The Sedona Conference Journal

Volume 9 2008

E-Discovery in Healthcare & Pharmaceutical Litigation: What's Ahead for ESI, PHI & EHR?

Kevin F. Brady, Amor Esteban,
Ronald J. Hedges & Katherine L. Ball

Recommended Citation: Kevin F. Brady et al., *E-Discovery in Healthcare & Pharmaceutical Litigation: What's Ahead for ESI, PHI & EHR?*, 9 SEDONA CONF. J. 167 (2008).

For this and additional publications see:
https://thesedonaconference.org/publications

E-DISCOVERY IN HEALTHCARE & PHARMACEUTICAL LITIGATION: WHAT'S AHEAD FOR ESI, PHI & EHR?[1]

Kevin F. Brady, Connolly Bove Lodge & Hutz, LLP
Wilmington, DE

Amor Esteban, Shook Hardy & Bacon, LLP
San Francisco, CA

Ronald J. Hedges, Nixon Peabody, LLP
New York, NY

Katherine L. Ball, MD, MSC,
Johns Hopkins University, School of Medicine,
Baltimore, MD

I. INTRODUCTION

The management of electronically stored information (ESI) is a major priority for most businesses today. In the healthcare industry, the management of protected health information (PHI)[2] is not only a major priority; it is of paramount concern.

The management of electronically stored protected health information (e-PHI)[3] presents a unique set of challenges not faced by most businesses. E-PHI, like business ESI, is dynamic in nature, and it has several characteristics that mandate special treatment not encountered in personal financial information. Through the Health Insurance Portability and Accountability Act (HIPAA), PHI is subject to added regulatory and security requirements, and the uses and potential consequences for misuse of PHI pose significant clinical, ethical and legal ramifications that may have far-reaching and more significant consequences than the risks faced by businesses with regard to the misuse of ESI.

To illustrate, when businesses' or individuals' financial information is lost or misused, they may likely be made whole through monetary damages supported by various jurisdictional laws. The ramifications resulting from the loss or misuse of an individual's PHI may not be so easily remedied. An individual whose PHI is inaccurate, unavailable or inaccessible could face severe consequences. For example, if a physician relies upon a medical record that contains inaccurate PHI (such as medication or allergy profile); the physician could make a clinical decision that results in harm or death to a patient.

1 The authors wish to acknowledge with sincere gratitude the assistance of Kimberly Baldwin-Stried Reich. Her contributions and insights with respect to complex issues related to the healthcare field were invaluable.

2 P.L. 104-191 – Sec. 1171(A) - Health Insurance Portability and Accountability Act (HIPAA) of 1996 defines protected Health Information (PHI) as "Any information in any form or medium created or received by a health provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. "

3 For purposes of this paper E-PHI is defined as Protected Health Information stored or maintained in electronic form; this is a subset of PHI.

Even with such risk, many Americans, policy makers[4] and academics[5] believe health information technologies (HIT) and electronic health record systems (EHRs) will improve the access and availability of clinical information and improve healthcare quality at the same time. In May 2008, the Congressional Budget Office issued a report on costs and benefits of HIT[6] that generally concludes that HIT has the potential to significantly increase the efficiency of the healthcare industry by helping providers manage information. Despite the advancements HIT and EHRs promise, consumer groups and others have significant concerns regarding privacy and security of their PHI, as such, they are reluctant to support healthcare initiatives that call for the exchange of e-PHI over the internet without scrutiny.[7] The perceived lack of trust consumer groups and others have in HIT and EHRs is not unfounded; the risks of loss, misuse of a patient's e-PHI or the failure of the EHRs are very real.

This paper will examine a few selected issues that are unique to e-discovery in healthcare litigation and will suggest how to plan ahead to avoid the traps and pitfalls that can arise. Even though a great deal has already been written about e-discovery, the healthcare industry is just coming to grips with the management of e-PHI. This paper is intended to serve as a foundation for dialogue as to how healthcare enterprises, through their in-house and outside counsel, IT, risk management, health information professionals, and compliance officers may begin to address issues of e-discovery and e-data management in the healthcare field.

Emerging legal issues related to ESI and e-PHI in the healthcare industry (the largest industry in the United States)[8] are not being addressed and are not even "on the radar" as an issue of importance in most healthcare organizations and their regulatory agencies.[9] Simultaneously, great pressures are being placed on healthcare organizations and providers by multiple external forces (e.g., federal and state government[10], business consortia[11], consumer advocates[12], and third party payers) to adopt electronic health records, computerized provider order entry, personal health records (PHR), electronic prescribing and other health information technologies, at a time when a comprehensive understanding of the emerging legal issues related to e-PHI contained in EHRs is lacking.

While leaders in health information management such as American Health Information Management Association (AHIMA) have taken notice of changes in electronic discovery laws[13] and the best practice recommendation of The Sedona Conference®[14] much work needs to be done to find significant organizational solutions which recognize the complexities of navigating an exceedingly regulated healthcare industry.

A fundamental problem is that there exists no single definition of what constitutes a record. A record is generally defined as a complete set of information required to provide evidence of a business transaction. However, the definition of a "record" has become increasingly more complicated as the healthcare industry moves from paper to electronic media to perform transactions. Defining and managing the disparate elements of the legal electronic health record for disclosure or discovery is no easy task for a health service organization (HSO) whether a large hospital or a small private practice deploying HIT.

