g.*, Phoenix Four, Inc. v. Strategic Res. Corp., No. 05 CIV. 4837 (HB), 2006 U.S. Dist. LEXIS 32211, at *10, 12, 14-15 (S.D.N.Y. May 22, 2006) (ordering sanctions when the producing party failed to search a server and several password protected accounts for relevant evidence).

223. *See, e.g.*, *Qualcomm Inc.*, 2008 U.S. Dist. LEXIS 911, at *23, 31.

224. *See, e.g.*, Balboa Threadworks, Inc. v. Stucky, No. 05-1157-JTM-DWB, 2006 U.S. Dist. LEXIS 29265, at *12 (D. Kan. Mar. 24, 2006); Toledo Fair Hous. Ctr. v. Nationwide Mut. Ins. Co., 703 N.E.2d 340, 354 (Ct. Com. Pl. Ohio 1996) ("[Defendants] will not be permitted to frustrate discovery of relevant material because the method it has chosen to store documents makes it burdensome to retrieve them."); *In re* Brand Name Prescription Drugs Antitrust Litig., No. 94 C 897, MDL 997, 1995 U.S. Dist. LEXIS 8281, at *6-8 (N.D. Ill. June 15, 1995) (holding that the plaintiff does not have to pay for the cost of e-discovery when the defendant's software has limited search capabilities); Playboy Enters. Inc. v. Welles, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999). *But see* Advante Int'l Corp. v. Mintel Learning Tech., No. C 05-01022 JW (RS), 2006 U.S. Dist. LEXIS 45859, at *4-5 (N.D. Cal. June 29, 2006) (holding where legitimate privacy or privilege concerns exist, plaintiffs' experts should be denied access to defendants' ESI).

225. *Qualcomm Inc.*, 2008 U.S. Dist. LEXIS 911, at *45, 64. While there does not appear to be any legal malpractice cases concerning ESI production, it is not hard to imagine a party bringing such a case after losing or having sanctions imposed on it, which alleges that the attorney of record failed to provide proper instructions concerning the production of ESI and metadata.

226. *Id.* at *28-29.

227. *Id.* at * 3.

228. *Id.* at *45-60. FED. R. CIV. P. 26(g)(1) ("[E]very discovery request, response or objection must be signed by at least one attorney . . . [which] certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry: (A) with respect to a disclosure, it is complete and correct as of the time it was made; and (B) with respect to a discovery request, response, or objection, it is: (i) consistent with these rules and warranted by existing law . . . (ii) not interposed for improper purpose . . . and (iii) neither unreasonable nor unduly burdensome or expensive . . .").

Accordingly, Qualcomm's attorneys were referred to the state bar for disciplinary proceedings.[229]

D. Epilogue on E-Discovery and EMRs

This overview of the 2006 amendments to the FRCP demonstrates that e-discovery is a more complex procedure than traditional discovery. This complexity likely will translate into the need for attorneys to retain both an IT specialist to determine where any relevant ESI may be stored and a search strategy expert to facilitate document identification and review. In litigation where voluminous ESI is produced, (*e.g.*, in a class-action proceeding), identifying documents, reviewing documents, and maintaining chain of custody documentation can easily become burdensome. Thus, it is not surprising to find commentators, like the Sedona Conference and others, taking a conservative position on the scope of e-discovery. For example, several courts have ruled that metadata is to be produced only when it is "material and necessary" to a claim or defense.[230]

On the other hand, regardless of whether the physician is a defendant in a medical malpractice action or a respondent before a BOME, the amount of ESI at issue would likely be limited to the EMR of a single patient, or perhaps the EMRs of a few patients.[231] Thus, the amount of documents subject to e-discovery may not be significantly larger than the amount of documents subjected to traditional paper discovery. In litigation involving the professional services of physicians, there is virtually always a medical record available for review. The reason for the ubiquitous medical record, whether paper or electronic, is that physicians may be disciplined for failing to adequately document the care they have given.[232] However, the quality of medical records that is kept by physicians is varied.[233]

---

229. *Qualcomm Inc.*, 2008 U.S. Dist. LEXIS 911, at *64 (re-evaluating sanctions against the outside counsel because they were not allowed to pierce the attorney-client privilege to defend themselves).

