

Analog Records In A Digital Age -- Pitfalls for Discovery Involving Electronic Health Records

Laird A. Pisto, J.D.
Associate General Counsel
MultiCare Health System, Tacoma, WA

1) Introduction

Expansive development of the electronic health record (EHR) is underway. In many instances:

- EHR developments have not kept pace with developing approaches to disclosure in litigation settings.
- Past practices of converting digital records to analog form, and then replicating the chart from the analog form, are passé and arguably improper under developing standards.
- Attempts to produce EHRs in an analog or “print” format present many problems and expose health care organizations and treating professionals to new and unforeseen risks.
- Best practices point toward digital access to EHRs in their native format. But there are numerous obstacles to that path.
- Recent amendments to the Federal Rules of Civil Procedure accelerate the need for assessment of best practices as they relate to the production of electronic health records in litigation settings.

This paper discusses developing trends in discovery processes in the context of litigation surrounding the EHR and suggests several factors which should be considered when developing methodologies to share the digital record outside of the environment of care.

2) Background

Historic production of the “medical record” involved assembly by health information management professionals, coupled with production of records using discrete replicable processes. Copies of records were simply “images” of the original, and anyone accessing the record set could locate specific data elements within the set using the same techniques used by treating professionals who had access to the original chart. For example, tabs were often embedded in the duplicate record set that matched the original chart in every

detail. As copying technologies improved, it became difficult to distinguish the original chart from a duplicate copy.

Health care professionals who were called upon to testify with regard to a typical analog record set could do so with confidence, knowing that the “certified” record before them was essentially a mirror image of the original record contained within the health system’s or provider’s records.

The development of more sophisticated electronic health record systems has been conducted in an environment of rapid change with few recognized “rules” concerning methodologies for producing and sharing duplicate copies of the EHR with others.

The absence of standards in terms of printing and replication of the digital record, coupled with the wide range of print and display options available to users, has led to enormous variability in how digital records are compiled and printed and has resulted in a much less uniform and much riskier environment from which the “legal medical record” is produced.

In turn, the variability in production methodologies has led to confusion among health professionals called upon to testify as to the care provided using the “print” version of the EHR to support their testimony.

Hybrid medical records, composed of both digital and analog records, are the norm in many health systems. Again, the methodology for compiling hybrid record sets is often inconsistent and dependent upon individuals familiar with only parts or “components” of the full record set. Typically, multiple system hosts are called upon to compile and deliver elements of the legal record set, again resulting in widely variable processes for reproduction of the “legal” medical record set.

When called upon to testify as to care documented within hybrid record sets, care providers are often confounded by the seemingly “foreign” record placed before them. And increasingly, providers are confronted by patients or opposing counsel holding seemingly contradictory or incomplete documents, or worse, record sets that are substantially different than the record set that they recall.

Confusion in the processes of delivering legal record sets, coupled with confusion on the part of care providers testifying in matters related to the legal record, have resulted in dissatisfaction with the process and have exposed providers and health care systems to increased risk of adverse rulings from the bench as well as adverse verdicts based upon finders of fact (juries) facing confusion and irregularities in the process of production of the legal medical record.

An “ideal” state for most providers called upon to testify as to matters contained within their EHR would be to simply display the EHR at the time of their testimony, and testify from the EHR in its “native” digital format.

Unfortunately, few EHRs are sufficiently portable or flexible enough to allow for real-time viewing of the chart in a portable, litigation environment. And even where such

display is feasible, few EHRs are capable of displaying the chart in its exact format as of a specific date and time in the past. Consequently, entries made in the chart after the date and time of a critical event ordinarily appear as part of the chart, making it difficult if not impossible to ascertain exactly what might have been before a provider at any particular moment in time.

Recently approved changes in the Federal Rules for Civil Procedure, (effective in December 2006) coupled with companion activities at the state level, cause HIM professionals to accelerate their review of processes for disclosing digital records in litigation settings.

3) Existing Underlying Rules

Underlying every medical record are state and federal laws pertaining to the record sets maintained by health care providers. AHIMA offers numerous resources for purposes of defining the “legal medical record.”¹

Whenever the legal medical record comes into play in the context of litigation, every jurisdiction has rules under which the parties must produce documents and other things of interest in the context of that litigation.

Previously, Rule 34(a) of the Federal Rules of Civil Procedure provided:

(a) Scope.

Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents (including writings, drawings, graphs, charts, photographs, phonorecords, and **other data compilations from which information can be obtained**, translated, if necessary, by the respondent through detection devices into reasonably usable form), or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

Every state also has a companion discovery rule substantially equivalent to Fed R Civ P 34, making not only the analog version of the medical record discoverable, but also potentially all underlying *data compilations* from which the analog version is produced.

Principles for the production of electronic records have been under discussion in many contexts, but there has been little uniformity in approach to the problems of “e-Discovery” as it is recognized, separate and apart, for the time being, from “Discovery.”

Several recent high profile cases have caused the courts to wrestle with e-Discovery issues, leading to recommended changes in the discovery rules to more directly address the myriad issues raised by the prevalence of electronic data of relevance in litigation contexts.

For an excellent discussion of the state of the art, see *The Sedona Principles for Electronic Document Production*.² Principle 8 is of particular interest in this context:

8. The primary source of electronic data and documents for production should be *active data and information* purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources. Sedona Conference, *ibid*.

Juxtaposed between traditional rules for production of business records (of which health records are but one example) and emerging rules for production of electronic records and data compilations, lie the various forms of electronic health records in use today. Many such records are only a small part of the complete legal record set.

HIPAA attempts to impose some order on these processes through the requirement for documenting the “Designated Record Set” which comprises any covered entity’s health care record.

Designated record set means:

- (1) A group of records maintained by or for a health plan or health care provider, that is:
 - (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
 - (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
 - (iii) Used, in whole or in part, by or for the health plan or health care provider to make decisions about individuals.
- (2) For purposes of this definition, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a health plan or health care provider.³

As noted, HIPAA views its Designated Record Set as a series of *compilations* of data from multiple sources.

And separately, organizations within the purview of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) are bound by several specific Information Management (IM)⁴ standards that directly tie to these issues.

4) Federal Rules Changes

In response to a series of high-profile cases involving discovery abuse in which electronic records were either disclosed late in the proceedings, or were destroyed in advance of their disclosure, the courts have been urged to develop rules specific to the exchange of electronic information.

