Electronic Medical Records and E-Discovery: With New Technology Come New Challenges

by JEFFREY L. MASOR

Introduction ............................................................................................. 246
I. Challenges of E-Discovery of Electronic Medical Records............. 248
   A. Format ...................................................................................... 249
   B. Metadata ............................................................................... 252
      1. Audit Trail ........................................................................ 254
      2. Pop-up Warnings ............................................................ 255
      3. Preliminary Questions and Checkboxes that Make
         Up a Finalized Doctor’s Note ........................................ 256
   C. Discovery Rules – Tampering with Evidence? .................... 257
   D. Copy and Paste ..................................................................... 260

II. Embracing Electronic Discovery While Finding a Balance to
    Protect Both the Healthcare Provider’s and Requesting
    Party’s Interests ............................................................................ 262
   A. Proposal: Add/Modify a Provision to the Federal Rules
      of Civil Procedure .................................................................... 262
   B. Proposal: Develop a Way for Lawyers to Access
      Electronic Medical Records Digitally in a Manner that
      is Secure, Remote, and Limited to Only Necessary
      Information ............................................................................. 264
      1. Mandate Remote, Limited Access for Lawyers to
         Specific Patient Data in Electronic Medical Records .... 265
         a. Client-Server (Local) Electronic Medical Record
            Systems ........................................................................ 266
         b. Software as a Service (Cloud-Based) Electronic
            Medical Records ............................................................. 266
         c. Implementation ........................................................... 268
         d. Necessary Features ..................................................... 270
         e. Admissibility of Remote Access Electronic
            Medical Records as Evidence ...................................... 271

[245]
Introduction

When a case involving a patient reaches the discovery phase, the lawyer handling the case often requests all records pertaining to the patient's medical care.¹ Traditionally, healthcare providers organize patient information in paper form and catalogue the records on spacious shelves.² When a lawyer requests a patient’s paper medical records, the healthcare provider simply makes a photocopy of the binder containing the medical records and produces that copy to the requesting lawyer.³ However, there has been a recent trend toward adoption of electronic medical records.⁴ A 2011 survey by SK&A queried 237,562 U.S. medical providers and found that 40.4% of physician offices use electronic medical records.⁵

---

¹ I would like to thank Professor Sharona Hoffman and Ms. Stephanie Corley for their feedback and support while writing this piece.


Recovery and Reinvestment Act of 2009 also established funding through Medicare and Medicaid to subsidize healthcare providers switching to electronic medical records. As electronic medical records continue to be widely adopted across the United States, lawyers using those records have faced a number of new challenges.

In 2007, a patient filed a malpractice suit against Northshore University Health System and requested all records related to the patient’s treatment. However, the hospital had difficulty fulfilling the request. The electronic medical record system it was using had no print feature, so staff had to take screenshots of every page of the record from the computer. When printed to paper, this information filled four banker boxes and was difficult to interpret. The court then ordered the hospital to create a read-only electronic version of the records to be given to the plaintiff. This was a novel issue for the hospital. It had to work closely with the electronic medical records vendor to produce a digital copy of the records. Unfortunately, this did not solve all the electronic discovery problems, and the case continued for at least three more years.

This Note will explore issues that have arisen during electronic medical record discovery and will make two recommendations for how to solve them. Part I of this Note will discuss contemporary problems with the discovery of electronic medical records. First, printing an electronic medical record causes a number of difficulties; it requires a large amount of paper and creates a document fundamentally different from the original electronic version. Second, metadata, like audit trails and popup warnings, pose many unique challenges during electronic medical record discovery. Third,

6. Electronic Health Record Technology Incentive Program, 42 C.F.R. § 495.2(a) (2010); see also EHR Incentive Programs, CENTERS FOR MEDICARE & MEDICAID SERVICES, https://www.cms.gov/echrincentiveprograms/30_Meaningful_Use.asp (last visited Jan. 23, 2012). Medicare subsidies are only given if the adopted electronic medical record system conforms to “meaningful use” standards; Jha et al., supra note 5 at 1631.


8. Id.
9. Id.
10. Id.
11. Id.
12. Id.
evidence rules, like spoliation,\textsuperscript{14} have become an important question for constantly updated electronic medical records. Fourth, copying and pasting portions of the doctor’s note has become a pronounced issue since the introduction of electronic medical records, and this issue can potentially cause problems with patient care.

Part II of this Note will outline two potential solutions to these discovery challenges. One option allows lawyers to access portions of an electronic medical record remotely, using a special login that restricts access to only necessary information. This is the first law journal piece to explore the application of this approach to discovery of electronic medical records. Alternatively, medical care providers can export medical records to a common, standardized electronic format. Other authors have discussed this general approach, but this article goes into a unique, detailed analysis of how a complete, interoperable standard could be achieved.

I. Challenges of E-Discovery of Electronic Medical Records

In a legal setting, new and different challenges have arisen during the transition from paper medical records to electronic medical records. A major question that medical care providers face is how to produce a single patient’s electronic medical record to the lawyer. There are a number of challenges. First, the healthcare provider could run multiple electronic medical record systems within its facility for different departments or purposes.\textsuperscript{15} How does the healthcare provider produce an electronic medical record if each system displays different formats or includes different data? Second, how much metadata must be produced?\textsuperscript{16} For instance, warnings frequently pop up if a prescribed medication could interact negatively with another medication.\textsuperscript{17} Should that be produced as well? Third, how should the healthcare provider cope with the fact that discovery rules prohibit tampering with evidence,\textsuperscript{18} but the electronic medical record

\textsuperscript{14} See infra Part I.C.


\textsuperscript{16} See infra Part I.B.


\textsuperscript{18} See infra note 115.
changes over time as new patient information is added? Fourth, how should healthcare providers deal with copy and paste functionality in electronic medical records?

A. Format

The format of electronic medical records may differ based on the software system used and the specialty of the medical professional. First, the electronic medical record systems themselves are not standardized. There are over two hundred electronic medical record programs available; each designed specifically for medical care providers. Some popular programs include Centricity, EpicCare, Cerner PowerChart, and eClinicalWorks. The U.S. Department of Veterans Affairs has their own system, VistA, designed by the US government. Each system has a different user interface for accessing patient records.