230. *See* Mark A. Berman, *New York State E-Discovery Law: Scope Limits on E-Discovery Under Recent State Decisions*, N.Y.L.J., Oct. 29, 2007, at 3, *available at* http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1193735030065#12 (discussing cases that involve expansive discovery requests but not e-document integrity concerns as in Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005)).

231. *See* PUB. CITIZEN'S CONG. WATCH, MEDICAL MISDIAGNOSIS IN TEXAS: CHALLENGING THE MEDICAL MALPRACTICE CLAIMS OF THE DOCTOR'S LOBBY 8 (2003), *available at* http://www.citizen.org/documents/Texas%20Report.pdf (explaining that only 6.5% of physicians have made multiple payments to settle medical malpractice actions).

232. *See, e.g.*, CAL. BUS. & PROF. CODE § 2266 (West 2003) ("The failure of a physician and surgeon to maintain adequate and accurate records relating to the provision of services to their patients constitutes unprofessional conduct.").

233. *See* PATRICIA DAEHNKE, BONNE BRIDGES, P.C., THE MEDICAL RECORD AS EVIDENCE: HOW WILL YOUR CHART LOOK TO A JURY? (2007), *available at* http://www.bonnebridges.com/pdf/November_07_News_brief.pdf.

Moreover, paper and electronic medical records must be stored for a variable number of years, depending on nature of the record (*e.g.* actual records, pathologic slides, or radiographic images). These archived files may be stored off-site or in a legacy system (*e.g.* microfiche), but as a general rule, a patient's medical records are retrievable within twenty-four hours. As the EMR must be readily available in a patient emergency, e-discovery in healthcare litigation is unlikely to involve issues of off-site or legacy system storage. Finally, because the amended FRCP does not create any new privileges, privilege barriers in healthcare e-discovery may not be significantly greater than in traditional discovery. Because patients have access to their own medical records, these e-documents are not confidential communications between providers.[234] Absent confidentiality, it is hard to imagine that an EMR contains privileged information. Further, specific EMR metadata information is unlikely to be confidential because system metadata is not a statement and application metadata is hearsay. Accordingly, the scope of EMR discovery likely will be at least as broad as the scope of PMR discovery. The real question in healthcare litigation will be whether a party must produce the EMR with its metadata as a native file, or whether the courts will accept an EMR image file.

Since the cost of the attorney's time most significantly impacts the overall cost of e-discovery, the production of an EMR native file is unlikely to have a negative impact on the cost of litigation.[235] After all, it usually does not take an attorney much longer to review an e-document that contains "track change" annotations than it does to review a clean copy of the same document. Nor is it likely, as some commentators have implied, that the routine production of EMR system metadata would raise substantial issues of privilege.[236]

If EMR system metadata automatically is created during the routine course of business, it may be invaluable for authentication and as a way to provide documentation of a chain of custody of an EMR.[237] It is not likely that EMR application metadata will contain privileged information. To the extent that EMR metadata application may contain privileged information, one party in healthcare litigation always will raise the argument that e-discovery of the actual care given by a doctor outweighs the disclosure of

234. *See, e.g.*, U.S. Department of Veterans Affairs, MyHealtheVet, http://www.myhealth.va.gov/ (last visited Jan. 26, 2009) (providing online access to healthcare information).

235. *See* LEXISNEXIS APPLIED DISCOVERY, THE TRUTH ABOUT NATIVE FILE REVIEW 4-5 (2006), https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_WP_TruthAboutNativeFileReview.pdf (explaining that the cost to preserve ESI as a native or image file is negligible).

236. *See, e.g.*, Anderson, *supra* note 191, at 1000.