On April 12, 2006 proposed amendments to the Federal Rules of Civil Procedure that address the discovery of electronically stored information were approved without comment by the United States Supreme Court. The new rules and amendments went into effect on December 1, 2006.⁵

While these rules were not necessarily developed as a result of any issues pertaining to EHRs, they portend sweeping changes in the way that EHRs are to be shared with litigants. For the most part, EHR developers and end-users are equally ill-prepared to deal with these changes.

At the heart of the rules change are major changes to the wording of Fed R Civ P 34:

Rule 34. Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes

(a) Scope.

Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or **electronically stored information** — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations **stored in any medium** from which information can be obtained — translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

As can be seen, amended Rule 34(a) is significantly more expansive in its sweep than the prior rule. Changes to Rule 34(a) are accompanied by several other rule changes pertaining to electronically stored information⁶, including:

a) Rule 34(b): Incorporates changes related to electronically stored information, including:

- i) A request may specify the *form* in which electronically stored information is produced.
 - ii) An objecting response to the *form* sought must be timely filed, and must include a *proposed form* for production of electronically stored information.
 - iii) If a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms **in which it is ordinarily maintained** or in a form or forms that are **reasonably usable**.⁷
- b) Rule 16(b)(5)& (6): Pretrial Conferences, Scheduling Management. A scheduling order may:
- i) Include provisions for disclosure or discovery of electronically stored information
 - ii) Include any agreements the parties reach for asserting claims of privilege or protection as trial-preparation material after production.
- c) Rule 26(a)(1)(B): General Provisions Governing Discovery; Duty of Disclosure; Required Disclosures; Methods to Discover Additional Matter.
A party **must now, without awaiting a discovery request, provide to other parties a copy of, or description by category and location of, electronically stored information.**
- d) Rule 26(b)(2)(B): General Provisions Governing Discovery; Duty of Disclosure; Discovery Scope and Limits; Limitations.
A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. The burden will be on the responding party to show that the information is not reasonably accessible because of undue burden or cost. Even if that showing is made, the court may order discovery from that party if the requesting party shows good cause, considering the limitations that are set . The court may also specify conditions for the discovery.
- e) Rule 26(f)(3) & (4): General Provisions Governing Discovery; Duty of Disclosure; Conference of Parties; Planning for Discovery. When parties meet and confer regarding discovery, they are to:
- i) Discuss any issues relating to preserving discoverable information
 - ii) Discuss any issues related to disclosure or discovery of electronically stored information, to include the form or forms in which electronically stored information is to be produced.
- f) Rule 33(d): Interrogatories to Parties; Option to Produce Business Records.
If an answer to an interrogatory can be found within electronically stored information, and the burden of discovering the answer is substantially the same for the responding

party and the requesting party, it will now be a sufficient answer to the interrogatory to specify the records from which the answer may be found or ascertained. The responding party will be required to allow the requesting party reasonable opportunity to examine, audit or inspect all such electronic records and make copies, compilations, abstracts or summaries.

- g) Rule 37(f): Failure to Make Disclosures or Cooperate in Discovery Sanctions; Electronically Stored Information.
If electronically stored information is lost as a result of the routine, good faith operation of an electronic information system, a court will not impose sanctions under the rules on a party whose information is lost, absent extraordinary circumstances.
- h) Rule 45 Subpoena; Form; Issuance.
A subpoena may command each person to whom it is directed to attend and give testimony or to produce and permit inspection, copying, testing, or sampling of electronically stored information. A subpoena may specify the form or forms in which electronically stored information is to be produced. Subpoenas may be served to not only inspect materials but to *copy, test or sample* those materials. Like Rule 34, if a subpoena does not specify the form or forms for producing electronically stored information, a responding party will be required to produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and a party need not produce the same electronically stored information in more than one form. The safeguards noted in Rule 26(b) are mirrored here.
- i) Form 35: Report of Parties Planning Meeting.
The form will now require inclusion of a brief description of the parties' proposals on handling the disclosure or discovery of electronically stored information.

The new federal rules make clear that electronic data in its native form is discoverable, and remove any argument that discovery is limited to compilations of that data.⁸

5) Legal Health Record & the EHR

Issues pertaining to the retention, production and validation of the legal medical or health record have been before us for many years.

There are numerous excellent resources for establishing a covered entity's designated record set.⁹ The following excerpts from the Update: Maintaining a Legally Sound Health Record—Paper and Electronic produced by the AHIMA e-HIM Work Group on Maintaining the Legal EHR point toward the problems raised here:

a) Output Format

Organization policy should determine:

- o whether the record must be complete before output is generated

- who has the authority to generate output from the EHR
- the standardized forms, formats, and order based on user needs (e.g., different views, formats, and order for lawyers, insurance companies, patients, or healthcare providers)
- what versions of documents will be provided
- a standard technology for output according to the information system capability, privacy and security standards, and user need and capability to use the format chosen

b) Printing Guidelines

The organization must define:

- the standard form and format of the paper health record
- who can reproduce paper documents for internal or external disclosure
- the scope and reasons for printing paper internally

c) Electronic Health Records

Organizations must:

- decide if they will reproduce the EHR in paper format
- determine who has the authority to print and under what circumstances
- define the form and format of documents that print from the EHR. For example, is it a screen print of the clinician view or a form that mimics the traditional paper record forms? What interval of time is printed as a standard—by encounter, date ranges, any point in time, or at discharge?
- determine which version is printed—only the most current version of a document or other versions as well. If other versions are printed, determine under what circumstances previous archived versions are printed.
- determine whether to print the traditional final lab results report versus all the preliminary results and whether lab result trends are printed.
- define what information from a shared clinical data repository can be printed
- determine if preliminary, unauthenticated reports can be printed and under what circumstances

The absence of controls, verifiable processes and replicable methodologies for producing printed versions of the electronic health record have predictably posed problems for providers and health care entities alike.

The EHR of today is so much more than the paper record of old, and the promise of even greater functionality, and benefit, to be derived from the interoperable health record envisioned by ONCHIT and others will continue to push us toward increased reliance upon electronic record systems and decreasing reliance upon the paper chart. Many entities with active EHRs in place are now abandoning paper entirely, opting for scanning to include any necessary analog data within the digital record set.