Finally, even within healthcare systems, different departments and staff may use different versions of the same electronic medical record system customized for their field, or entirely different and independent systems altogether. For instance, the radiology department may use a separate electronic medical record system than the rest of the hospital. Furthermore, nurses may use a different electronic medical records interface than doctors, and medical information about the same patient may be displayed differently. In

22. Hudock, supra note 19.
25. History, WORLD VISTA, http://worldvista.org/AboutVistA/VistA_History (last visited Nov. 8, 2011). This system is distributed at no cost to any healthcare provider. Id.
27. See Hospital Information Systems (HIS), supra note 15.
28. Id.
addition, some healthcare providers use a mixed system of paper and electronic records, forcing them to look at different sources to create the complete record.\textsuperscript{30}

In light of these differences, how should electronic medical records be produced to the lawyer? Some healthcare providers produce records by using an automated printing function built into the software that prints out the record.\textsuperscript{31} However, only some systems have this built-in print feature.\textsuperscript{32} Of the systems that do have a built-in print feature, each may print the record differently.\textsuperscript{33} If the system does not have a built-in printing feature, healthcare providers often must make screenshots of every page of the electronic medical record.\textsuperscript{34} Screenshots entail manually saving a picture of each computer screen within the medical record.\textsuperscript{35} This requires displaying every part of the record and individually saving a picture of the contents on the screen, a tedious and unwieldy process that takes a great deal of time and resources.\textsuperscript{36} It is also often difficult for the lawyer to decipher; they are unwieldy and hard to organize and interpret.\textsuperscript{37} Furthermore, if different specialties or departments use different interfaces with their electronic medical records,\textsuperscript{38} from which interface does the healthcare provider take the screenshots?\textsuperscript{39}

\begin{itemize}
\item \textsuperscript{31} See Laura Hale Brockway, \textit{Potential pitfalls: risk management for the EMR}, TEX. MED. LIABILITY TR. (June 19, 2009), https://www.tmlt.org/newscenter/featured/article/214/Potential+pitfalls%3A+risk+management+for+the+EMR.
\item \textsuperscript{32} See Nowik, supra note 30.
\item \textsuperscript{33} Each electronic medical record system is different. See generally HUDOCK, supra note 19.
\item \textsuperscript{34} See Hudock, supra note 19; see also Dimick, supra note 7.
\item \textsuperscript{35} See Dimick, supra note 7.
\item \textsuperscript{36} Id.
\item \textsuperscript{37} Id.; see also Fred Trotter, \textit{EHR Can Make the Paper Problem Worse}, THE HEALTH CARE BLOG (June 17, 2011), http://thehealthcareblog.com/blog/2011/06/17/ehr-can-make-the-paper-problem-worse/ (printing out a patient paper record produces a large document that is difficult to decipher).
\item \textsuperscript{38} Hospital Information Systems (HIS), supra note 15.
\item \textsuperscript{39} See Hudock, supra note 19. The healthcare provider does not have to produce screenshots from every interface version. \textit{Id.}; FED. R. CIV. P. 34(b)(2)(E)(iii) (“A party need not produce the same electronically stored information in more than one form.”).
In general, printouts of computer data are admissible as evidence under the Federal Rules of Evidence. However, producing a static document in a different format than the computerized electronic medical record creates a number of problems for discovery. Primarily, the document being produced is fundamentally different from the electronic record on the computer. First, electronic medical records have many clickable fields, like hyperlinks on a web page, that lead to other screens. This computerized design creates an easy to use interface and logical flow, allowing related parts of the medical data to connect with each other. When receiving screenshots or printouts of electronic medical records, that logical flow is lost. What remains is a large number of documents that are often disorganized and difficult to interpret.

To illustrate, consider a reader of a news website looking for analysis on a recent presidential debate. This news website is organized with a main page divided into sections based on the different and broad topics discussed during the debate. From there, each broad topic is narrowed to various subtopics. Each subtopic consists of multiple articles from different authors about that subtopic. In order to find the articles that the reader is seeking, he or she clicks on the topic, then clicks on the subtopic, and finally clicks on the needed articles. Alternatively, the reader could use a search feature to find the correct commentary. Now, consider the alternative. Rather than an organized web page, the reader is presented with a box of paper filled with every article about this recent presidential debate on the website. In order to find the relevant articles, the reader must look at and interpret every article in order to ensure that all have been found.

--

40. “An ‘original’ of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, ‘original’ means any printout—or other output readable by sight—if it accurately reflects the information . . . .” FED. R. EVID. 1001(d).
41. See Hudock, supra note 19.
42. See Smelcer, supra note 29.
43. See Dimick, supra note 7.
44. Id.
45. Id.
B. Metadata

Metadata is “data about data.” Metadata is evidence . . . that describes the characteristics, origins, usage and validity of other electronic evidence. Metadata is not always constant: It can change over time, even without human intervention, by the computer’s software and operating system. There are two kinds of metadata: application metadata and system metadata.

Application metadata is located within “the file it describes and moves with the file when you copy it.” A common, everyday example of application metadata is in Microsoft Word documents. By default, any Microsoft Word document will contain metadata that includes the author’s name, the name of the computer used to create the file, the last time it was saved, the date it was created, and the creator’s company name. This data is embedded in the Word file, created automatically, and updated in real time.

System metadata is stored in a separate file on the computer. The computer uses this metadata to keep track of where all the files are on the hard drive. It also keeps track of information about each file such as “each file’s name, size, creation, modification and usage.” Therefore, as the data of a computer system changes, the

49. See Ball, supra note 46, at 3.
50. Id.
51. Id.
53. See Farrar, supra note 52.
54. See Ball, supra note 46, at 3.
55. Id.
56. Id.
metadata that keeps track of that data dynamically changes with it.\textsuperscript{57} In practice, this means that viewing a file without employing specialized techniques, like rendering all relevant files unalterable, can alter the metadata.\textsuperscript{58} While some metadata is accessible by clicking certain buttons or menus in the operating system or program, other metadata is only accessible by using specialized applications.\textsuperscript{59}

What metadata must healthcare providers produce for the requesting party? In \textit{Williams v. Sprint/United Management Company}, a class action suit, an employee argued that she was terminated due to her age.\textsuperscript{60} A piece of evidence, an Excel document, was scrubbed for metadata before production.\textsuperscript{61} The court sanctioned the defendants for this action.\textsuperscript{62} The court held that parties should produce documents with all metadata unless the parties agree otherwise or “the producing party requests a protective order.”\textsuperscript{63} Once the court orders production of an electronic file, the burden shifts to the producing party, which must convince the court that producing the metadata is too burdensome.\textsuperscript{64}

Not all metadata is necessarily amenable to a printed format, and not all of it is relevant.\textsuperscript{65} Printing all metadata for the entire electronic medical record would take an inordinate amount of paper, and the data would be virtually indecipherable to lawyers.\textsuperscript{66} Nevertheless, according to \textit{Williams}, by default all metadata should be produced.\textsuperscript{67} However, since production of most electronic medical records is traditionally done in paper form, only relevant metadata that can be printed can be produced.\textsuperscript{68} Such relevant metadata sources include audit trails, pop-ups, and preliminary questions and checkboxes that make up a finalized doctor’s note.

\begin{itemize}
\item \textsuperscript{57} Id. at 7.
\item \textsuperscript{58} Id.; see also \textit{Best Practices & Principles for Addressing Electronic Document Production}, 5 SEDONA CONF. J. 151 (June 2007), available at http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCIP_2nd_ed_607.pdf.
\item \textsuperscript{59} See Ball, supra note 46, at 3.
\item \textsuperscript{61} Id.
\item \textsuperscript{62} Id. at 641–42.
\item \textsuperscript{63} Id. at 652.
\item \textsuperscript{64} Id.
\item \textsuperscript{65} See Ball, supra note 46, at 5–6.
\item \textsuperscript{66} Id. at 5.
\item \textsuperscript{67} See Williams, 230 F.R.D. at 652.
\item \textsuperscript{68} See Ball, supra note 46, at 5–6.
\end{itemize}
1. Audit Trail

An audit trail, a record of every change or addition to an electronic medical record, can be produced if requested. This is particularly useful for authenticity verification; how can the healthcare provider prove that the electronic medical record is authentic and accurate? With paper medical records, medical staff could go back and alter the record or not be entirely truthful when entering data. Lawyers would have to resort to depositions of other staff members and handwriting and ink analysis to determine what really happened.