---

4 *See*, Smith, V. K., K. Gifford, S. Kramer, et al. "State E-Health Activities in 2007: Findings from a State Survey." The Commonwealth Fund. February 2008. Available at www.commonwealthfund.org/publications/publications_show.htm?doc_id=669309 Accessed 6/22/2008; and Blumenthal, D. "Health Information Technology: What Is the Federal Government's Role?" The Commonwealth Fund, Commission on a High Performance Health System. March 2006. Available at www.commonwealthfund.org/usr_doc/Blumenthal_HIT_907.pdf?section=4039. Accessed 6/22/2008; eHealth Initiative Policy > Congress: Current Legislation. Available at http://www.ehealthinitiative.org/policy/ . Accessed 6/22/2008

5 Institute of Medicine (U.S.). Committee on Quality of Health Care in America. Crossing the quality chasm : a new health system for the 21st century. Washington, D.C.: National Academy Press; 2001.

6 Congressional Budget Office - Evidence on the Costs and Benefits of Health Information Technology . Available at http://cbo.gov/doc.cfm?index=9168

7 http://www.patientprivacyrights.org/

8 BEA: News Release: Gross Domestic Product.Available at:http://www.bea.gov/newsreleases/national/gdp/gdpnewsrelease.htm.

9 Even basic issues such as the scope of attorney-client privileged communications have crept into the legal-healthcare relationship. In *Scott v. Beth Israel Med. Center Inc.*, 2007 WL 3053351 (N.Y. Sup. Ct. Oct. 17, 2007), a physician sued the hospital for breach of contract based upon the hospital terminating his employment. The physician used the hospital's computer system to communicate with his lawyer about his employment situation. When the hospital discovered the emails on its system, it informed the physician who claimed that they were privileged. The hospital disagreed and refused to return the emails referencing its email policy which stated, among other things, that electronic mail systems were property of the hospital and that employees "have no personal privacy right in any material created or received" on the hospital's computer systems. The Court agreed with the hospital and found that the communications were not privileged.

10 Health Information Technology. Available at: http://www.hhs.gov/healthit/community/background/. Accessed 3/27/2008.

11 *See*, eHealth Initiative's Blueprint: Building Consensus for Common Action. Available at:http://www.ehealthinitiative.org/blueprint/. Accessed 3/27/2008; and Markle Foundation. Available at: http://www.markle.org/. Accessed 3/27/2008; and The Leapfrog Group - About us. Available at: http://www.leapfroggroup.org/about_us. Accessed 3/27/2008.

12 *See*, Bridges to Excellence. Available at: http://www.bridgestoexcellence.org/. Accessed 3/27/2008; and National Patient Advocate Foundation - A National Network For Healthcare Reform. Available at: http://www.npaf.org/.

13 *See*, Baldwin-Stried K. E-Discovery and HIM: How Amendments to the Federal Rules of Civil Procedure Will Affect HIM Professionals. *Journal of AHIMA* October 2006;77(9):58-60ff; and AHIMA e-discovery e-HIM Workgroup. "The New Electronic Discovery Civil Rule." J. AHIMA October 2006;77(8).

14 Quinsey, Carol Ann. "Digital Disclosure and Discovery: the Sedona Conference Counts the Ways that Electronic Documentation is Different." *Journal of AHIMA* 78, no.8 (September 2007): 56-57.

To encourage accurate reporting and clinical trial participation, the FDA requires that names or other information, which would identify patients or research subjects in any medical or similar report, test, study, or other research project, be deleted before the record is made available for public disclosure, 21 C.F.R. 20.63(a). The FDA also requires that the same information be deleted from any record before it is submitted to the FDA. 21 C.F.R. 20.63(b). On July 3, 1995 the FDA adopted yet a third privacy regulation to enhance protection of the identities of voluntary reporters and patients experiencing adverse events that are the subject of voluntarily submitted adverse reports concerning human drugs, biologicals and medical devices. 21 C.F.R. 20.63(f).[15]

The risks to parties that administer ePHI today are much greater than they were in 1995 when 21 C.F.R 20.63 was put into effect or even 1996 when HIPAA was enacted. Media reports and privacy clearinghouses[16] are widespread with publications of data breaches of ePHI. For example, in reviewing data from colleges and universities in 2007, 112 different educational institutions reported a total of 139 different educational security incidents.[17] These 139 incidents lead to the exposure of 1,245,668 records containing at least one type of sensitive and/or personal information.[18] If that is not enough of a concern, the number of incidents reported by institutions of higher education rose 67.5% over 2006. Personal identifiable information ranked as the most common type of information exposed by information security incidents at colleges and universities.[19] There were 129 incidents that exposed 1,244,851 records containing personally identifiable information. With respect to EHR alone, there were 15 incidents, which exposed a total of 60,822 records containing such medical information such as diagnosis and treatment information.[20]

With health information security breaches on the rise, the government through Health and Human Services, Office of the National Coordinator (ONC) has turned its attention to preventing medical identity theft. ONC is responsible for coordinating the federal initiatives to adopt healthcare information technology and creating a nationwide health information network for the electronic exchange of medical data. Most recently in May 2008, the ONC Commissioned Medical Identity Theft Assessment which has been charged with focusing on the intersection of health IT, medical identity fraud of personal health identifiable information.[21]

In an article "Medical Identity Theft: The Information Crime That Can Kill You"[22] it was reported that between January 1, 1992 and April 12, 2006, the Federal Trade Commission received complaints from 19,428 individuals about medical identity theft. Faced with a greater risk when dealing with EHR, should healthcare enterprises be held to a higher standard than a company that does not handle EHR or PHI? Should, for example, EHR be given the same level of protection that the company's trade secrets are?