Just as numerous data sources from divergent areas have merged in today's aircraft as "flight directors" with essentially all relevant information displayed for the pilot in real-time format, with a hierarchy of displays layered to reveal the most critical information at the forefront, today's emerging electronic health records hold great promise for the delivery of evidence-based medicine with the potential for better real-time management of patients in care settings ranging from home to the NICU / ICU and all points in between.

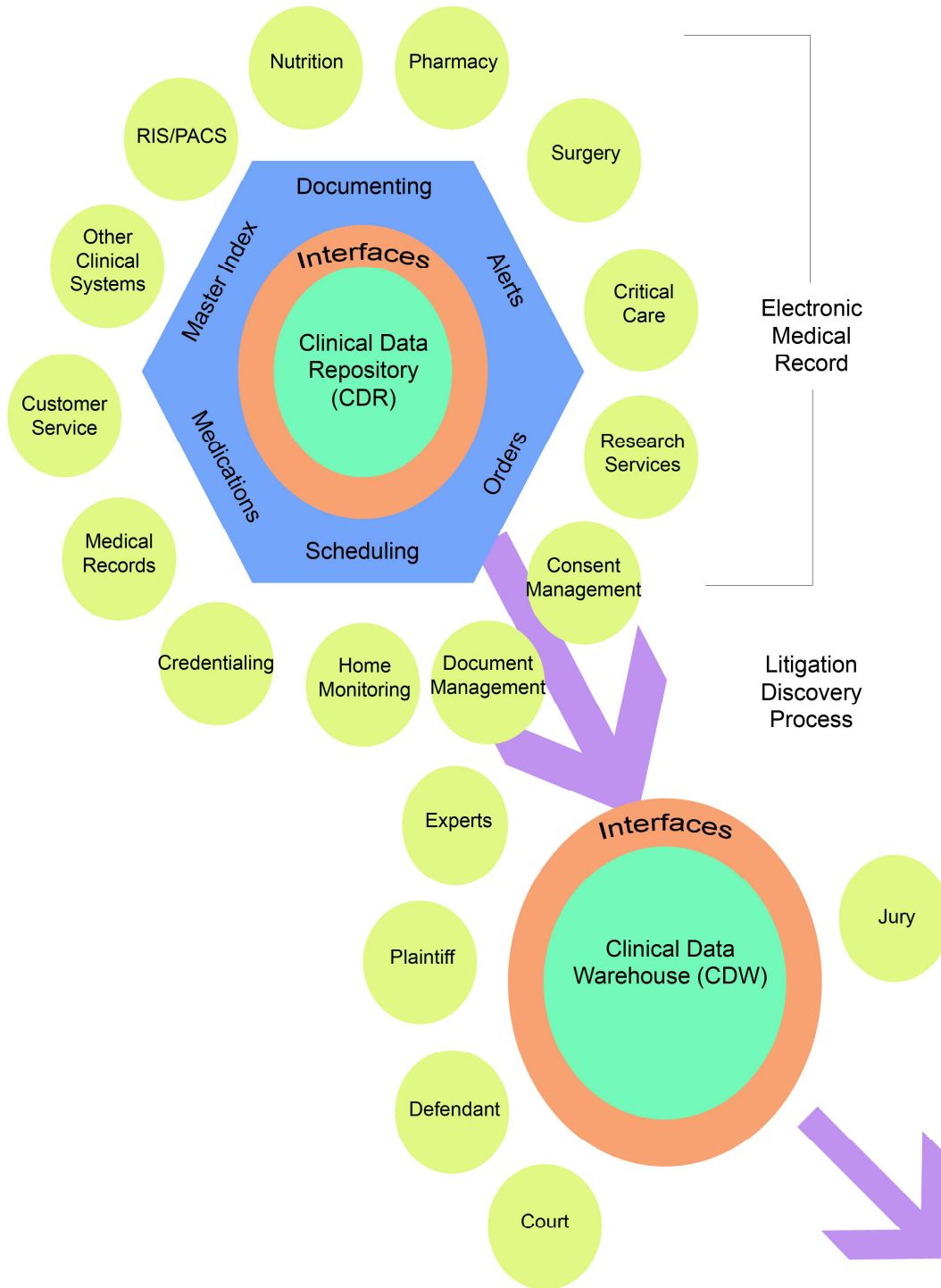
The struggle we are currently in involves the inability of a single system to fully capture all of the data emerging from these disparate systems. Many providers interface with multiple electronic systems in the course of a single day – often, for example, encountering more than one electronic health record system within a single health care system. It is not uncommon for a provider to encounter multiple electronic systems under one roof, covering the entire spectrum of care delivered by the organization, with separate interfaces for Lab, Pharmacy, Imaging, Home Health, Intensive Care, Cardiovascular ICU, OR, ED and primary acute care medical records maintained by the organization, often with an additional layer added for the organization's ambulatory care records. This may be complicated further by separate specialized systems supporting pediatric care, oncology, research, or other areas of the care spectrum.

The following chart demonstrates the problem at hand. The model shown below is representative of many health systems, in terms of the architecture of the systems and sub-systems that house elements of a typical health care organization's EHR.

From this chart, one can see that there are myriad potential collision points between the revised Civil Rules and the EHR in its present state. Each of the upper segments of this chart may:

- Represent separate, stand-alone components of the Legal Medical Record, or Designated Record Set.
- Operate entirely independently of the remaining components
- Be subject to entirely different licensing terms than its peers
- Operate under unique operating systems, interfaces or protocols
- Constitute digital, analog or hybrid record sets

SOURCES OF ELECTRONIC HEALTH RECORD DATA:



Design concept borrowed from the National Institute of Health's depiction of its Clinical Research Information System¹⁰

6) Trends

The recent changes to the Federal Rules did not happen in a vacuum. Electronic discovery has raised issues of increasing concern to both the bench and bar. While computer law has been a recognized subspecialty within the profession for the last thirty or more years, the trend of business data to increasingly reside *solely* within electronic forms has caused the courts to grapple with the impacts of the digital convergence upon traditional rules of discovery.

As the court noted in National Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1262 (E.D. PA., 1980) only .003% of the unique information produced in the world *at that time* was in print form. Consider the evolution of the computer in the last 25 years.