A benefit of electronic medical records is that they keep audit trails of every edit of the record. An audit trail includes the identification of the terminal used to access the record and the date, time, and author of the change or addition to the electronic medical record. This can be discovered by the lawyer and used as evidence. However, the challenge with audit trails is that they do not always give an accurate representation of what occurred. For instance, if a nurse took the temperature of a patient at 9 a.m., but did not finalize the entry into the record until 9:30 a.m., the record may show a timestamp of 9:30 a.m. and therefore would be inaccurate. Furthermore, a nurse may begin work on a patient and then be called away only to have another nurse complete the task. The record would be


70. See May v. Moore, 424 So. 2d 596, 603 (Ala. 1982) (holding trial court did not commit error when allowing testimony that Dr. May may have tampered with evidence).

71. See Gaydar v. Sociedad Instituto Gineco-Quirurgico Y Planificacion, 345 F.3d 15, 25 (1st Cir. 2003) (holding physician can testify without expertise in handwriting analysis on handwriting of a medical document); see also FED. R. EVID. 901(b)(2).

72. See Richardson ex rel. Richardson v. DeRouen, 920 So. 2d 1044, 1047 (Miss. Ct. App. 2006) (allowing withdrawal of medical records to be forensically tested for alteration and ink analysis).

73. See Audit Trails and Medical Malpractice Cases, supra note 69.

74. See Dimick, supra note 7.

75. See Audit Trails and Medical Malpractice Cases, supra note 69.

76. Id.

77. See Dimick, supra note 7.

78. Id.; see also Ralph C. Losey & Kristen A. Foltz, Electronic Medical Records: What are some of the Practical Issues Lawyers Should be Aware of During Discovery and Litigation?, ABA HEALTH ESOURCE (June 2009), http://www.americanbar.org/newsletter/publications/aba_health_esource_home/Losey.html.

79. See Dimick, supra note 7.
timestamped with the first nurse’s identification, even though she was not the one who completed the record.\textsuperscript{80} Furthermore, if the first nurse then accessed records at the same time from another part of the facility, it could raise credibility issues that would have to be explained in court.\textsuperscript{81} Finally, oftentimes the staff member logged into the electronic medical record is not the only staff member in the room; a nurse may document a patient’s condition, while a doctor performs a procedure or makes an assessment.\textsuperscript{82}

Another issue is that the contents of the audit trails are not always well defined, and terminology may differ across different electronic medical record software.\textsuperscript{83} In one instance, metadata in the electronic health record stated that “an order was placed by a clinician and ‘accepted.’”\textsuperscript{84} But this order was not included in the electronic health record.\textsuperscript{85} This concerned the lawyers handling the case, as they feared important data was withheld or erased.\textsuperscript{86} However, depending on the circumstances surrounding the entry, “[a]ccept’ could mean a record was pended, filed, shared, or officially accepted by a physician.”\textsuperscript{87} In that case, according to those circumstances and that electronic health records program, “accepted” simply meant that the order was “pend[ing]” and never actually carried out.\textsuperscript{88} Therefore, it was never entered into the electronic medical record and was not produced.\textsuperscript{89}

2. Pop-up Warnings

Many electronic medical record systems include alert and reminder pop-up features that warn the doctor of potential interactions between two medications a patient is taking that could cause an adverse reaction\textsuperscript{90} and potential allergic reactions.\textsuperscript{91}

\textsuperscript{80} Id.
\textsuperscript{81} Id.; see also Losey, supra note 78.
\textsuperscript{82} See Losey, supra note 78.
\textsuperscript{83} See Nowik, supra note 30.
\textsuperscript{84} See Dimick, supra note 7.
\textsuperscript{85} Id.
\textsuperscript{86} Id.
\textsuperscript{87} Id.; see also Nowik, supra note 30.
\textsuperscript{88} See Dimick, supra note 7.
\textsuperscript{89} See Rose, supra note 17.
However, many doctors feel that the warnings are conservative and give a large number of “false-positive alerts” that do not take into account the patient’s entire situation.92 Furthermore, they occur so frequently that many doctors often ignore them and prescribe the medication anyway.93 This can lead to “alert fatigue,” which occurs when too many alerts overwhelm the doctor and can cause other unimportant or important alerts to be ignored.94 Thus, some electronic medical records programs provide the option to limit warnings based on their level of severity.95 Other electronic medical records program manufacturers prefer having the extra alerts to allay their fears of additional liability or litigation.96 This shifts the risk of liability onto any doctor ignoring the alert. If a patient suffered a complication because of a drug-drug interaction, metadata could be useful evidence if it shows that the program warned the doctor about the possibility of an adverse reaction.97

3. Preliminary Questions and Checkboxes that Make Up a Finalized Doctor’s Note

Doctors’ notes can also contain metadata. Doctors commonly write their notes in the SOAP format: a subjective description of the patient, an objective description of the patient’s condition, assessment of the condition, and plan of action for the patient to treat the condition.98 Some electronic medical record systems allow the doctor...
to dictate, type, or digitally write this report. Other electronic medical record systems use a series of screens with questions and checkboxes about the patient’s visit.

The system then automatically takes that information and creates a note that describes the visit. Still others use a hybrid system including elements of both. However, this interactive method of data entry is not easily translatable to printed records. Should the healthcare provider simply produce the finalized doctor’s note, the answers to each of those questions and checkboxes, or both? This issue has not been uniformly addressed.

C. Discovery Rules – Tampering with Evidence?

The Federal Rules of Evidence allow electronic medical records to be admitted over a hearsay exception if (1) the record is made “in the course of a regularly conducted activity of a business . . .” and (2) it is “regular practice” to create such a record. In addition, under the Federal Rules of Evidence, records must be authenticated before they can be admitted as evidence. The producer of the records “must demonstrate 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.” Authentication of electronic records can be achieved through identifying distinctive characteristics or through comparisons by an expert witness. Distinctive characteristics can include using metadata to verify the legitimacy of

99. See Smelcer, supra note 29, at 81–82.
101. Id.
103. See Losey, supra note 78.
104. Id.
105. FED. R. EVID. 803(6); see also FED. R. CIV. P. 34(b)(2)(E) (“[A] party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request.”); Deborah Adair, Update: Maintaining a Legally Sound Health Record—Paper and Electronic, 76 J. OF AHIMA 10 (Nov.—Dec. 2005), available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_028509.hcsp?dDocName=bok1_028509.
106. FED. R. EVID. 901(a).
108. FED. R. EVID. 901(b)(4).
109. FED. R. EVID. 901(b)(3).
An expert witness can verify the legitimacy of a record by comparing it with records that have been confirmed as legitimate.