237. *See supra* Part II.

privileged information. Indeed, the next section demonstrates how EMR application metadata can be a deciding factor in the outcome of healthcare litigation.

IV. APPLICATION OF E-DISCOVERY LAWS TO EMRS AND EMR METADATA

A. EMR Metadata Discovery

As an electronic analogue to the traditional PMR, an EMR is an electronic writing within the meaning of FRCP 34(a)(1)(A).[238] Under Rule 34(b), a party may request ESI production in its native format, *i.e.*, as it is used in the ordinary course of business.[239] Metadata is part of the functioning of an EMR during the ordinary course of business. Accordingly, if a physician wishes to avoid sanctions for spoilage in the future, the physician should store a copy of the EMR complete with metadata.[240] This does mean that a native copy of the EMR should automatically be produced.[241] The purpose of a Rule 26 conference is to make automatic disclosures and to discuss the format for producing the EMR. At this conference, parties should only offer an image file of the EMR, as *Williams* and other cases teach that, absent a court order, EMR metadata does not need to be produced.[242] More accurately, EMR metadata simply needs to be available for the courts to review.[243] Alternatively, if it is known that the EMR metadata only contains information that is exculpatory from the physician's point of view at the Rule 26 conference, the physician's attorney should consider offering the EMR as a native file.[244]

Hypothetically, both parties may agree at the beginning of discovery that an image file of the EMR will be sufficient. Such a situation may arise where the parties do not dispute the authenticity of the EMR and anticipate admitting the medical record into evidence under the Business Records Exception (BRE) to the rule on hearsay,[245] just as a traditional PMR would be admitted. Subsequent discovery could raise questions concerning the integrity of the EMR. For example, discovery that yields two image-file

238. FED. R. CIV. P. 34(a)(1)(A) ("any designated documents or electronically stored information – including writings . . . stored in any medium from which information can be obtained . . .").

239. FED. R. CIV. P. 34(b).

240. FED. R. CIV. P. 26(a)(1)(A)(ii).

241. *See* Kevin F. Brady, *Should Metadata Automatically Be Produced?*, 2 CGOC REV. 5, 5-6 (2006), *available at* http://www.pss-systems.com/resources/Brady_Metadata.pdf.

242. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 654 (D. Kan. 2005).

243. *See* Brady, *supra* note 241.

244. FED. R. CIV. P. 26(f).

245. FED. R. EVID. 803(6).

versions of the EMR with different hash values raises questions of corruption in the EMR.[246] Non-identical hash values in an EMR could indicate that one version of the EMR was read by one more person than the other or that a superuser[247] imperceptibly has altered the record.[248] Since issues concerning the integrity of EMR may only arise late in the discovery process, the physician ideally will have preserved a native version of the EMR.[249]

As the courts become more comfortable with metadata in healthcare litigation, they may routinely order that EMRs be produced with metadata. There are two reasons for adopting such a policy. First, late in the discovery process, disputes over authenticity and/or creditability[250] are likely to become increasingly common. Second, the courts will tire of hearing production motions late in the discovery process. To understand why authenticity disputes will arise in close proximity to the time of a trial, it is useful to compare how a PMR and an EMR are admitted into evidence.

A PMR is admitted into evidence under the BRE when a medical records custodian (MRC) testifies that the medical record has been in his or her custody and control[251] and has not been altered.[252] Once a MRC provides

246. This may commonly occur in traditional healthcare discovery. After an adverse event, the patient or patient's family will frequently obtain a copy of the medical record at discharge, and this record will not be identical to the medical record provided to the plaintiff's attorney after filing a medical malpractice action.

247. Indiana University, Superuser, http://www.ussg.iu.edu/usail/concepts/superuser.html (last visited Oct. 28, 2008) ("The superuser is a privileged user [or network administrator] who has unrestricted access to the whole system; all commands and all files regardless of their permissions.").