There are now numerous web sites focused solely on rulings by state and federal courts on matters involving electronic discovery. Because of several high profile cases arising in conjunction with widespread corporate impropriety, the courts have recognized that piecemeal approaches to electronic discovery no longer work.

For an interesting summary of several dozen e-Discovery cases in which sanctions were awarded, see Scheindlin, Shira A. and Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*.¹¹

What emerges from the Scheindlin and other innumerable reports on e-Discovery is a clear trend toward imposing sanctions whenever breaches result in actual prejudice to a party or are deemed to be *willful* or in flagrant disregard for a court or other tribunal's orders or rules.

While it may take a few years for the courts to catch up with the EHR and its progeny, and how the EHR relates to the "new and improved" CR34, it is inevitable that those health care entities who are responsible for the development and management of the EHR must eventually recognize that sharing the EHR in any format other than its native state is likely to be problematic. Paper renditions of modern EHRs are no longer acceptable as a substitution for access to the EHR itself.

7) Discussion

As so aptly noted by the AHIMA e-HIM Task Force:

From a strategic standpoint, it is important to go beyond the information creation phase and develop a plan that results in an EHR and EHR system that maintain a high level of integrity for business and legal purposes. The management of the EHR and the EHR system is and will continue to be a mission-critical function in the provision of care across the healthcare continuum. However, in today's urgency to begin deploying EHRs, healthcare entities, vendors, and others sometimes neglect to build in the processes and system capabilities needed to enable optimal EHR

management functions and ensure the electronic rather than the paper version can stand as the legal business record.¹²

EHR developers and health care professionals must collaborate to develop methodologies to mitigate concerns about the record sets being produced, providing health care providers with a solid basis from which to render testimony concerning the care provided and removing confusion and doubt from the proceedings at hand.

Careful thought must be given as to the rights currently held by end-users of EHR systems, and how those rights might be impacted by the pending changes under CR34?

For example:

- Will an end-user violate the license by displaying the EHR to unrelated party litigants or their counsel?
- Must an end-user obtain additional licenses for parties to litigation? At whose expense? Who will train such users on system nuances?
- Can duplicate or composite copies of the EHR be maintained by litigants “outside” the EHR?
- Are elements of the EHR protected by copyright, trademark or trade secrets acts that trump the rights of litigants to view the data in its native state?
- Can EHR systems be set up to view the “chart” at a point in time earlier than the current date? For example, would it be possible to “freeze” the data within the EHR effective as of a moment in time, and then allow subsequent viewers to see the chart “as if they were there” at that point in time? Would they see what the providers saw?

These questions all point toward a broader question that has yet to be resolved by EHR developers, that being: What is the “ideal” patient record?

A quick review of Google® hits on the “ideal patient record” make clear that there is little or no consensus on the definition of the ideal patient record. Instead, most references to such an ideal arise from relatively narrow points of view and become user-dependent.

Rather than looking at the chart from the perspective of the end-user, a more patient-centric approach might yield a better view of what the ideal EHR might consist of, when viewed from the perspective of CR34:

The ideal patient chart might:

- Restrict access to those with a need to know
- Allow access to those with a need to know

- Allow access to those portions of the chart that are relevant in the context of the need
- Provide a snapshot in time of the patient’s medical condition, plan of care, and health status at any given point within the care continuum

If we were to view the foregoing in a light similar to the Five Rights which we afford each patient receiving medication (right patient, drug, time, dose, route) a definition of the ideal EHR might look something like this:

- Correct patient
- Correct EHR
- Correct elements of the EHR
- Correct time frame of the EHR
- Correct recipients of the EHR

Such an approach would truly allow all litigants to see the record in its native state, providing each viewer with the tools necessary to navigate the EHR, displaying key data in the same manner as that data was displayed for the providers involved in the care of the patient.

But what about collateral data – i.e. drug-to-drug interaction data, tables, practice recommendations and other data elements contained within the “view” but maintained in separate databases? Would it also be necessary to view that collateral data in its native format? And who would maintain and archive each of these respective databases, operating systems, hardware and software, so as to ensure the ability of an end-user or otherwise authorized litigant to view such records, often years after the fact?

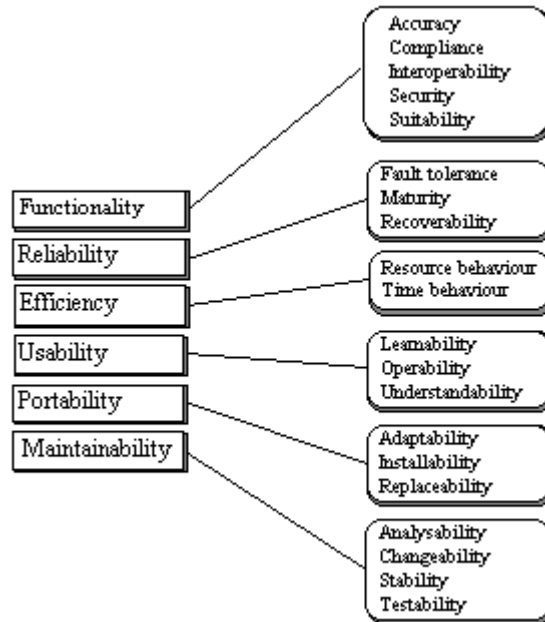
8) Strategies

The process of achieving quality software that meets all needs of all anticipated users cannot occur by happenstance. As Dave Zubrow of the Carnegie Mellon Software Engineering Institute noted, this process:¹³

- Requires planning and intentional design
- Requires more than achieving the desired functionality
- Must explicitly attend to both functional and non-functional requirements
- Requires ongoing vigilance to verify that all requirements are being met throughout the life cycle of the software

Unfortunately, most software development processes focus primarily, if not exclusively, upon achieving the desired functionality, with little if any thought as to non-functional requirements.

Standards boards have been attempting to come to grips with universal standards for software development for some time. In their article, *Evaluation of Quality Characteristics in Health Care Information Systems*¹⁴, Fabrizio Fabbrini and Mario Fusani point to the ISO/IEC 9126 Quality Model as an example of the importance of looking at software quality from the perspective of the end-user:



While health care is moving towards standards-based processes, such as HL7, there remain no government-mandated forms or formats for the exchange of PHI within and among the many electronic systems now in operation, nor is there any existing standard by which parties to health-care related litigation can presume to begin the exchange of EHR for discovery purposes.