II. PERSONAL HEALTH RECORDS AND ESI

Given the great concern many Americans have with exposing their PHI to security breaches on the Internet, how would you expect residents in "Our City" to react to the following email:

> Dear My**Chart** User:
>
> Recently Our City Clinic began working with Goggle - the world's leading internet search company - to support a new product Google will be launching that will help patients manage their medical records and personal health information online.
>
> You already know the benefits of managing your medical records online because you have experienced the power of a secure, online service that connects you to your healthcare provider whenever and wherever you choose because you are a member of the Our City Clinic My**Chart** community. What you may not know is

15 See *In re Medtronic,* 184 F.3d 807, 808 (8th Cir.1999) (reversing an order which granted plaintiff's request to discover the names of patients, physicians and facilities involved with other allegedly defective Medtronic pacemakers.); *Adcox v. Medtronic*, 131 F.Supp. 2d 1070 (E.D. Ark. 1999) (in accord) *Contratto v. Ethicon*, 225 F.R.D. 593 (N.D. Cal. 2004), (in accord).
16 Privacy Rights Clearing House : List of Data Breeches. Available at http://www.privacyrights.org/
17 Educational Security Incidents (ESI) Year in Review – 2007 at 11. Available at: http://www.adamdodge.com/esi/yir_2007 . Accessed 3/31/08.
18 Id.
19 Id. at 26.
20 Id. at 25.
21 Health Information Technology: ONC Commissioned Medical Identity Theft Assessment . Available at: www.hhs.gov/healthit/privacy/identytheft.html. Accessed, 6/19/08
22 "Medical Identity Theft: The Information Crime That Can Kill You" Pam Dixon, World Privacy Forum, May 3, 2006. Available at: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf Accessed 3/31/2008.

that these types of online tools are not available to Americans at large. This is why your unique My**Chart** experience makes your opinions regarding online healthcare management tools very important and why we need your help.

We are inviting a select number of My**Chart** users to try the new Google product and offer confidential feedback. The new Google product is being privately piloted at Our City Clinic and is available nowhere else at this time. At Our City Clinic, we believe that the level of service and convenience you experience as a My**Chart** user should serve as the model for all patients everywhere and that is why we are working with Google.

Sincerely,
Your Our City Clinic My**Chart** Service Team

Whether consumer forces, market necessity, public policy, good patient care, or patient empowerment, the advent of personal health records (PHRs) like the partnership between Google and the Our City Clinic is here to stay. Many of the available PHRs allow for uploading or importing of EHR records from hospitals and provider based electronic health repositories. The impending proliferation of PHR mandates new responsibilities for health information professionals and legal counsel deciding on how to verify accuracy of information no longer under provider or health service organization (HSO) control.

Not only have well recognized organizations like Goggle and Microsoft (HealthVault) entered into the PHR market, employers, payers, consumer and other market influences have also established a product presence using e-PHI. See Table 1 for a sample list of PHRs products presently available.

AHIP PHR Standards	KIS Medical Records	MyMedicalRecords.com
Allscripts Patient Portal	LAXOR	MyMedicare.gov
Angel Key	LifeLedger	myNDMA
Band of Life	LifeSensor	myuhc.com
Benefits Manager (American Airlines)	MedCard Online/Med-Id-Card	NoMoreClipboard.com
CapMed	MedCommons	PHR4me
Care Memory Band	MedDataNet	PatCIS
Chart Scout	MedeFile	Pathway Technology
CheckUp	Medic Tag	PatienTrak
Dr. I-Net	Medical Passport	Patient Power
E-HealthKEY (MedicAlert)	MedicAlert	Peoplechart
EMRy Stick	MediCompass	Personal Health Record (PepsiCo)
Enterprise Patient Portal	mediKEEPER	Portable Health Profile
ePHR	MediStick	ProfileMD
Evolution PHR	MedInfoChip	ReliefInsite.com (using Facebook)
FollowMe	MedNOTICE	Securamed
FullCircle	My Family Health Portrait	SGMSCorp
Global Patient Record	My Health Connection	SynChart
Google Health	My Health Record	Telemedical.com
Handymedical.com	My HealtheVet	The Smart PHR
Health Account Basic	My MediList	Touchnetworks H.U.B.
HealthFile	My Medical CD	Vital Key
HealthFrame	MyActiveHealth PHR	Vital Records
HealthVault (Microsoft)	MyChart (Epic)	VitalChart
iHealthRecord	myCIGNA	Vividea (Lifetime Personal Health Software)
Indivo (Dossia)	MyFamilyMD	Waiting Room Solutions
InfoVivo	MyHealth123.net	WebMD Health & Benefit Manager
iPHER	MyHealthAtVanderbilt	
IQHealth	myHealthFolders	
	MyLife	

Table 1 Sample list of available PHRs product

While the idea of greater access to health information may make PHRs and EHRs much more desirable to patients, payers, government and other stakeholders, there are the obvious risks with respect to managing e-PHI security and privacy issues, and less obvious but very real risks to records management, preservation and collection for litigation and business purposes.

III. CHANGING FEDERAL RULES — CHANGING PROCESSES WITHIN HEALTHCARE

When the Judicial Conference Rules Advisory Committee (the Committee) was involved in the lengthy drafting and review process regarding amending the Federal Rules of Civil Procedure (FRCP), the effect the FRCP amendments would have on healthcare operations and compliance was probably not on the Committee's "radar." Yet, the FRCP amendments are changing operations within the healthcare industry just as much as they are redefining and reshaping business and legal processes. As a result, e-discovery is becoming an important part of healthcare compliance and litigation management.

HSOs across the country are in the early stages of thinking about how their organization will respond to e-discovery requests for information.[23] Senior management of HSOs of all sizes and complexities may want to consider appointing a multi-disciplinary litigation response team to evaluate the process by which electronic information is preserved and produced in response to threatened or impending litigation.