248. When an EMR is altered, no evidence will be visible to the layman because hash values and metadata are not normally visible. *See* SIMSON L. GARFINKEL, PROVIDING CRYPTOGRAPHIC SECURITY AND EVIDENTIARY CHAIN-OF-CUSTODY WITH THE ADVANCED FORENSIC FORMAT, LIBRARY, AND TOOLS 1 (2008), http://www.afflib.org/downloads_files/affcrypto.pdf (discussing the forensic uses of hash values and metadata).

249. In situations where the authenticity of a business record is an issue, some courts may admit the record and allow the record's authenticity to be considered under the weight of the evidence. *See* Erin E. Kenneally, *Gatekeeping Out of the Box: Open Source Software as a Mechanism to Assess Reliability for Digital Evidence*, 6 VA. J.L. & TECH. 13 n.50 (2001), http://www.vjolt.net/vol6/issue3/v6i3-a13-Kenneally.html#_ednref52.

250. Even when authentication is not an issue, courts will likely order metadata production where the credibility of factual testimony is dispositive. For example, when a physician testifies that he or she reviewed an x-ray, the EMR metadata may be admitted to show the particular radiographic examination lacks the physician's electronic finger print. *See supra* note 73.

251. Other elements of the BRE, a business record made at the time of the event by someone with personal knowledge, are usually not at issue in healthcare litigation.

252. *See* KENT SINCLAIR, TRIAL HANDBOOK CA-611 (Practicing Law Inst. 3d ed. 2002 & Supp. 2008) ("Evidence must be shown to have suffered no material alteration after coming into custody of the proponent, though the rule does not expressly state this requirement (citing United States v. Collado, 957 F.2d 38 (1st Cir. 1992)); *cf.* First Union Nat'l Bank v. Woermer, 887 A.2d 893, 901-02 (Conn. App. Ct. 2005) (indicating that chain

such testimony, the actual PMR used by the physician(s) is entered into evidence. After that point, the fact finder in healthcare litigation can inspect the document. Having access to the tangible document allows the fact finder to identify alterations rather easily because erasure marks, different color ink, missing or extra pages in certain versions, and other changes are readily apparent in a PMR. Indeed, the reason why a BRE foundation has worked well for admitting the PMR into evidence is that a fact finder could personally test the document for its veracity by inspection.

On the other hand, admitting an EMR record into evidence is more complex. First, the testimony of the MRC does not readily allow the EMR to be admitted. It would be difficult for a MRC to testify truthfully that an intangible EMR, which is circulating in a computer system, was in his or her custody and control. A CD-ROM image file version of the EMR could have been preserved to allow the MRC to testify that version of the medical record was in his or her custody and control. However, as already discussed, such testimony comes with its own set of problems. For example, a MRC must also testify, "that the record that has been retrieved from the file, be it paper or electronic, is the same as the record that was originally placed into the file."[253] Making such a statement is not easy in an electronic world because even companies with sophisticated IT departments cannot always prove the truth of such a statement.[254] The reality of CD-ROM image file versions of the EMR is that, absent the metadata, proving that the copy is true and accurate can be extremely difficult. This is the reason why some courts require elaborate foundations before admitting an e-document.[255]

If an adequate foundation is established and an image file EMR is admitted into evidence without its metadata, the fact finder would have no way of knowing whether the EMR had been altered. This is because an

---

of custody testimony is not mandatory for the admittance of a record under the BRE).

253. Am. Express Travel Related Servs. Co. v. Vinhnee (*In re* Vinhnee), 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005) (citing FED. R. EVID. 901(a)).

254. *See, e.g.*, Jerold S. Solovy & Robert L. Byman, *Don't Let Your E-Evidence Get Trashed*, NAT'L L.J., June 4, 2007, 13, *available at* http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1181293533711.

255. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 557-59 (D. Md. 2007); *see also In re Vinhnee*, 336 B.R. at 447-49 (refusing to admit ESI that did not satisfy the eleven-step process outline by Imwinkelried); IMWINKELRIED, EVIDENTIARY FOUNDATIONS, *supra* note 151. An Imwinkelried foundation requires the MRC to testify that: (1) the business uses a computer, which is (2) reliable (3) because the business developed procedures for data input, (4) error detection, and (5) maintained the system in good working order. *Id.* The MRC must also testify that (6) he or she directed the computer to print out the desired material (7) by using proper procedures, (8) and that the computer was functioning properly. *Id.* After the MRC (9) explains how he or she recognizes the exhibit as the printout, the MRC must (10) explain how he or she recognizes the printout and (11) translate any strange symbols. *Id.*

image file is, in essence, a "finished product" devoid of erasure marks, lineouts, and multi-colored ink. Screening such a document with hash values would be of little help to identify alterations, as hash values provide only an indication that one e-document has been altered relative to another version of that document. Simply, hash values alone cannot identify which copy has the alteration and which copy is the original. Instead, if a fact finder wants to see erasure marks, lineouts, and multi-colored ink, then the fact finder will need the EMR's metadata.

As a result, even if an EMR is authenticated without metadata, an image file EMR always would have a credibility issue. Accordingly, courts involved in healthcare litigation may order the production of EMR metadata liberally, if not routinely. If a disagreement arises regarding EMR metadata production, the parties likely will contest how much metadata should be produced for litigation. Attorneys for physician-defendants might credibly argue that while an opponent may be entitled to some of the metadata in the defendant's notes, the application metadata attached to all the other physician's notes is irrelevant, and therefore not subject to discovery.[256] Similarly, defense attorneys may argue that while an opponent may be entitled to the EMR system metadata, the opponent is not entitled to EMR application metadata for the doctor's note, because the image-file EMR note is the final expression of the doctor's thoughts and opinions. The particular facts of a case may determine whether either or both of these arguments win.

The idea of courts liberally ordering the production of EMR metadata may surprise many defense attorneys. Many healthcare attorneys create litigation holds by preserving only CD-ROM EMR image files, and they make no attempt to preserve the underlying metadata.[257] Accordingly, many healthcare providers may soon find themselves in a situation similar to the defendant in the *Williams* case.[258] In *Williams*, the defendant only was willing to produce an image file of the Microsoft Excel spreadsheet, thereby making it impossible to determine how certain calculations were made.[259] After the defendant "failed to show cause why it should not produce the electronic spreadsheets in the manner in which they were

256. *See* FED. R. CIV. P. 26(b)(1); *see also* FED. R. CIV. P. 16(c)(2)(D).

257. Personal knowledge of author based on conversations with several hospital attorneys.

258. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 642-45 (D. Kan. 2005). The key difference between this hypothetical and *Williams* is that the defendant in *Williams* apparently still had access to the native documents and metadata. *Id.*

259. The credibility, and not the authentication, of the spreadsheet was at issue. *Id.* at 643-44. This is a common situation in healthcare litigation.

maintained," complete with metadata, the court ordered the production of a native version of the Excel spreadsheet.[260]

Accordingly, because healthcare providers do not routinely preserve EMR metadata, these providers accrue potential sanction liability.[261] The factors for applying sanctions against a healthcare provider for the non-production of metadata include: (1) whether a motion to produce was filed;[262] (2) whether the non-production of the EMR metadata was justified;[263] and (3) the harm done during discovery due to non-production[264] or spoilage.[265] Of these factors, non-justification of EMR metadata non-production should cause healthcare attorneys the most concern. Since it has been two years since the implementation of the new e-discovery rules, courts probably will not allow attorneys to justify EMR metadata non-production based on a lack of knowledge. Instead, limited system capacity to store metadata constitutes a better justification since relevant metadata may have been deleted by the time the parties were put on notice of litigation.

A more prudent litigation-hold strategy would be to preserve both an EMR image and a native file.[266] At the Rule 26 conference, attorneys representing physicians would offer only the EMR image file. A healthcare defense attorney should take the position that an image file of the EMR is how a patient's medical record appears to the doctor in the normal course of business.[267] Therefore, only an image version of the EMR needs to be disclosed. If the opponent does obtain an order for some or all of the EMR's metadata, the defense attorney will not need to fear sanctions

260. The court did allow certain information with its metadata to be redacted. *Id.* at 656.

261. *See* FED R. CIV. P. 37(b).