Various entities have attempted to overcome the absence of set standards through the formation of open-platform methodologies for sharing PHI. See, for example, The Patient-Driven, Open-Source Digital Health Records Platform, A project of Harvard Medical School, MIT, and Children's Hospital Boston¹⁵

As Regional Health Information Organizations become more robust, it is likely that the role of Standards Development Organizations such as Health Level Seven (HL7¹⁶) will become increasingly important in the exchange of health data.¹⁷ Certainly a common set of data elements within the HL7 hierarchy will emerge as common touch-points between the many disparate EHR systems in place as well as those new systems likely to emerge in the coming years.

However, even if EHR systems are able to exchange data with one another, such solutions will not resolve the many issues raised for end-users of the EHR under the e-Discovery rules noted above. End-users of EHR systems must work toward educating EHR developers on the importance of developing human interfaces to the EHR that will allow for:

- Restricted access to individual patient records meeting HIPAA and State Law requirements for viewing PHI within such records
- Portability, allowing the EHR to be viewed remotely
- Context-sensitive access, allowing a view of the EHR “as it appeared” to the provider or facility at a fixed point in time
- Licensed use of, and access to, the EHR by litigants and their respective representatives, experts, the court and potentially the trier-of-fact (juries.)

It is imperative that end-users work closely with EHR vendors to develop strategies for displaying the chart in a consistent and replicable manner that most closely mimics the views of the care team involved with the patient. Such processes will enhance the ability of the trier-of-fact (juries) to fully understand and appreciate the nature and complexity of the patient’s condition and the information relied upon by the care team in establishing and maintaining the plan of care.

Health care litigation is a high-stakes activity for all parties. Forcing providers and health care professionals to testify without access to their “real” health care records (the EHR) forces them to rely upon paper records which often do not adequately portray the clinical picture that was before them at the time of the alleged incident or event, and in fact often portrays the parties in an unnatural light.

Development of interoperable health care systems will only compound the tasks at hand, as they relate to discovery. It is common for a health care provider to interface with many sources of data related to a single patient, as demonstrated on the chart above, “Sources of Electronic Health Record Data. Consider that sources of the EHR may include data from:

- Legacy systems
- Hand-held devices
- Portable electronics
- Imported data
- Imaging systems
- Pharmacy systems
- Laboratory systems
- Home Health systems

- Specialists & Subspecialists
- Multiple community sources
- Regional Health Information Organizations
- Plus the traditional “hybrid” elements arising from prior paper charts and records either maintained by the organization prior to installation of its EHR, or paper charts and records passed along to the Provider from other sources – often from other states.

Assuming these systems each contributed to the EHR, and further that each of these systems were available and on-line at the time of the litigation, it would be feasible under CR34(a) for a court to require access to the source systems depicting the patient’s chart data, and if the systems were connected and interactive or interoperable, a court may well require that the data be presented in that format.

Obviously, the complexity of dealing with these many potential points of failure will be a challenge for courts and litigants for many years to come. One commentator has referred to the new discovery rule as the “Chernobyl” of Information System management.¹⁸

To avoid potentially large sanctions, end-users must now get on their EHR vendor’s list of serious development objectives addressing not only their operational and functional needs within the context of the EHR, but also the business needs triggered by the EHR under CR34 and other applicable discovery rules.

Healthcare organizations need to analyze and assess all downstream uses of EHRs and see those uses reflected in requests for proposals, system selection, development, installation, and implementation in order to ensure that all needs of the organization are met.¹⁹

9) Conclusion

Continued reliance upon historic methods of producing paper / print copies of a patient’s electronic medical record in the context of litigation are no longer warranted.

Changes in discovery rules currently in process at the federal level are highly likely to be mimicked at the state level in the very near future. Many states already have electronic discovery rules that are substantially similar to the Federal Civil Rules amendments noted above.²⁰

Software tools that will enable third parties involved in litigation to access and view EHR data are not yet in development, in most instances. Such tools may take several years to develop and refine to the point where they can be used in the ordinary course of discovery.

Unless EHR developers recognize the criticality of these tools as part of the “minimum functionality” of an EHR, they will have no motivation or incentive to make the changes needed to allow end-users to fully comply with the emerging discovery rules for e-

Discovery in the 21st Century. 19th Century methods for sharing information among parties are no longer logical or suitable.

Licensing, copyright, trademark and trade secret issues must be overcome, along with appropriate privacy and security issues applicable to dissemination of the EHR in litigation.

Teaming together with other similarly-situated EHR end-users may provide end-users with the voice and consistency of approach needed to marshal the enormous resources that will be required to append these tools to existing EHRs in operation, and to ensure that new releases continue to address the discovery needs of the organizations, large and small, that will be in increasing reliance upon their EHR systems as tools for the effective management of their health care operations.

In the meantime, end-users must work closely with the courts and opposing parties to demonstrate best efforts in complying with the spirit, if not the letter, of the emerging rules of e-Discovery as they apply to the EHR.

10) Other Resources: [Also See 10A Below]

AHIMA e-HIM Work Group on Defining the Legal Health Record. "The Legal Process and Electronic Health Records." *Journal of AHIMA* 76, no.9 (October 2005): 96A-D. [expanded online version]

Amatayakul, Margret et al. "Definition of the Health Record for Legal Purposes (AHIMA Practice Brief)." *Journal of AHIMA* 72, no.9 (2001): 88A-H.

Anderson, Ellen M., "Online Clinical Documentation in the Electronic Legal Medical Record." 2004 IFHRO Congress & AHIMA Convention Proceedings, October 2004

Bakker, Ab, "The Need for a Time Machine in the Distributed EHR." 2004 IFHRO Congress & AHIMA Convention Proceedings, October 2004

Dougherty, Michelle. "Understanding the EHR System Functional Model Standard." (AHIMA Practice Brief) *Journal of AHIMA* 76, no.2 (February 2005): 64A-D.

Gasser, Urs and Domino Burki, as posted at Harvard Workshop, Law & Technology of Digital Information Management: Promises, Challenges, and Perspectives Observations in the Aftermath of an Interdisciplinary Workshop, <http://cyber.law.harvard.edu/eon/SummaryFIR-CSGWorkshop.pdf>

Kohn, Deborah. "When the Writ Hits the Fan." *Journal of AHIMA* 75, no.8 (September 2004): 40-44.