As a result, the FRCP amendments are creating a new set of roles and responsibilities for healthcare legal counsel, risk management, compliance, IT, HIM, and medical informatics[24] professionals including chief medical information officers (CMIO)[25]. Along with these new responsibilities come questions and gaps in understanding the impacts of the changes in disclosure, retention, destruction, preservation, and spoliation of ESI and e-PHI in the L-EHR.[26]

Traditionally, the discovery process was paper based and the risk management and health information management (HIM) departments played key roles in the preservation and production of documents for litigation. While the actual structure and reporting relationships vary in most healthcare organizations today, the risk management professional, with legal oversight, coordinates the litigation process within the organization. For example, the HIM generally works closely with risk management in maintaining its key role in the processing of subpoenas. The Director of the HIM Department is often named as the organization's official records custodian. In this capacity, the HIM director may be deposed as a corporate representative to attest to the authenticity of records produced for litigation and/or testify about organizational operations regarding the management of information. The HIM director, however, may lack the requisite knowledge or technical expertise to satisfy new demands imposed by the recent amendments of the FRCP.

One of the most significant changes to the legal process has been a reshaping and redesign of the roles and responsibilities of legal counsel in management of the legal process.[27] FRCP 26(f) and 16(b) require the parties to meet early on in the litigation process and discuss matters related to the discovery of ESI. Therefore, in-house and outside counsel now have a duty to become informed as to the details of the organizations' systems and processes by which information is managed within their healthcare organizations. As a result, HIM, medical informatics and IT professionals have a responsibility that includes defining and describing the "good faith operations" of the organization's information systems as well as a method for determining the organization's true costs and burdens for production of ESI.

Until enactment of the FRCP amendments, the IT Department and medical informatic professionals played little to no role in the litigation process. However, now with the tremendous increase in ESI, other health information professionals also play key roles in the preservation and production of ESI. As a result, HSOs may want to consider establishing a litigation response team comprised of professionals from among such departments as: legal, risk management, HIM, medical informatics, security and IT. Cross-domain expertise is necessary to assist counsel (inside and outside) in identifying the locations of potentially responsive information, as well as educating legal counsel about the structure and operation of the organizations information systems.

23 Reich, Kimberly Baldwin-Stried. "Developing a Litigation Response Plan." *Journal of AHIMA* 78, no.9 (October 2007): 76-78,86.
24 Hersh WR. Who are the informaticians? What we know and should know. *Journal of* the American Medical Informatics Association 2006; 13: 166-70
25 Leviss J, Kremsdorf R, and Mohaideen MF, The CMIO - a new leader for health systems. *Journal of* the American Medical Informatics Association, 2006. 13: 573-578.
26 Addison K, Braden JH, Cupp JE, Emmert D, Hall LA, Hall T, et al. Update: guidelines for defining the legal health record for-disclosure purposes. *Journal of AHIMA* 2005 Sep;76(8):64A-64G.
27 *Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y, July 20, 2004)

Discovery vs. Disclosure

Because the concept and the scope of discovery versus disclosure can often be confusing for health information professionals who are involved in the release of information, many information managers in healthcare are seeking advice from counsel about those concepts. Realizing that the amount of information subject to discovery might be significant, HSO can save time and resources by identifying the form, content and format of a legal electronic health record for disclosure and discovery purposes.

The concept of "disclosure of information" in the healthcare field is a critical function for patient care continuity and business operations of HSO; it occurs routinely in varying forms. To contrast these differences, HIPAA defines disclosure as "the release, provision of access to, or divulging in any other manner of information outside the entity holding the information." In the healthcare setting, disclosure is usually performed in response to a signed authorization/request for medical records. The content and form (usually paper) of what is produced to the requesting party that is disclosed, is that information which the organization has defined as its' L-EHR.

Effective Records Management Procedures for EHR and HSO: Reality or Fantasy?

One of the unique aspects of healthcare litigation and e-PHI and ESI is not the amount of data but where the data is located. In the non-healthcare environment, a typical enterprise has ownership or custody of its "business records" – business critical information that the company needs for legal, regulatory or business reasons. While business critical data may be located in satellite offices, foreign subsidiaries or "agents" of the corporation (e.g., accountants, service providers, etc.), the company should have access to or control of the data at any given time. In the healthcare industry, data is much more "decentralized" and as a result, access to and control of that data can be very complicated. What constitutes a patient's "legal medical record" might be more like a jigsaw puzzle with pieces of different shapes and sizes located anywhere and everywhere.

While healthcare facilities and providers are primarily "responsible" for maintaining medical records (patients are not), what about e-PHI that is kept by the patient in the form of an electronic PHR? Is this also part of the patient's "medical record"? Is e-PHI critical information that would rise to the level of a "record" for records management purposes? Is it the type of information that is routinely relied upon by healthcare providers when administering care?

Moreover, the "official" custodian of records can vary depending on the practice setting and available resources. Thus, the use of existing protocols or policies for implementing effective legal holds for healthcare records when litigation or a regulatory investigation is pending or threatened, may not be very effective within a healthcare organization. Access to and security of the records can also vary significantly across clinical settings as well. Are there defensible and repeatable standards that are followed in the healthcare field that would survive judicial scrutiny? The spectrum of records management procedures may range from an untrained receptionist using an ad hoc paper filing system to an electronic practice management system (PMS) integrated with an electronic health record that automatically indexes and archives records or data elements. Clinicians in private practice may use PMS for scheduling and claims analysis, coding and electronic submissions, etc. In addition, PMS may be integrated with the electronic record system and may provide such information as allergy lists, medication lists, problem lists, continuing care records (CCR), decision support tools, electronic prescribing, telephone records, and even e-mail communications with providers and patients.