262. FED R. CIV. P. 37(a)(3).

263. FED. R. CIV. P. 37(c)(1); *see* Qualcomm Inc. v. Broadcom Corp., No. 05cv1958-B (BLM), 2008 U.S. Dist. LEXIS 911, at *29 (S.D. Cal. Jan. 7, 2008) *vacated in part*, 2008 U.S. Dist. LEXIS 16897 (S.D. Cal. Mar. 5, 2008). An independent legal issue that goes to whether non-production of EMR metadata is produced concerns the capacity of a party's computer system to store metadata. *See supra* Part II. However, a detailed discussion over how much and for how long EMR metadata should be stored is beyond the scope of this article.

264. *See* FED. R. CIV. P. 26(g)(3); *see also* Chambers v. NASCO, Inc., 501 U.S. 32, 51 (1991).

265. *See* FED. R. CIV. P. 37(c)(1); West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999).

266. *In re* Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 91 (D. Conn. 2005).

267. *See* FED. R. CIV. P. 34(b)(2)(E) ("(ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms . . ."); *see also In re* Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., No. MD 05-1720 (JG)(JO), 2007 WL 121426, at *4 (E.D.N.Y. Jan. 12, 2007). However, a physician appearing before a BOME may not have a choice in the production format of an EMR. The BOME's subpoena may stipulate that the EMR be produced as a native document.

because the prepared attorney will be able to produce the native version of the EMR that is being held in reserve.

B. A View of EMR Reality

The majority of physicians probably are not technically capable of altering EMRs, nor do they have sufficient knowledge of commercially available software to be able to infiltrate an EMR system or corrupt its metadata. Moreover, EMR systems often have software safety features that prevent an EMR entry from being altered after it has been signed.[268] Therefore, if a MRC was to testify to these safeguards, the courts may not be so liberal in granting motions for EMR metadata production.[269]

Still, demand for EMR metadata will be high in situations where the documented care is at odds with the clinical outcome. All too often, physicians memorialize the care that they should have given, rather than the care that they actually gave. This characteristic of physicians' documentation helps to explain why medical records often read as if the physician did everything correctly, even though the patient died. EMR metadata changes the nature of a medical record because it allows inferences about the actual care given to a patient. Accordingly, even when a physician's note states that he or she reviewed a radiographic examination and the physician's metadata fingerprint is not linked to that radiograph, then the physician's creditability will be tarnished. Thus, EMR metadata is like an Orwellian Big Brother who silently records the actual care given to patients.

A few years ago, Feldman surveyed a large number of healthcare providers to determine what, if any, impact the EMR had on medical malpractice litigation.[270] Although Feldman had only about a fifty percent response rate to his surveys, he concluded that as an evidentiary vehicle, the EMR was no more detrimental to physicians' defenses than the PMR.[271] In 2006, a medical malpractice case shattered this view, by demonstrating how EMR metadata could be dispositive in litigation because it documented the actual care given rather than the care that should have been given.[272]

---

268. EMR entries are not unalterable though. Superusers have the power to delete documents and presumably to alter the text. While such acts are possible, they are unlikely. Moreover, these acts can be detected by examination of the metadata.

269. *See* IMWINKELRIED, *supra* note 151 (discussing the use of Imwinkelried's foundation).

270. Jeffrey M. Feldman, *Do Anesthesia Information Systems Increase Malpractice Exposure? Results of a Survey*, 99 ANESTH. ANALG. 840, 840 (2004).

271. *Id.* at 841-43.