Raw. Josephine, "Going Paperless: Dreams and Reality." 2004 IFHRO Congress & AHIMA Convention Proceedings, October 2004

Rhodes, Harry and Michelle Dougherty. "Document Imaging as a Bridge to the EHR (AHIMA Practice Brief)." *Journal of AHIMA* 74, no.6 (June 2003): 56A-G.

Tomes, Jonathan P. "Spoliation of Medical Evidence." *Journal of AHIMA* 76, no.9 (October 2005): 68-72.

Williams, Adrian. "Design for Better Data: How Software and Users Interact Onscreen Matters to Data Quality." *Journal of AHIMA* 77, no.2 (February 2006): 56-60.

Biography:

Laird A. Pisto is Associate General Counsel at MultiCare Health System, in Tacoma, WA, where he has supported MHS' Integrated Delivery Network of two adult acute care hospitals, one pediatric acute care hospital and several dozen clinics, ambulatory surgery centers and related ancillary services and support for the past six years. He previously served as Ass't Gen'l Counsel to Catholic Health Initiatives in its Western Region offices, supporting several hospitals and health systems in the Northwest. As General Counsel for Care Computer Systems, he supported the expansion of what was then the largest provider of software to the long term care industry in the United States. He maintained a general litigation practice in South King County, WA., for a dozen years after leaving an in-house counsel position with Pan American World Airways where he began his legal career. Married, with two adult children, he enjoys as much time away from the office as he is allowed (not much!) skiing, road bicycling and traveling.

Laird A. Pisto

MultiCare Health System

PO Box 5299

315 Martin Luther King Jr. Way

Tacoma, WA 98415-0299

253-403-1186

Laird.Pisto@multicare.org

10A SUPPLEMENTAL MATERIALS & RESOURCES January 2007

Summaries of the e-Discovery Rules:

<http://www.ediscoverylaw.com/2006/11/articles/federal-rules-amendments/a-complete-set-of-the-pending-ediscovery-amendments/>

K&L | Gates A Complete Set of the Pending E-Discovery Amendments

<https://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp>

LexisNexis Applied Discovery Site: Court Rules

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031860.hcsp?dDocName=bok1_031860

AHIMA HIM Body of Knowledge FORE Library: The New Electronic Discovery Civil Rule

<http://soundevidence.discoveryresources.org/cat-rules-legislation.html>

Discovery Resources / Sound Evidence: Court Rules

<http://www.ironmountain.com/knowledge/ediscovery/index.asp>

Iron Mountain: Knowledge Center eDiscovery Rules

http://www.dwt.com/related_links/adv_bulletins/12-06_FRCPAmendments.htm

Davis Wright Tremaine FRCP Amendments

<http://acc.com/php/search.php>

Association of Corporate Counsel Articles:

The New Federal eDiscovery Rules: How Your eDiscovery and eRecords Management Practices Should be Revised for Compliance

<http://www.arma.org/profiler/ediscovery.cfm>

ARMA Risk Profiler Self-Assessment for E-Discovery

E-Discovery Whitepaper In Process: AHLA Member Briefing Will Discuss Many Evolving Issues (Spring '07):

1. Federal Rules Changes

- 1.1. High Level Summary of FR CivP Rules Amendments
- 1.2. History
- 1.3. Third-Party Resources

2. Case Law

- 2.1. Key e-Discovery Cases
- 2.2. Sanctions Imposed
- 2.3. Best Practices
- 2.4. Pitfalls

3. Educating Management & Outside Counsel

- 3.1. What Should Every Board of Directors Know?
- 3.2. What Should Management Know?
- 3.3. What Should Every CIO Know?
- 3.4. What Should Every Outside Attorney Know?
- 3.5. Connecting IS/IT with Outside Counsel?

4. Witness Preparation

- 4.1. Has Anything Changed?
- 4.2. Working With Primary Source Data vs. Paper?
- 4.3. Familiarity With Process of Conversion (Digital to Paper, etc.)
- 4.4. Limitations of Print vs. Online Versions of Charts & Records

5. Developing & Managing An Inventory of Electronic Sources

- 5.1. Primary Records Systems
- 5.2. Recovery / Backup / Secondary Systems
- 5.3. Transient Systems
- 5.4. Overlapping / Duplicative Data
- 5.5. Hand-Helds, PDAs, Blackberry Devices
- 5.6. Home computers
- 5.7. Internet & Intranet Sites / Workgroups
- 5.8. Third Party Records?
 - 5.8.1. Employees
 - 5.8.2. Agents
 - 5.8.3. Contractors
 - 5.8.4. Vendors
 - 5.8.5. Trade Organizations

- 5.8.6. Quality Oversight Agencies
- 5.8.7. Auditors
- 5.8.8. Regulators
- 6. Building & Maintaining A Disclosure Catalog – Metadata**
 - 6.1. Minimum Data Set Required?
 - 6.2. Manual or Automated Processes?
 - 6.3. Retroactive Effect? What must be built now?
 - 6.4. Custodian?
- 7. Managing Relevance & Timeliness**
 - 7.1. Managing Relevance Against Automatic Required Disclosures
 - 7.2. Context of Litigation, Claim or Known Unanticipated Outcome or Occurrence
 - 7.3. Early Evaluation As To Scope
 - 7.4. Timeliness – 90 Day Rule
- 8. Preservation of Data**
 - 8.1. Managing a Litigation Hold
 - 8.2. Documenting Record Retention Practices
 - 8.3. Permanent Data Elements? Destruction Archives?
 - 8.4. Managing “Pending” or “Threatened” vs. “Actual” Litigation
- 9. Privilege**
 - 9.1. Maintaining Attorney-Client Privilege
 - 9.2. Peer Review
 - 9.3. Quality Assurance
 - 9.4. Physician-Patient
 - 9.5. Developing Privilege / Work Product Agreements With Opposing Counsel
- 10. Handling Special Categories of Data**
 - 10.1. HIV / AIDS
 - 10.2. Drug & Alcohol Treatment
 - 10.3. Mental Health
 - 10.4. STDs
 - 10.5. Employment
 - 10.6. Workers Compensation
 - 10.7. Human Subjects Research Records
 - 10.8. Other
- 11. Native Format Disclosures**
 - 11.1. When Paper Just Doesn’t Work?
 - 11.2. Producing Data in Electronic Form – What Is New or Different?
 - 11.2.1. What About Evolving Records – i.e. Patient Chart With Ongoing Updates?