Electronic medical records, by design, change dynamically as new information is recorded into the system. However, tampering with or altering evidence could trigger sanctions under the Federal Rules of Civil Procedure. Furthermore, courts can order a legal hold on potential evidence. A legal hold is an order issued by the court to preserve data relevant to anticipated or current litigation. If data is destroyed improperly, this can lead to a claim of spoliation. Spoliation is the intentional “destruction, . . . alteration, or concealment of evidence.” If there is a loss of data material to the case, the burden of proof rests on the healthcare provider to prove to the court that this data loss was in good faith. If the healthcare provider is unable to prove that the loss was in good faith, then the provider may be sanctioned by the court or required to reconstruct the data—a potentially costly procedure. Because electronic medical records are dynamically altered as new information is added, it can be difficult to convince opposing counsel and a judge that the information in the electronic medical record has not been tampered with and is legitimate.
Healthcare providers have protected themselves from court sanctions or costly data reconstruction orders by keeping periodic backups of all medical record data in conformance with a retention policy.\footnote{122} This data can be useful in showing whether the data provided in a medical record or audit trail has been illicitly altered.\footnote{123} Retention policies differ from provider to provider, but Medicare requires that records be retained “for a period of at least 5 years.”\footnote{124} In addition, the Civil False Claims Act places a ten-year statute of limitations on federal fraud and abuse.\footnote{125} This creates an incentive for medical care providers to maintain backups of records for at least ten years in case of a potential suit for violation of this act.\footnote{126} Healthcare providers have also established policies to suspend their normal retention policy if they receive a legal hold issued by a court.\footnote{127}

Some healthcare providers transitioning to electronic medical records have scanned their old paper medical records into their computerized system and then destroyed the originals.\footnote{128} This creates a number of potential problems. First, if the scanned image is illegible, it could lead to a claim of spoliation because the original paper records may have been legible.\footnote{129} Second, if litigation is reasonably anticipated, there may be a duty to preserve potential evidence.\footnote{130}

Therefore, it is a major concern for medical providers to determine how to authenticate and avoid spoliation of electronic medical records—a source of evidence that is updated in real time as the electronic evidence when a debtor argued a bankruptcy issue with his creditor, but the creditor’s electronic business records were not admissible as evidence because the lower court “concluded that the defective evidentiary foundation was not cured”).\footnote{122} See Anderson, \textit{supra} note 114; see also Chapter 10: Data Collection and Quality Assurance, \textit{in Registries for evaluating patient outcomes: A user’s guide} 235 (RE Gliklich & NA Dreyer eds., 2d ed. 2010), available at http://www.ncbi.nlm.nih.gov/books/NBK49444/pdf/TOC.pdf.\footnote{123} See generally Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 215, 217–18 (S.D.N.Y. 2003) (holding that, in a nonmedical case, the defendant had a duty to preserve backup tapes that may have contained emails relevant to the case).\footnote{124} See 42 C.F.R. 482.24(b)(1); see also Kathie McDonald-McClure, \textit{Conversion to electronic health record and retention of paper records}, HITECH LAW BLOG (Feb. 18, 2010), http://healthitlawblog.wordpress.com/2010/02/18/conversion-to-electronic-health-record-and-retention-of-paper-records/.\footnote{125} See 31 U.S.C. § 3731(b)(2) (2006); see also McDonald-McClure, \textit{supra} note 124.\footnote{126} See McDonald-McClure, \textit{supra} note 124.\footnote{127} See Anderson, \textit{supra} note 114.\footnote{128} See Losey, \textit{supra} note 78.\footnote{129} Id.\footnote{130} Id.
patient data changes. It can be difficult to convince opposing counsel or a judge that a constantly changing record was not altered improperly. Ways to verify authenticity and disprove spoliation include examining audit trails and electronic medical record backups.

D. Copy and Paste

The copy and paste function of electronic medical records is also problematic in the context of discovery. The use of computers with electronic medical records allows doctors to copy and paste from one part of the record to another. While copying medical records began before electronic medical records, it is now much easier and faster to do so using computers. When copying and pasting occurs, it can make the record more difficult to understand, and can include redundant information. A study also identified copying and pasting as a major source of electronic medical record documentation errors. This often occurred when medical staff would copy and paste a portion of text without properly proofreading it to ensure that it was still accurate. An example includes writing that a “patient walked for the first time” repeated for three days. This is a widespread phenomenon; one study of 167,076 VA records found copying and pasting in “about 3% of all exams.”

---

131. See Hudock, supra note 19; see also In re Vee Vinhnee, 336 B.R. 437, 440–45 (B.A.P. 9th Cir. 2005).
133. See Chapter 10: Data Collection and Quality Assurance, supra note 122, at 233, 235.
134. See Losey, supra note 78.
135. Id.
139. Id. at 63.
140. Id.
occurrences, about 1.6% were “[h]ighest” risk for harm to the patient and 0.6% were “[m]oderate” risk for harm to the patient.\textsuperscript{142} For a lawyer, copying and pasting can make the identity of the author of that part of the record difficult to discern.\textsuperscript{143} In addition, it may be unclear which doctors are liable and who should be deposed. Can the doctor who wrote the original text share liability with other doctors who use that original text?\textsuperscript{144} Did every doctor who used an incorrect portion of the record make an error, or just the original author?\textsuperscript{145} Can doctors who copy an earlier doctor’s work assume that the original doctor’s text was accurate or is still accurate, or is it the later doctor’s job to determine this him or herself?\textsuperscript{146} Based on these questions, which doctor or doctors should the lawyer depose?\textsuperscript{147} Furthermore, parts of the copied and pasted text may no longer be applicable, making it more difficult to interpret the medical record.\textsuperscript{148} Some have responded by disabling the copy and paste feature.\textsuperscript{149} However, some researchers warn that this approach could have a negative impact on the effectiveness of electronic medical records.\textsuperscript{150} Copying and pasting is efficient in certain circumstances and can be useful if utilized with care.\textsuperscript{151} Instead, researchers recommend better education and guidelines on writing notes coupled with a monitoring system to supervise and give feedback.\textsuperscript{152} Other researchers have recommended that medical professionals should only copy historical facts about the patient, not recent data that is likely to change.\textsuperscript{153}

\begin{flushright}
\textsuperscript{142} Id. at S125. Risk in this context concerns from whom the copying took place and/or the age of the original text. Id. at S124. For instance, “highest risk” consisted of “copying from another author or from more than 6 months in the past.” Id. “[M]oderate risk” consisted of “copying from oneself from 1 to 6 months before.” Id.
\textsuperscript{143} See Losey, supra note 78.
\textsuperscript{144} Id.
\textsuperscript{145} Id.
\textsuperscript{146} Id.
\textsuperscript{147} Id.
\textsuperscript{148} Id.; see also Hirschick, supra note 137, at 2335–36.
\textsuperscript{149} See Losey, supra note 78.
\textsuperscript{151} Id.
\textsuperscript{152} Id.
\textsuperscript{153} See Hersh, supra note 136.
\end{flushright}
II. Embracing Electronic Discovery While Finding a Balance to Protect Both the Healthcare Provider’s and Requesting Party’s Interests

In order to use electronic discovery methods for electronic medical records, two things must be done. First, a new rule must be added to the Federal Rules of Civil Procedure that requires medical care providers to release electronic medical records in an electronic form that adheres to seven requirements. Second, methods must be established that create a practical and secure way to produce patient records electronically.