272. Vigoda & Lubarsky, *supra* note 13, at 1799.

In this case, a fifty-eight-year-old patient underwent a seven-hour operation.[273] After the patient awoke as a quadriplegic, the competency of the surgeon was the initial focus of attention.[274] During the discovery phase of the ensuing lawsuit, the plaintiff obtained the patient's EMR complete with metadata.[275] The EMR metadata revealed that the anesthesiologist wrote a postoperative note minutes after the operation began asserting the procedure was uncomplicated, and the log of administered anesthetic gas contained a ninety-minute gap.[276] Subsequently, the anesthesiologist entered into a confidential out-of-court settlement.[277]

More generally, this case also serves to highlight the fact that both a PMR and an image file version of an EMR reflect only a certain point of view.[278] Even when not self-serving, the quality of documentation within a PMR or image file version of the EMR is frequently at issue. As evidence, a point of view is not determinative of the outcome of the case. Unfortunately, the evidentiary quality of a PMR or image file version of the EMR also is undermined since physicians feel encouraged to exaggerate and prevaricate in these unaudited business records.[279] For these reasons, it has been asserted that PMRs or image file version of the EMRs are merely uncorroborated hearsay.[280]

Because EMR metadata can be corrupted, it is not perfect evidence. Still, the courts are beginning to see that metadata is a useful tool to expose uncorroborated hearsay in business records. For example, in a recent case involving allegations that Maxim backdated its stock, Judge Chandler observed:

> For the following reasons, I grant plaintiffs' motion to compel. First, metadata may be especially relevant in a case such as this where the integrity of dates entered facially on documents authorizing the award of stock options is at the heart of the dispute. This relevance is further illustrated by the fact that Maxim's special committee, as well as Deloitte & Touche, undoubtedly reviewed metadata as part of their investigation

273. *Id.* at 1798.

274. *Id.* at 1798-99.

275. *Id.* at 1799-1801.

276. *Id.* at 1800-01.

277. *Id.* at 1802.

278. *See* Laura Gater, *The EHR on Trial: Is It a Legal Document?*, FOR THE REC., Sept. 12, 2005, at 14, 15, *available at* http://www.fortherecordmag.com/archives/ftr_091205p14.shtml.

279. In any other business record, prevarication should be discovered at the time of the next audit. In an unaudited medical record, a prevarication concerning the care that should have been given, rather than the care that was actually given, may never be detected. The possibility of an audit may make physicians more likely to be accurate and honest in their record keeping.

280. *See* Gater, *supra* note 278.

> into the backdating problems at Maxim. This latter fact also undermines the asserted burdensomeness of producing documents in native file format. Maxim need not produce metadata separately, but the Court does order the production of documents identified in plaintiffs' July 3rd motion to compel in a format that will permit review of metadata, as plaintiffs have clearly shown a particularized need for the native format of electronic documents with original metadata.[281]

Therefore, as more judges become aware of the power of metadata like Judge Chamber, attorneys should expect more orders for the production of metadata. In particular, out of fairness to patients and BOMEs, attorneys should anticipate more production orders for EMR metadata in healthcare litigation.

V. CONCLUSION

Experience in e-discovery has demonstrated that production of metadata can change the course of litigation. Given the volume and diversity of ESI stored within the walls of corporations, there is little question that some plaintiffs would abuse a liberal e-discovery process. Not surprisingly, corporate America ideally hopes to limit access to metadata.

However, the focus of this paper is considerably narrower. In healthcare litigation, the scope of e-discovery often is limited to the EMR of a single patient. It is hard to imagine that a healthcare provider could successfully argue that production of an EMR with its metadata is overly burdensome. Instead, the courts are likely to issue orders for the production of metadata to facilitate authentication and to resolve patients' issues and BOMEs' questions out of fairness. Recognizing the potential for metadata production, prudent physicians and their attorneys will preserve the relevant EMR with its metadata upon notice of impending litigation. However, because EMR metadata is not routinely available to physicians in the course of normal business, it should not be turned over to the opponent unless a court orders its production.

281. Ryan v. Gifford, No. 2213-CC, 2007 WL 4259557, at*1 (Del. Ch. Nov. 30, 2007).