Even in the most sophisticated electronic documentation systems, actual clinical documentation typically involves a hybrid of paper and electronic records. Paper maybe used for diagnostic results (e.g. Radiology, EKG and laboratory reports or other ancillary reports), consent signatures or specific forms. Clinical documentation (the 'old fashion history, physical exam and medical action plan) may also be in electronic form. The spectrum of EHR clinical documentation may be as simple as electronically scanned handwritten notes, imported notes from a voice activated transcription system, a dictated and then transcribed note or as sophisticated as a template driven

electronic document derived from databases of computable clinical content using a standard ontology of medical terminologies.

Healthcare facilities (hospitals, outpatient centers, diagnostic centers, outpatient surgeries, etc.) are responsible for maintaining the records for both the facility and the provider services within their organizations. Thus, the "business record" of a patient's clinical encounter with a private practice physician at that facility is routinely maintained by that facility. Yet, vast amounts of important information (PHI, e-PHI, ESI and paper) may reside outside the physical possession of the primary healthcare provider – for example — diagnostic and laboratories services (i.e., radiology or pathology). Other e-PHI sources included nurses' and therapist notes, patient tracking systems, surgical system notes, anesthesia systems notes, patient-physician, physician-physician emails, pager alerts, biomedical equipment data (e.g. smart IV pumps), digital photos, streaming images and so on. Each individual electronic health information system may interface and be interoperable with hundreds of servers and databases and the "outputs" of each may vary significantly in terms of format. Given the multitude of complex components that make up the electronic information system for a healthcare enterprise, great care should be taken in advance of litigation to design and implement a defensible and reliable records management protocol.

Counsel and health information professionals are struggling with the basic question of "What is the legal electronic health record?" The L-EHR is described as the form of the EHR produced and preserved for legal business, transactional and evidentiary purposes.[28] The dilemma of defining a "business record" from disparate computing systems, hybrid environments of paper, transcription, handwritten preliminary reports, and poorly defined outputs from electronic clinical documentation systems highlights the need for a multidisciplinary team to develop defensible and reliable processes, policies, and procedures.

Metadata has become extremely important in assessing reliability and dependability of healthcare information for legal, clinical, regulatory and research needs. While metadata plays an important role in assessing the integrity of the components of L-EHR systems, do existing EHR software applications have the functionality to preserve the minimum metadata necessary for assurance of non-repudiation of the health record?[29]

Recently, the Center for Medicare and Medicaid Services (CMS) issued an advisory opinion concerning the development of EHR interfaces between hospital and physician practice electronic record systems.[30] Simultaneously, the HHS Office of Inspector General finalized an anti-kickback regulation for certain financial relationships between clinicians for establishing health information technology systems.[31] The intent of this flow of information is to encourage physicians to have broader access to patient data; however, it leaves unresolved many issues of ESI and health information management for litigation and business purposes.

IV. RELIABILITY ISSUES

Courts have recognized that authentication of ESI is a critical step in the evidentiary process and that ESI may require greater scrutiny than that required for the authentication of "paper" documents. However, courts have been quick to reject calls to abandon the existing rules of evidence when doing so. In *In Re Vee Vinhnee,* 336 B.R. 437 (9th Cir. BAP (Cal.) 2005, the court addressed the authentication of electronically stored "business records". It observed "[a]uthenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained . . . ." However, it noted "[t]he paperless electronic record

28 *See*, AHIMA e-HIM Work Group on the Legal Health Record. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes." *Journal of AHIMA* 76, no.8 (September 2005): 64A-G; Cottrell CM. The Legal Health Record: A Component of Overall EHR Strategy. *Journal of AHIMA* 2007; 78(3):56-57; Dimick C. Charting the Legal Health Record. *Journal of AHIMA* 2007;78(5):30-30; and Dougherty, Michelle. "How Legal Is Your EHR?: Identifying Key Functions That Support a Legal Record." *Journal of AHIMA* 79, no.2 (February 2008): 24-30.

29 Ball, K. ORGANIZATIONAL APPROACHES TO EARLY LITIGATION READINESS FOR ELECTRONIC DISCOVERY OF ELECTRONIC HEALTH RECORDS: A MODIFIED DELPHI STUDY: A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Science. Baltimore, Maryland, March 2008.

30 CMS Issues Favorable Opinion Concerning Development of EHR Interface, BNA'S HEALTH L. REP. (June 5, 2008)

31 Aug. 8, 2006, Federal Register (71 Fed. Reg. 45110, 45140).

involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records. Ultimately, however, it all boils down to the same question of assurance that the record is what it purports to be." Id. at *445.

While computerized data raises unique issues concerning accuracy and authenticity, problems may be exacerbated when it comes to the healthcare industry because of the history of decentralized record keeping, lack of clear definition of a legal health record, and the more elusive definition of a legal electronic health record. Accuracy of health information may be impaired by incomplete data entry, mistakes in output instructions, programming errors, logic in decision support tools damage and contamination of storage media, power outages, and equipment malfunctions. These errors may be a result of human and system software failures all too common in healthcare. The integrity of data may also be compromised in the course of litigation by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy and the judge has to consider the accuracy and reliability of computerized electronic information systems. Only recently has the medical literature begun to address some of the intended consequence that HIT may have on ESI in EHRs.[32]

In *Lorraine v. Markel American Ins. Co*., 241 F.R.D. 534 (D. Md. 2007), Chief Magistrate Judge Paul Grimm noted that while there is no single approach to authentication that will work in all instances, it is possible to identify certain authentication issues that the courts and the commentators have identified with particular types of evidence such as computer stored records and data.