- 11.2.2. Demonstrating Chart or Record Status On Date Certain vs. Current Date
- 11.2.3. Documenting What Was Produced
- 11.2.4. Testing
- 11.2.5. Control Sets
- 11.2.6. Archives
- 11.3. Best Practices
 - 11.3.1. During Discovery Phase
 - 11.3.2. In Court or Deposition Settings
 - 11.3.3. Connecting Analog Output (Paper) to Digital Source (Native)
- 11.4. Processes For Controlling & Documenting Native-Format Discovery Forays?
 - 11.4.1. Documentation of Processes?
 - 11.4.2. How Much Help Is Required?
 - 11.4.3. “Providing Trained Operator?” or “Not”?
 - 11.4.4. Indexing?
 - 11.4.5. User Guide?
- 11.5. Access to Metadata Within Native Format Content?
 - 11.5.1. Audit Trails
 - 11.5.2. Amendments
 - 11.5.3. Modifications
- 11.6. Incomplete Sets?
- 11.7. Works in Process?

12. HIPAA

- 12.1. Managing Disclosures Against the Minimum Necessary Rule
- 12.2. Distinguishing “Designated Record Set” from “Legal Medical Record”
- 12.3. Expansion of Duties of Designated Privacy / Security Officer Roles?

13. Reasonable vs. “Unreasonable” Discovery Requests

- 13.1. Identifying Reasonable Access Pathways
- 13.2. Identifying “Unreasonable” Pathways in Advance
- 13.3. Documenting Basis For Unreasonableness
- 13.4. Advance Planning
- 13.5. Cost Shifting – Who Bears Burden Now?

14. Inadvertent Disclosures – Overbreadth Responses

- 14.1. Cataloging Inadvertent Disclosures
- 14.2. Responding / Follow-Up to Inadvertent Disclosures
- 14.3. Link to HIPAA
- 14.4. Developing Work Plan / Documentation With Opposing Counsel

15. Attestation & Validation of Completeness

- 15.1. New Meaning?
- 15.2. Best Practices
- 15.3. Inventory / Checklist
- 15.4. Disclaimers in Attestation?
- 15.5. Knowledge of Records Custodians vs. IS/IT Functions?

16. Legal Medical Record

- 16.1. Best Practices -- Defining the Legal Medical Record
- 16.2. Distinguishing from HIPAA Designated Record Set (see above)
- 16.3. Tying to State Law Requirements
- 16.4. Third Party Resources (AHIMA, etc.)

17. Safe Harbors

- 17.1. Compliance Plan Applicable to All Business Records
- 17.2. Hold Management / Automated Processes
- 17.3. Best Practices
- 17.4. Inadvertent Destruction or Loss
- 17.5. "Good Faith" Efforts

18. Security Standards

- 18.1. Role of Security in Safe Harbor / Best Practices
- 18.2. Documenting Security Processes
- 18.3. Audit Trails
- 18.4. Primary vs. Secondary Data Sources

19. Hardware & License Retention

- 19.1. How Long Should Hardware Be Retained?
 - 19.1.1. Plan of Retention
 - 19.1.2. Operability
 - 19.1.3. Operator Currency (Training & Support of Non-Functional Systems?)
- 19.2. How Long Should Licenses Be Maintained?
 - 19.2.1. Allow for non-productive use?
 - 19.2.2. Allow disclosure to third parties?
 - 19.2.3. Perpetual? Limited?
- 19.3. Archival Data – In Non-Native Formats?

20. Information Management Plan

- 20.1. Best Practices In Developing Information Management Plan
- 20.2. Who Should Be Involved?
- 20.3. Who Owns Process?
- 20.4. Disaster Recovery / Business Continuity

21. Compliance

- 21.1. Role of Compliance Department
- 21.2. Audits
- 21.3. Control Processes
- 21.4. Authentication of Automated Routines for Backup, Retention & Litigation Hold Management
- 21.5. Sarbanes – Oxley
- 21.6. JCAHO

22. Managing Information System Vendors

- 22.1. Role of Third Party Vendors?
- 22.2. Contract Issues
 - 22.2.1. Importing / Exporting Data
 - 22.2.2. Standard File Formats
 - 22.2.3. Standard Data Elements
 - 22.2.4. Data Portability
 - 22.2.4.1. Entire Record Set?
 - 22.2.4.2. Partial?
- 22.3. Defining Vendor Role(s) In Discovery & Retention Process

23. Using Discovery Service Vendors

- 23.1. Best Practices
- 23.2. Selecting Vendors
- 23.3. Selecting Systems
- 23.4. Authenticating Output
- 23.5. Testing Assumptions
- 23.6. Auditing Work Performed

24. State Law Requirements

- 24.1. Statutory Requirements By Jurisdiction
- 24.2. Case Law Supplements – key e-Discovery Cases

25. Employer Sponsored Electronic Health Records

- 25.1. Special Rules?
- 25.2. Distinguish from Provider Records?

Zenith Radio Corp. v. Matsushita Electric Industrial Co

But no one has been as diabolical as Judge Edward R. Becker, who imposed the "Time Out Rule" in *Zenith Radio Corp. v. Matsushita Electric Industrial Co.*, 478 F. Sup. 889, 959 (E.D. Pa. 1971). In this 71-page opinion in a complex anti-trust case, Judge Becker first disposed of pending motions and entered a comprehensive pretrial order setting deadlines for completion of discovery, expert witness dispositions, pretrials, trial and all other conceivable aspects of the case. Then, seemingly as an afterthought, he added the "Time Out Rule as Appendix B:

"Time Out Rule"

"A. Statement of Rule.

For no good cause shown each side will be entitled to three time outs between now and the date of trial. A time out is defined as a one-week period in which no discovery can be served, all deadlines are postponed and counsel can generally goof off.