A. Proposal: Add/Modify a Provision to the Federal Rules of Civil Procedure

Federal Rule of Civil Procedure 34(b)(2)(E)(i), addressing production of electronically stored information, states, “[a] party must produce documents [1] as they are kept in the usual course of business or [2] must organize and label them to correspond to the categories in the request.” Federal Rule of Civil Procedure 45(d)(1)(A), states, “[a] person responding to a subpoena to produce documents must produce them [1] as they are kept in the ordinary course of business or [2] must organize and label them to correspond to the categories in the demand.” If electronic medical records are produced in paper form, these records are not produced in the form used “in the ordinary course of business”—an electronic format. For many reasons, printing and labeling the documents is inadequate for electronic medical; one reason is that it makes the records harder for the lawyer to decipher, as discussed in Part I. With the Rules in their current form, medical care providers have the option of picking either electronic or physical production of documents. Therefore,


157. For instance, printed electronic medical records do not retain the ease of use that the digital form used by medical staff during their ordinary course of business offers. See *supra* Part I.

medical care providers currently may produce medical records physically.  

In order to solve the problems discussed in Part I, a new rule must be added to the Federal Rules of Civil Procedure. Due to the uniqueness of electronic medical records, this new rule must be narrowly tailored to only electronic medical record discovery. The goal of this new rule is to retain the benefits of paper record discovery while utilizing an electronic format for production. The new rule will mandate that electronic medical records be produced in an electronic form.

This electronic form must adhere to seven elements. First, the electronic form must be read-only for the viewer of the record. This means that the record must be locked in such a way that a viewer cannot alter the record. This prevents any wrongful tampering of the record once it is produced.

Second, the record must be secure so that only the necessary individuals during the litigation may view it. For instance, during discovery in a medical malpractice case, the electronic form of the record could be encrypted with a secure password that is only divulged to the lawyers involved in the case. This protects the patient’s privacy so that only the few individuals who know the password can view the record.

Third, each party’s lawyer must have independent access to the record. This means that the lawyer can access the record at any time during the full duration of the case from his or her own computer. This is significant because it gives lawyers the same flexibility of paper records, the ability to view the electronic record at any time.

Fourth, the electronic form must protect other patients’ privacy. Therefore, only electronic medical records of patients at issue in the case may be produced; all other patients’ electronic medical records must be inaccessible to the party requesting the records.

Fifth, the electronic form must allow for redactions by the producer. For instance, the medical care provider may want to redact information relating to individuals who are not parties to the case, including other patients. However, these redactions must be clear and obvious to the viewer and may be appealed to the judge. This allows for the producer of the record to protect patient privacy with respect to non-relevant parts of the electronic medical record. On the

160. See infra Part II.B.1.d.
other hand, it also allows the other party to appeal if that party feels that a redacted portion of the record is relevant to the case.

Sixth, the electronic form must support the ability to limit the amount of information accessible based on a set time period. This time period is determined by the wording of the discovery request or subpoena, and it can be appealed to the judge. This is important because cases sometimes focus on a particular time period of the medical record. For instance, discovery of a medical record in a medical malpractice case may only require the portion of the record concerning the circumstances surrounding the alleged medical error.

Seventh, the electronic form must resemble the interface used by electronic medical record systems. This means that the general user interface format that is used by electronic medical record systems must be preserved or emulated for the viewer. Since this user interface format is how the records are used in the “ordinary course of business,” it ensures an accurate reproduction of the record electronically and makes the records easier to read and interpret. Currently, it is impractical for many systems to produce electronic medical records, as they are kept electronically “in the ordinary course of business,” because mechanisms to do so have not been implemented. It is commonplace for different electronic medical record systems to employ their own, unique method of storing data. This makes complete and seamless interoperability among different electronic medical record systems difficult. However, mechanisms can be implemented that would allow a solution with minimal impact on the current electronic medical record ecosystem.

B. Proposal: Develop a Way for Lawyers to Access Electronic Medical Records Digitally in a Manner that is Secure, Remote, and Limited to Only Necessary Information

In order to devise a method for digital access to electronic medical records by lawyers, with minimal impact on current electronic medical record systems, three goals must be met. First, any method must be as easy to implement as possible for the electronic

162. See supra Part I.A.
164. See Hudock, supra note 19.
165. Id.
166. See generally id.
medical record vendors. Therefore, rather than radically changing pre-existing functionality, changes should focus on using existing functionality where possible, while allowing for relatively small changes when necessary. Second, the method must not infringe on the privacy of other patients or include data not specified in the subpoena or valid discovery request. Third, since the method must aim to replace paper record discovery, it must be capable of displaying any medical information that could be produced from an electronic medical record through a printout.

Two methods fit these criteria. First, electronic medical record systems that support remote access to patient records should implement a limited, read-only access login for lawyers. Second, electronic medical record systems should support a standardized export feature of specific patient information that can be viewed by a read-only, freely available viewer application.

1. Mandate Remote, Limited Access for Lawyers to Specific Patient Data in Electronic Medical Records

The simplest way to allow lawyers direct access to electronic medical records is for the medical care provider to give them remote, limited access to only the patient data requested in a valid discovery request or subpoena. In order to do this, the Federal Rules of Civil Procedure must mandate that (1) electronic medical record vendors include the capability to create unique logins for lawyers with read-only access limited to specifically requested patient data. The Federal Rules of Civil Procedure must also mandate that (2) medical providers with remote access to electronic medical records allow limited access to lawyers with a valid discovery request or subpoena. This implementation would differ based on whether the electronic medical record system is primarily based on a client-server (local) model167 or based remotely in the cloud.168 However, it is important to note that implementations can include elements of both types.169 For instance, an electronic medical record system may store all the patient data locally but store back-ups remotely on internet-based cloud servers maintained by the electronic medical record vendor.170

167. See supra Part II.B.1.a.
168. See supra Part II.B.1.b.
170. See, e.g., Enterprise Cloud Services, supra note 169.
a. Client-Server (Local) Electronic Medical Record Systems

Client-server (local) electronic medical record systems are software suites that store data on servers at a medical provider facility. This data is often backed up periodically to maintain the safety of patient data, and some implementations also back up over the Internet to remote servers. The advantage of this method is that the medical provider has direct control of maintenance and security of patient data. In addition, client-server electronic medical record systems do not rely on an active Internet connection. This is because implementations that rely on a local server do not require a constant Internet connection to function. This method is recommended for larger medical care facilities that can support the investment of servers and teams of individuals to run and provide upkeep for them. Furthermore, many medical providers use methods of remote access, including Citrix or VMware, for medical staff to remotely access their electronic medical record systems outside the medical care provider facility.

b. Software as a Service (Cloud-Based) Electronic Medical Records

Some electronic medical record systems, like GE’s Centricity Advance, have moved entirely online using a method called

172. See Chapter 10: Data Collection and Quality Assurance, supra note 122, at 235; see also Anderson, supra note 114.
173. See Enterprise Cloud Services, supra note 169.
175. See Flam, supra note 171.
176. Id.
178. See Flam, supra note 171.
software as a service (SaaS), a component of Internet-based cloud computing. This method hosts data on servers, maintained by the vendor, and allows for remote access over the Internet. This service is advertised as an attractive alternative to client-server (local) based electronic medical records for smaller medical care providers: the start-up and upkeep costs are lower, and it is easier and faster for the medical provider to set up. Web-based email clients like Gmail or Yahoo are examples of this type of service. Rather than using installed email software like Microsoft Outlook and storing emails on the hard-drive of a computer, all emails are stored only on servers operated by the email provider and accessed through a web-based interface accessible from any computer in the world with Internet access.