V. COMPUTER STORED RECORDS AND DATABASES

While many EHR systems rely on database outputs as the L-EHR problems may arise due to the dynamic nature of electronic information. For example, somewhere between structured databases and the L-EHR document management repositories are enterprise reports from the L-EHR. The major problem with disclosure of records, generated from queries or outputs from database reports is their dynamic nature. Many interoperable EHR systems use common report writers (e.g., Crystal Reports/Business Objects, SQL reports).

Given the current business practice to store massive amounts of personal healthcare data on computers, major authentication problems may arise down the road because, as Judge Grimm noted, there is a great disparity between the most lenient approaches and the most demanding approaches regarding authentication.

Judge Grimm referred to *In Re Vee Vinhnee*, 336 B.R. 437, 444 (B.A.P. 9th 2005) as the "high water mark" for demanding approaches.

The primary authenticity issue in the context of business records, as identified by the Court in *In Re Vee Vinhnee*, is "on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created . . . . Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created." *Lorraine* *558. The *Vee Vinhnee* Court went on to state that, for electronic information, "[t]he logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as

32 Harrison MI, Koppel R, Bar-Lev S. Unintended Consequences of Information Technologies in Health Care An Interactive Sociotechnical Analysis. J Am Med Inform Assoc 2007 September 1;14(5):542-549; Wachter RM. Expected and Unanticipated Consequences of the Quality and Information Technology Revolutions. JAMA 2006 June 21;295(23):2780-2783; Weiner JP, Kfuri T, Chan K, Fowles JB. "e-Iatrogenesis": The Most Critical Unintended Consequence of CPOE and other HIT. J Am Med Inform Assoc 2007 May 1;14(3):387-388; Walker et al. EHR Safety: The Way Forward to Safe and Effective Systems. J Am Med Inform Assoc.2008; 15: 272-277; and Ash et al. The Extent and Importance of Unintended Consequences Related to Computerized Provider Order Entry. J Am Med Inform Assoc.2007; 14: 415-423.

the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation." Id. Judge Grimm then noted that in order to meet the heightened demands for authenticating electronic business records, the *Vee Vinhnee* Court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

Id. at 446-47 (citation omitted).

Based upon the above factors, the following issues should be part of any discussion about setting up a defensible records management program in the healthcare field: where is the relevant information located and who are the custodians? Should there be an in-house individual that is charged early on in the process with understanding the electronic information systems and memorializing the protocol and procedures? Are there any special problems that can be identified early with respect to identifying, preserving, collecting and producing relevant non-privileged information? How are these issues complicated by federal mandates and regulatory and jurisdictional requirements in healthcare industry?

The following e-discovery cases demonstrate how the healthcare industry, like many businesses today, needs to transition from a paper-based records system to an electronic-based system. There needs to be a sense of urgency in addressing ESI given the staggering volume and the tremendous risk with respect to PHI data at issue.

VI. RECENT E-DISCOVERY DECISIONS IN HEALTHCARE LITIGATION

Carrie, et al. v. Goetz, 2007 U.S. Dist. LEXIS 75457 (United States District Court, Middle District Tenn. (October 10, 2007) reconsidered 2007 U.S. Dist. LEXIS 84557. This is a class action on behalf of approximately 550,000 children who are alleging that the defendants deprived them of their right to early and periodic screening, diagnosis and treatment (EPSDT) services for children under State's TennCare program. Under a 1998 Consent Decree, the defendants and their Managed Care Contractors ("MCC") were obligated to provide EPSDT services to the class members and to report on their provision of such services. They were also required to maintain various types of ESI. The plaintiffs moved to compel discovery regarding the state's compliance with the consent decree and the Court found an "absence of any effective attempt by the Defendants to preserve and segregate relevant ESI since the filing of the lawsuit in 1998." The state failed to issue a litigation hold from

1998 until March 2004. Upon reconsideration, the court determined that the actions or inactions by the state with respect to the litigation hold "raises serious concerns about preservation" and "suggest[s] a deliberate decision not to take ...necessary steps... to preserve data . . . " The Court granted the Plaintiffs' motion to compel, which included allowing Plaintiffs' computer expert to be present at the state's production. The Court also appointed a neutral monitor.

Diabetes Centers of America, Inc. v. HealthPia America, Inc., 2008 U.S. Dist. LEXIS 8362, (United States District Court, Southern Dist. TX (February 5, 2008). This is a breach of contract case brought by a cell phone purchaser against the cell phone seller and its officers. The plaintiff is a full-service treatment center for persons with diabetes. The defendant HealthPia develops and markets mobile healthcare devices — a cell phone that tests and reads a patient's glucose levels, stores the result and transmits the test results to physicians or others designated by the patient. Both parties cross moved for sanctions for a spoliation instruction – each claiming that the other lost or destroyed relevant emails. Plaintiff claims that Defendant failed to back-up emails that were subsequently lost when two laptops containing those emails were stolen. The Defendant claimed that the Plaintiff failed to preserve and produce critical emails that were contrary to Plaintiff's position in the lawsuit. Defendant also alleged that Plaintiff failed to produce copies of emails showing that Plaintiff was aware that its failure to provide certain security documentation was a major problem in getting certification from at least one cellular phone company. At the hearing on the cross motions, Plaintiff's counsel conceded that the task of searching Plaintiff's records for relevant emails in response to Defendant's discovery requests was entrusted to a junior associate with little or no direct supervision. Moreover, the search terms used by the associate were woefully inadequate – they did not even include the term "phone" in the search. Since neither party presented evidence of bad faith, the Court declined to sanction the parties.