1. The procedure for calling a time out will be as follows:

Both plaintiffs and defendants will designate one individual as the official time out persons (hereinafter referred to as the "Designated Whistler"). The designated whistler will be issued a whistle from the case liaison logistics committee which will be strung around his, her, or its neck. When a time out is desired, the designated whistler will go to the offices of opposing lead counsel (See XVLE.) and blow the whistle three times. Thereafter there will be a one-week time out.

2. As stated above, each side is entitled to three time outs. However during the period of the two month warning (see B below) each side will be entitled to only one time out, providing that side still has remaining at least one time out.

3. Time outs must not be called on two consecutive one-week periods. That is there must be an intervening week between time out periods. This rule is designated to prevent counsel from spending more than one week of their time with their family, friends, partners and associates.

4. As stated above, each side will be entitled to only three time outs. Any attempt by any side to exceed this three time out limit will be regarded by the Court as a serious infraction of the rules (hereinafter 'illegal use of whistle'). The sanction for illegal use of whistle will be that such counsel attempting to exceed the three time outs will have his, her or its desk moved five yards (in the event of a non-flagrant violation) or 15 yards (in the event of a flagrant violation) further from the jury box at trial.

"B. Two Month Warning.

As stated above, there will be a two-month warning. Such a two-month warning will be called by the Court two months prior to trial. At this point there will be a three day stoppage of the clock in which all counsel will be required to get their personal affairs in order. Personal affairs will include such items as Last Will and Testament, final instructions to spouse and family, arrangements for publication of memoirs and other less important details. During the two month warning, the clock will run continuously except for time outs described in A above." (478 F. Supp. at 959-60).

http://www.texasbar.com/saywhat/weblog/buchmeyer_article_archive/Feb83.asp

As cited by US District Judge Jerry Buchmeyer, "Discovery Abuse & The Time Out Rule"

End Notes:

¹ AHIMA e-HIM Work Group on Maintaining the Legal EHR. "Update: Maintaining a Legally Sound Health Record—Paper and Electronic." *Journal of AHIMA* 76, no.10 (November-December 2005): 64A-L. This updates the 2002 source document on the same topic.

² Retrieved from "http://hcs.harvard.edu/~cyberlaw/wiki/index.php/Sedona_Principles"

Sedona Conference, Berkman Center for Internet & Society, Cyberlaw/Evidence/Biotech 2006 wiki , external web site, 3/10/06. Produced by the Sedona Conference think tank, this document seeks to present party-neutral guidelines that could be applied to the facts of specific litigation matters.

³ 45 C.F.R. §164.524. See also 45 C.F.R. §164.526

⁴ See JCAHO Information Management standards. I.M.1.10, I.M.3.10. Copyright, Joint Commission on Accreditation of Healthcare Organizations, Accreditation Manual for Hospitals: The Official Handbook, CAMH 2006:

- Information Management processes are designed to meet *internal* as well as *external* information needs.
- Information Management processes are in place to manage information, including the capturing, reporting, processing, storing, retrieving, disseminating and displaying of clinical and non-clinical data and information.

⁵ <http://www.uscourts.gov/rules/index.html#supreme0406>

⁶ Note: The amendments to Rule 34 and other rules contained within the Federal Rules of Civil Procedure include numerous other amendments beyond the scope of this memorandum, particularly relating to Attorney-Client Privilege and Work-Product materials. See:

Rule 26(b): General Provisions Governing Discovery; Duty of Disclosure; Discovery Scope and Limits; Claims of Privilege or Protection of Trial Preparation Materials; Information Produced.

Because of the breadth of changes to Rule 34(a), amendments to Rule 26(b) are proposed to ameliorate against the likely inadvertent disclosure of Attorney-Client Privileged or Work-Product documents when opposing parties are afforded access to e-Discovery materials now mandated under Rule 34. Rule 26 will now provide that if information is produced in discovery that is subject to a claim of privilege or protection, the party making the claim may notify any party that received the information of the claim and the basis for it. After notification, the receiving party will be required to promptly return, sequester, or destroy the specified information and any copies it has and will not be able to use or disclose the information until the claim is resolved. A receiving party can present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it will be required to take reasonable steps to retrieve it. The producing party will be required to preserve the information until the claim is resolved.

http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf

⁷ <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf#page=155>

⁸ Isom, David, Electronic Discovery Primer for Judges, 2005 Fed. Cts. L. Rev. 1

http://hcs.harvard.edu/~cyberlaw/wiki/index.php/Isom%2C_Digital_Discovery_Primer

⁹ See footnote 1 above.

-
- ¹⁰ Model derived from depictions of the NIH Clinical Research Information System – CRIS <http://cris.cc.nih.gov/public/gfx/architecture.gif>.
- ¹¹ 11 Mich. Telecomm. Tech. L. Rev. 71 (2004), also available at <http://www.mttr.org/voleleven/scheindlin.pdf>
- ¹² AHIMA e-HIM™ Task Force. "The Strategic Importance of Electronic Health Records Management." *Journal of AHIMA* 75, no.9 (October 2004): 80A-B.
- ¹³ Zubrow, Dave, Carnegie Mellon Software Engineering Institute, June 14, 2004, as posted at: <http://www.sei.cmu.edu/sema/presentations/zubrow/esepeg/sld016.htm>
- ¹⁴ Fabbrini, Fabrizio and Mario Fusani, Evaluation of Quality Characteristics in Health Care Information Systems, ERCIM News No.28, January 1997
- ¹⁵ <http://ping.chip.org/> PING personally controlled health record. A project of Harvard Medical School, MIT, and Children's Hospital Boston
- ¹⁶ HL7 is a trademark of Health Level Seven, Inc., an ANSI-certified SDO. <http://www.hl7.org/>
- ¹⁷ For a comprehensive list of Standards Development Organizations involved in health data standards, see: <http://faculty.washington.edu/ocarroll/infrmatc/database/data/players.htm>
- ¹⁸ Schwartz, Ephraim, Document management systems go to court: New federal rules for 2006 could come down hard on IT, http://www.infoworld.com/article/05/12/27/01OPreality_1.html
- ¹⁹ See Strategic Importance of Electronic Health Records Management, supra.
- ²⁰ States such as Delaware, Kansas, Mississippi and Texas have e-Discovery rules in place. Other states such as Arkansas, New Jersey and Wyoming have local Federal rules and/or local state e-Discovery rules in place, covering elements of these rule changes.