Cloud-based electronic medical record systems store patient data on servers operated by the electronic medical record vendors, rather

---

184. Id.
than the medical care provider.\textsuperscript{189} This externalizes the cost of maintaining the electronic medical record system to the vendor; updates to the system’s software are handled directly by the vendor.\textsuperscript{190} However, medical providers pay a monthly fee for the service.\textsuperscript{191} Using the vendor’s electronic medical record interface, medical care providers can access the patient data remotely from any computer\textsuperscript{192} or iPad\textsuperscript{193} with Internet access. Despite the benefits of this approach, some medical care providers are wary of trusting all their patient data to an electronic medical record vendor. Specifically, providers are concerned about potential liability if patient data is compromised due to security breaches\textsuperscript{194} or data loss if the vendor goes out of business.\textsuperscript{195}

c. Implementation

In practice, a medical care provider’s lawyer works with its system administrator to produce the records requested. This lawyer would instruct the administrator to provide access to particular patient records for specified time periods and to redact certain information.\textsuperscript{196} This gives the lawyer control over the content of the records being produced. Access would be granted to the requesting party for the duration of the legal action until there is no further possibility of appeal. Afterwards, the producing party may discontinue access to the account to protect patient privacy.

\begin{footnotes}
\item[189] See Polack, supra note 185; see also LA & KIM, supra note 183, at 278; Web Based EMR, supra note 181.
\item[190] See Web Based EMR, supra note 181.
\item[191] For Centricity Advance, the medical care provider pays a monthly fee to use this product, rather than purchasing the necessary server hardware and software licenses. See GE Healthcare Introduces True Web-based EMR for Independent Physician Practices, supra note 185.
\item[195] See Polack, supra note 185; see also Flam, supra note 171.
\end{footnotes}
However, the other party may still obtain a court order to keep access open, if the judge grants it.\footnote{197}

To implement remote access for lawyers on a client-server records system, an electronic medical records administrator could provide a unique login for the lawyer by creating a new user and utilizing a permissions settings feature to reduce access privileges.\footnote{198}

The electronic medical record vendor must ensure that its system can manage access privileges for users so that the administrator could specify which patients’ electronic medical record can be accessed and what information within those patient records can be accessed. In addition, the provider would create a special remote login for the lawyer for the duration of the legal action that would allow access to only the electronic medical record system that holds relevant patient records. The lawyer would then use this unique, secure, and limited login to access specific patient data. A requirement under the Federal Rules of Civil Procedure for the presence of these features in electronic medical record systems would make electronic discovery of specific patient data within these systems practical.

Electronic medical record systems that rely on Internet-based cloud computing often already have features that allow medical care providers to set access limitations for users.\footnote{199} For instance, Centricity Advance has a “practice management system” that can adjust specifically which functions each user may access.\footnote{200} This allows medical providers to control access permissions for each user.\footnote{201} Practice Fusion has a feature to customize users’ access level based on professional qualifications and credentials.\footnote{202}


\footnote{198. There is a demonstration of this process for Centricity 9.5. See GE HEALTHCARE, supra note 177, at 90–97.}


\footnote{201. Id; see also System Planning and Requirements for Centricity Practice Solution, supra note 177, at 63.}

\footnote{202. See Customized EMR Access for Everyone in Your Practice, supra note 199. For another example, see OpenEMR’s implementation for different access level permissions for different professional qualifications and credentials; OpenEMR Version 4.1.0 Demo, supra note 199; Id.}
remote lawyer access for electronic medical records vendors, they would simply have to add features that allow lawyers limited access using this pre-existing functionality. First, they would have to create a new lawyer access level with permissions specific to lawyers. This new access level would allow read-only viewing of specifically selected patient information. Second, vendors would need to integrate tools that further limit the specific user’s ability to view the record. These tools must allow medical providers to customize the scope of user access by allowing them to select specific patients, redact parts of the record, and limit the scope of time viewable in the record.203 Requiring this functionality in the Federal Rules of Civil Procedure would allow direct, limited access to Internet-based cloud electronic medical records to be a viable method of electronic document discovery.

d. Necessary Features

For either client-server or SaaS (cloud-based) medical record systems to replace paper records in discovery, the records viewable to a new user created for a lawyer on any electronic medical record system must be redactable, time-limited, and narrowed to only the relevant patient’s data.

First, any information in the electronic medical record must be redactable only when viewed by the new user. Any redactions must be visibly obvious to the viewer so that the other party may appeal the redaction. Therefore, a red box over any redacted text or images would appropriately cover over that information while still presenting a visible cue that the redacted information exists. Entire sections may also be redacted with a red box over that section. However, to prevent unnecessary appeals, functionality should also exist to allow the producing lawyer the option to add a short note explaining why any item was redacted.

Second, the electronic medical record system must be capable of limiting the new user to viewing only information within a specific time period. Not every case may require this feature.204 However, this capability is important for those cases that rely on a static, unchanging record. To create this functionality, all references in the record to a time period must be utilized. The important distinction is the difference between the date entered into the electronic medical

---

203. Look to the next section for more details on how to implement these three features. See infra Part II.B.2.d.
204. See infra II.B.1.f.
record and the time period described in the record. For instance, a nurse may enter into the medical record on April 4, 2011 that a patient broke his leg on March 2, 2001. As a result, the electronic medical record system must have the capability to limit the scope of the medical record viewable to the lawyer by both the time period that the record was entered and the time period specified in the record. Many electronic medical record systems already have the functionality to search or view based on date of entry. Therefore, because the necessary metadata is already present within these systems’ records, it should be relatively easy for medical records vendors to implement a feature that limits viewable information based on date of entry. Since doctors’ notes are primarily just searchable text, it is possible to automatically find all dates mentioned within a time period and flag them for review by the medical provider’s counsel. He or she can go through each flagged portion of the medical record and decide what data should be produced.