In re Seroquel Products Liability Litigation, MDL 2007 WL 2412946 (M.D. Fla. Aug. 21, 2007). This is a multi-district pharmaceutical products liability case where the Court, in reviewing the discovery behavior of the defendants found that they had engaged in "purposeful sluggishness" in responding to discovery. The Court criticized the Defendant's behavior which included, among other things, failing to meet and confer in advance of electronic searches to discuss search term methodology, producing ESI without metadata or load files, producing multi-page .TIFF images (some as large as 20,000 pages) and producing electronic documents without Bates numbers. Relying on *The Sedona Principles* and the *Manual for Complex Litigation* (4th), the Court noted that many of the problems that existed could have been avoided or "could have been resolved far sooner and less expensively had [the defendant] cooperated by fostering consultation with the technical staff responsible for the production." The Court did not decide on any sanction pending further discovery on the extent of prejudice to the plaintiffs and the related costs.

U.S. ex rel. Kelly A. Woodruff et al. v. Hawaii Pacific Health et al., 2008 U.S. Dist. LEXIS 4933, (United States District Court, District of Hawaii, (January 23, 2008). This is a qui tam action alleging, among other things, violations of the Federal False Claims Act. Plaintiffs claimed that Defendants submitted false claims for procedures performed by nurses who were not licensed to perform those procedures. Plaintiffs also claimed that Defendants submitted false UB-92 forms for the reimbursement of charges associated with those procedures. While Defendants initially denied that they possessed any UB-92s, when Defendants were confronted with Plaintiffs request to inspect Defendants' computer systems and a Rule 30(b) (6) deposition notice, Defendants admitted that they had the requested information all along in microfiche format. While the court questioned the integrity of the program which Defendants used to print the PDF-forms because the software could change the content of the claims forms without leaving an audit trail of the changes, the Court deferred Plaintiffs' request for production of the information in native format pending further briefing.

In *Rush University Medical Center. v. Minnesota Mining and Manufacturing Co., (3M)* No. 04 C 6878 (N.D. Ill. Nov. 21, 2007), an Illinois District Court held that the Rush University's Consumer Fraud Act claim against Minnesota Mining and Manufacturing (3M) was time barred by the Act's three-year statute of limitation period. On December 24, 1998, after nearly three years of negotiations with 3M, Rush signed a contract with the EHR vendor to license 3M's Care Innovation

system, an integrated clinical information system designed to give medical providers improved medical electronic access to patient records. During the negotiations leading up to the parties' agreement, 3M made certain representations to Rush that caused Rush to believe that 3M had the capabilities to provide for all of Rush's requested functions. The Care Innovation system went "live" at Rush by the fall of 1999. The parties' contract required the 3M Care Innovation System to link Rush's different clinical and administrative systems into a single integrated patient information system. On October 26, 2004, Rush filed a complaint alleging that the Care Innovation system that 3M provided lacked some or most of the functionalities that 3M had contractually agreed to provide. Rush brought claims for breach of contract, breach of warranty, and statutory fraud. 3M denied all allegations and moved for summary judgment. The court found that there was a genuine controversy that existed as to whether 3M acted with gross negligence or willful misconduct and so it granted the 3M's motion in part and denied it in part. This case provides an excellent example of the impact poorly procured EHRs have on healthcare operations. The court's decision demonstrated that the functional requirements for an EHR should be clearly delineated and set forth in the contract that the healthcare provider signs with the vendor. There should also be timelines for the review of the status of implementation. In addition, system performance should be closely monitored.

With respect to the 2006 changes to the Federal Rules of Civil Procedure, many companies have had to make a number of changes to adapt how they conduct business. While the healthcare industry will face many of the same problems that other industries might face, there are a few issues that are unique. In particular, given the "decentralization" of data storage in terms of EHR, how does a healthcare enterprise determine what information is "not reasonably accessible due to undue burden or cost" under Rule 26(b)(2)(B)?

VII. WHAT IS "NOT REASONABLY ACCESSIBLE" IN HEALTHCARE LITIGATION?

While FRCP 26(b) (2) (B) permits a party to withhold from discovery "electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost," Rule 34(a) (1) (A) requires production of documents or ESI "stored in any medium from which information can be obtained either directly, or if necessary, after translation by the responding party into a reasonably usable format."

Rule 26(b)(2)(B) was promulgated to protect parties from wasting time and resources culling through data from sources that are not generally considered "active" data sources such as legacy systems, backup tapes, and "erased, fragmented or damaged data."[33] However, the label of "reasonably accessible" or "not reasonably accessible" cannot be made based solely on the type of media used. The key to this analysis is the "undue burden or cost."

In *W.E. Aubuchon Co. v. BeneFirst, LLC*, 245 F.R.D. 38 (D. Mass. 2007), a case that involved the administration of qualified benefit plans under ERISA, the plaintiff (who was the employer, sponsor and administrator of the plan) sought all medical claims files, including the actual medical bills in BeneFirst's custody or control. BeneFirst was no longer in operation, so in order to comply with the Court's discovery decision, BeneFirst would have had to hire personnel to retrieve the claims sought by the Plaintiffs. Moreover, the uniqueness of BeneFirst's "method of storage and lack of an indexing system" made it prohibitively expensive to retrieve the requested information.[34] Therefore, the court ruled that the data was "not reasonably accessible."

In making a determination of whether the requesting party had established "good cause," the court looked at whether:

33 *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 318-19 (S.D.N.Y. 2003).

34 Id at 43. The search process for retrieving claims was further complicated by the fact that there was no index of images *per se*. The images were stored on BeneFirst's server first, according to year of processing, then by claims examiner, then by the month of processing, and finally by the actual processing date. BeneFirst's system was not set up to for the wholesale retrieval of claim images on a group by group basis. BeneFirst explained that its storage system "was designed to locate, within a reasonable amount of time, a particular claim if it became necessary to locate the associated image. However, the image itself was generally not required in the normal course of BeneFirst's claims processing operations. The organization of the image files was not designed for the wholesale retrieval of images on a group-by-group basis." *W.E. Aubuchon Co.*, 245 F.R.D. at 43 n.3.