Third, the electronic medical record system must be capable of limiting the new user to only a certain patient’s data. Therefore, when a lawyer uses this user account, only the patient contained in a valid discovery request or subpoena would be accessible. This protects the privacy of other patients not involved in the legal action.

e. Admissibility of Remote Access Electronic Medical Records as Evidence

Remotely accessed electronic medical records can be admitted into evidence as long as: (1) a separate user account is created for admitting evidence and (2) it is configured appropriately to ensure that the data in the record remains static. First, a separate user account must be created for admitting evidence. This isolates potentially admitted evidence in a separate user account; not all evidence discovered necessarily will be introduced in court as evidence. Both parties and the judge would have access to this user account. After the producing party represents to the judge that the records are genuine, the party that received the records must communicate to the medical provider administrator the parts of the


206. Id.

207. Not all evidence is relevant. Fed. R. Evid. 401.

208. A “health record custodian” authenticates the records “by providing testimony about the process or system that produced the records.” Adair, supra note 105.
record they want to admit into evidence in order to have those portions visible in the user account. A mutually agreeable deadline to accurately make the modifications to the account must then be set. The judge may impose sanctions on the producing party if the deadline is materially breached. 209 After both parties have decided which material they wish to admit into evidence, both parties can seek approval from the judge and voice objections. 210 The judge can then accept portions or the entire electronic medical record into evidence. 211 Alternatively, the evidence can be admitted at trial as an exhibit. 212

Second, the user account must be configured appropriately to ensure that the data within the record remains static to the viewer over time. This is important for admissibility of evidence because the judge has already approved the medical record. Any changes to already admitted evidence at trial is not allowed. 213 This can be accomplished with user account permissions. 214 By setting the user account to display only information added to the medical record within a range of dates, information will remain static when viewed while logged in to the electronic medical record via that user account. 215

f. Analysis

Remote access to limited patient data from electronic medical records would have a variety of advantages. First, it is a proven and secure method of accessing patient data, as this remote access technology is already in use for medical professionals with much broader access to patient records. 216 Second, lawyers would have access to the same interface and format that medical professionals use, sidestepping the formatting problem of paper printouts of

211. FED. R. EVID. 902(11).
213. This would be tampering with evidence. See, e.g., OHIO REV. CODE ANN. § 2921.12 (2012).
214. See infra Part II.B.1.d.
215. Id.
electronic medical records for legal use. Third, the medical information will be more easily decipherable by lawyers because the information would be in the electronic form that the electronic medical record vendor intended for use. Fourth, medical providers would be able to limit lawyer access easily and effectively via a user permission feature to prevent lawyers from gaining access to restricted information. Lawyers may also appeal to the judge if too much information is withheld. Fifth, once the system is set up, adding additional users with limited access takes only a few clicks of the mouse compared to the relatively high cost of printing all of a patient’s medical information. Furthermore, with appropriate user permissions, lawyers could access metadata, such as audit trails, electronically.

Another difference between this method and electronic medical records printouts is that the lawyer could potentially have access to the record in real-time during discovery rather than a static copy of the record from the date of the printout. This presents unique advantages. If a lawyer’s user account was configured so that he or she could see real-time changes in the electronic medical record, that lawyer would be able to see the records dynamically as they changed over time. In situations where a periodically updated medical record is required, such as in disability claims, there would be no need to request an updated version of the record; lawyers would have continual access to any changes. On the other hand, if the electronic production of the record were set to display only a specific period of time, then the medical record would be static.

217. See supra Part I.A.
218. See Dimick, supra note 7; see also supra Part I.A.
219. See System Planning and Requirements for Centricity Practice Solution, supra note 177, at 90–97.
220. See FED. R. CIV. P. 45(a)(1)(D).
221. See System Planning and Requirements for Centricity Practice Solution, supra note 177, at 90–97.
223. See System Planning and Requirements for Centricity Practice Solution, supra note 179, at 63–70.
224. Hudock, supra note 19.
This implementation has one clear disadvantage. Not all medical care providers have remote access to their electronic medical records. In those cases, this approach would not be feasible. However, there is another alternative to fill this gap.

2. Mandate That Every Electronic Medical Record Vendor in the US Be Able to Export a Patient’s Record into a Standardized Format

In 2009, Congress passed the American Recovery and Reinvestment Act, which allocated funds to support the transition from paper records to electronic medical records. On July 28, 2010, a new regulation created “meaningful use” standards that medical care providers’ electronic medical record systems must meet before they qualify for subsidies. The purpose of “meaningful use” standards was to guide the development of electronic medical records to ensure that they include certain important features. One such mandatory feature, in meaningful use stage 1, is interoperability, so that some key patient data can be exported to a common format. This enables patients to request certain key data in electronic form, like their medication list, and transfer it to other medical providers’ electronic medical record systems. While each electronic medical record system interface has slight differences, the objective of these systems is the same: each electronic medical record system seeks to display and store patient data. Therefore, the data entered into each system, like lab tests and doctor’s notes, and the required


229. See CMS EHR Meaningful Use Overview, supra note 227.


231. Id.

232. See Hudock, supra note 19.


interface to access them, have major similarities across software systems. While interoperability standards have been developed, none is currently ready to serve as a completely interoperable standard for all electronic medical record systems. Despite these difficulties, a complete interoperable standard is possible with industry cooperation and governmental support.

a. Current Interoperability Standards

Two formats have been developed: Continuity of Care Record (“CCR”) and Continuity of Care Document (“CCD”). These two competing formats are capable of storing exported medical data in a form that can be transferred to other electronic medical record systems. The major difference between CCR and CCD is that CCR data is more unstructured than CCD. This makes the way information is stored more flexible to implement in electronic medical record systems, but it is less standardized. CCD is more structured because it uses templates and standardized terminology. However, CCR is more widely used. Despite these advances, the creation of CCR and CCD formats is only a first step in creating a standardized format for an entire medical record to be interoperable with all electronic medical record systems. These formats are only required under “meaningful use” stage 1 for exporting key medical data, like medication lists, rather than an entire medical record.


237. Id.


239. See Kibbe, supra note 236.

240. Id; see also The Continuity of Care Document, supra note 238, at 3–4.

241. See Meaningful use glossary and requirements table, supra note 230, at 2.

242. See Kibbe, supra note 236.

243. Id.

244. See Meaningful use glossary and requirements table, supra note 230, at 6.
b. Difficulties in Creating an Interoperable Standard

There are multiple practical difficulties in creating a standardized export format, but using standards and adding additional metadata to the exported file can help resolve them. First, terminology can differ across software systems.\textsuperscript{245} For instance, the word “accepted” in one electronic medical record system could actually mean “pend[ing]” in another.\textsuperscript{246} In order to create a standardized export format, standard terminology must be utilized.\textsuperscript{247} Sharona Hoffman and Andy Podgurski’s article from 2008, \textit{Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems}, suggested that that vendors should utilize a “common exchange representation” to “unambiguously represent[] the [terminology].”\textsuperscript{248} This method could be based on an existing “standardized clinical terminology such as SNOMED-CT.”\textsuperscript{249} Currently, the CCD format uses a standardized terminology framework, such as SNOMED or LOINC, in order to maintain an accurate representation of patient data during export.\textsuperscript{250}

Second, abbreviations and terminology vary among practice areas.\textsuperscript{251} For instance, “MS” could stand for “multiple sclerosis’ in neurology” or “morphine sulfate’ in anesthesia.”\textsuperscript{252} In order to counter this, the export feature should include, and the interface should display, metadata of the practice area of the medical professional who wrote the text in order to guide the reader to the correct interpretation.\textsuperscript{253} This would give the viewer context in order to determine what the abbreviation meant.\textsuperscript{254}

\begin{itemize}
\item \textsuperscript{245} See Dimick, \textit{supra} note 7; see also Nowik, \textit{supra} note 30; see also infra Part I.B.1.
\item \textsuperscript{246} See Dimick, \textit{supra} note 7.
\item \textsuperscript{247} See Sharona Hoffman & Andy Podgurski, \textit{Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems}, 22 HARV. J.L. \\& TECH. 1, 152–53 (Fall 2008).
\item \textsuperscript{248} Id. at 153.
\item \textsuperscript{249} Id. \textit{See also SNOMED Clinical Terms® (SNOMED CT®), U.S. NAT’L LIBR. MED.}, http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html (last visited Jan. 22, 2012).
\item \textsuperscript{250} See Meaningful use glossary and requirements table, \textit{supra} note 230, at 2.
\item \textsuperscript{251} Hoffman, \textit{supra} note 247, at 152.
\item \textsuperscript{252} Id.
\item \textsuperscript{253} Id.
\item \textsuperscript{254} Id.
\end{itemize}
c. Requirements for a Complete, Interoperable Standard

There are four major requirements that an export feature must satisfy in order to replace paper printouts during discovery. First, the format used by the export feature must be capable of including any data currently being produced by the current printout implementation of electronic medical record discovery. Otherwise, the export feature would not produce a complete medical record. Therefore, it is imperative that the electronic medical records’ export feature include the capability to export all data needed for production during discovery. Furthermore, electronic medical record vendors should create their own, free, read-only viewing software, or work with current viewing software vendors, to ensure that these viewers can adequately display all necessary patient data.

Second, the format must be viewable in a layout and user interface similar to the digital version of electronic medical record systems. Therefore, a lawyer would be able to view the electronic medical record in a similar fashion to the way medical staff view the record in the “usual course of business.” This ensures that the patient data is easily viewable by a lawyer, and it ensures that the production adheres to the Federal Rules of Civil Procedure. Multiple programs exist or are in development that can read these formats. For instance, HealthFrame can act as a reader for CCR formatted records. VistA is also working on import functionality for CCR and CCD formats.

Third, the export feature must have the capability to narrow the data exported to only specific data necessary for production. If this is implemented, then the medical provider’s lawyer will be able to interpret a subpoena or valid discovery request and will have the ability to only produce relevant data. Furthermore, since an export feature simply uses a standardized format for the storage of electronic patient data, electronic medical record systems should be able to

---

255. See Fed. R. Civ. P. 34(b)(2)(E)(i) ("A party must produce documents [1] as they are kept in the usual course of business . . . .").

256. Id.


259. See Kibbe, supra note 236.
include as little or as much patient data as needed. However, parties may object if relevant information is missing.260

Fourth, the export feature must have the capability to encrypt the exported data using a strong method of encryption. The recommended standard is the well-proven encryption method, Advanced Encryption Standard (“AES”).261 AES is a very secure encryption method created by the National Institute of Standards and Technology.262 The US government has used AES since 2001.263 AES is capable of using encryption key lengths of 128-bits, 192-bits, and 256-bits; however, the 256-bit encryption key length is recommended for optimal protection.264 To ensure additional security, all passwords should include at least ten characters, including at least one number, one symbol, and one capital letter.

d. Analysis

There are multiple benefits to using an electronic medical record export format for discovery. First, as in the case of the remote login access proposal in Part II(B)(1),265 the medical care provider can restrict access by sending only the specific patient data required by the subpoena or valid discovery request. Second, the data can be transferred and stored physically on a USB flash drive, CD, or DVD.266 Third, lawyers would have access to the records through a digital interface, which solves many of the formatting issues present in printouts of electronic medical records.267 Fourth, if records are produced by the medical care provider, the lawyer may access metadata information that would be difficult to produce with paper printouts of electronic medical records.268 Fifth, this export function

---

263. See Intel® Advanced Encryption Standard Instructions (AES-NI), supra note 261.
264. Id; see also Advanced Encryption Standard (AES), supra note 262.
265. See supra Part II.B.1.
266. See The Continuity of Care Document, supra note 238, at 3.
267. See supra Part I.A.
268. Metadata can include a great deal of information. See Ball, supra note 46, at 5. Some metadata is easily understandable, while others are very complex. Id. For instance, registry keys often contain “thousands upon thousands of attribute values” about a computer system. Id.
can help alleviate any risk of spoliation by the medical care provider, as they would have another way of creating static backups of patient data; they could periodically export patient medical records into an interoperable format as another means of backup.  

However, there are some disadvantages to this approach. First, it would almost certainly be more difficult and expensive, and it would require more time to implement than the remote login approach. This is because it is difficult to implement a workable standard that every different electronic medical record system can use for all necessary patient data. However, because some preliminary steps to implement a workable standard have been included in meaningful use stage 1, there are already large incentives for vendors to include some export functionality. This is an important early step in creating a comprehensive standard export feature. Nevertheless, future government action to expand upon these requirements will likely be necessary to complete a standard export feature. Second, this approach can only create static files rather than potentially supporting access to real-time changes like the remote login approach. However, a static frame of reference, similar to paper records, has been sufficient for lawyers through the present day.

C. Both Approaches Should Be Applied

In order to cover any eventuality, both recommended approaches in Part II(B) should be adopted. The Federal Rules of Civil Procedure should focus on the remote login access approach during discovery, if practical for the medical provider. This method is superior because it is easier to implement and would give lawyers access to the same interface as medical professionals. Therefore, this method fits the Federal Rules of Civil Procedure’s “usual course of business” standard the best. If the medical provider does not have the necessary infrastructure to allow a lawyer to access the records remotely, then that medical provider should export the records to a standardized digital format. While this export approach boasts some of the same advantages of the remote login access approach, it has its

269. See The Continuity of Care Document, supra note 238, at 3; see also supra Part I.C.
270. See supra Part II.B.1.
271. See supra Part II.B.1.
272. See supra Part II.B.1.
273. See The Continuity of Care Document, supra note 238, at 3.
274. See supra Part II.B.1.
own unique advantages and is vastly superior to printouts of electronic medical records.

Upon the successful adoption of one or both approaches, continuing legal education ("CLE") courses should be offered in order to teach lawyers how to use this new technology effectively in a legal setting. Courses should include how to use electronic medical record viewing software, how to read and interpret an electronic medical record, and any new changes in electronic medical record discovery and evidence procedure. Electronic medical record vendors should work with CLE instructors to allow lawyers to learn from the actual software vendors used by medical providers in their practice area. Alternatively, free demos of electronic medical record software, like OpenEMR, are available to learn how to use and interpret electronic medical records.276

Conclusion

A major problem with discovery of electronic medical records today is that an electronic medical record system is converted to paper format for production during discovery. The current system of printing out electronic medical records for discovery has many flaws. Accessing electronic medical records remotely or by a common, interoperable exported format corrects many of these issues. However, electronic access of patient records by lawyers during discovery must preserve the advantages of the current printout system for electronic medical records. Therefore, it must be implemented in a manner that is secure, read-only, and protects the privacy of patients. The electronic form must also allow the producing party to redact non-relevant material in the record. But, an appeals process must be available to other parties if relevant material is not produced. Electronic medical records are the future of the healthcare industry. It is time for the legal community to establish new standards that adapt to our new, digital world.

276. OpenEMR has a free demo of their software available on their web site. OpenEMR Version 4.1.0 Demo, supra note 199.