> (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.

Id. at 43 (citing Fed. R. Civ. P. 26(b) (2) (C)).

In this case, the records sought by the Plaintiffs were stored on a server used by BeneFirst in Pembroke, Massachusetts. However, because of BeneFirst's method of storage and lack of an indexing system, it was extremely costly to retrieve the requested data. The Court noted:

> I am hard pressed to understand the rationale behind having a system that is only searchable by year of processing, then claims examiner, then the month of processing, and finally the claims date. None of these search criteria reflect the name of the individual claimant, the date that the claimant received the medical service, who the provider was, or even the company that employed the benefit holder. It would seem that such a system would only serve to discourage audits and the type of inquiries that have led to the instant litigation. [Footnote Omitted]. Nevertheless, the retrieval of the records will be costly and for the purposes of this decision, I find that such retrieval would involve undue burden or cost. Accordingly, the images are not reasonably accessible within the meaning of Fed. R. Civ. P. 26(b) (2) (B).

Id. Next the Court had to determine whether there was "good cause" to order the production. The Advisory Committee Note to Rule 26 lists the following factors that courts may also consider:

> (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

See, Fed. R. Civ. P. 26(b) (2) and Advisory Committee note. The court then weighed these factors (taking into consideration that some are duplicative) and after determining that Aubuchon had established "good cause," determined that BeneFirst must produce the requested data and bear the entire cost of production. *Id.* at 43-45.

In another example, *Static Control Components, Inc. v. Lexmark Int'l, Inc.*, No. Civ. A. 04-84-KSF, 2006 WL 897218 (E.D. Ky. Apr. 5, 2006), plaintiff, Static Control Components ("SCC") brought a declaratory judgment action alleging that it had not violated the Copyright Act or the Digital Millennium Copyright Act. While SCC sought production of a Lexmark database containing certain customer information, Lexmark argued that it did not have to produce that information because it was maintained: "(a) in a form that is not text-searchable; (b) using software that is no longer commercially available; and (c) software which it modified for its own use."[35] Lexmark offered to allow SCC to inspect Lexmark's database. SCC countered by arguing that Lexmark's offer would not allow SCC to gain "meaningful access" to the relevant information because "the only way to

35 *Id.* at *3.

retrieve information from this database is by inputting a specific caller's name, phone number, or call reference number (which is an internal designation created by Lexmark.)"[36] Since SCC did not retain this information, the court granted SCC's motion to compel stating that the "Federal Rules do not permit Lexmark to hide behind its peculiar computer system as an excuse for not producing this information to SCC."[37]

VIII. WHAT ARE COURTS SAYING ABOUT RECORDS MANAGEMENT AND "BEST PRACTICES" ?

Records managers and corporate counsel (in-house and outside) alike continue to scour court decisions for guidance as to "Best Practices" (or if not "Best Practices," then any guidance as to "acceptable practices") for companies dealing with records management issues. The recent changes to the FRCP regarding electronic discovery are grounded in ideals of "good faith" and "reasonableness", but they do not address pre-litigation records management policies. While these concepts are good enough to provide companies with guidance to create defensible and cost-effective records management policies, is "good enough" not good enough when it comes to what the courts are expecting? Should companies be doing more?

The earliest guidance from the Courts on record retention is *Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472 (S.D. Fla. 1984). In that case, the defendant's document retention/destruction policy had as its stated purpose "the elimination of documents that might be detrimental to it in a lawsuit." While the Court might appreciate the company's honesty in describing its record retention policy, the Court noted that a policy with a stated purpose such as that would not survive judicial review. Instead, the company needed what the Court called a "reasonable" document retention program. This "reasonableness" standard was reinforced by the 8th Circuit Court of Appeals decision in *Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988). It is still the standard today, but how should a company use this standard to measure the "reasonableness" of its records management program.

The most significant case for validating the destruction of corporate records in the ordinary course of business is the United States Supreme Court decision of *Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005). There the Court stated that "[d]ocument retention policies," which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. (citation omitted). It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances." Id. at 704. Those ordinary circumstances the Court was referring to — without litigation pending or a Government subpoena served.

After the *Arthur Andersen* decision, the standard seems pretty clear — in a "litigation free" atmosphere, if the company has created and implemented a clearly defined and reasonable record retention plan that identifies those business-critical records that should be kept for legal, business or regulatory reasons and has set appropriate retention periods, then information not meeting the retention guidelines can be destroyed. *However*, with pending or threatened litigation or regulatory investigation, the destruction component of the record retention plan must be flexible enough to preserve potentially relevant information that does not exist elsewhere for fear of destroying data relevant to the litigation and then facing a spoliation charge.

IX. ADVICE ABOUT CORPORATE GOVERNANCE AND "BEST PRACTICES"

More courts have struggled with situations where they are forced to address the interface between records management programs and the implementation of a plan to preserve relevant data. While they strive to find what should be considered "Best Practices" citing with approval *The Sedona*

36 *Id.*
37 *Id.* at *4 (citing *Dunn v. Midwestern Indem.*, 88 F.R.D. 191, 197 (S.D. Ohio 1980); and *Kozlowski v. Sears, Roebuck & Co.*, 73 F.R.D. 73, 75.

Principles, almost without exception, they do not provide very much guidance in terms of the process that should be used.

In many of these cases, the problems associated with information not being found or available started with the company's record management program. Did the company "map" its electronic information system such that there would be a checklist for lawyers and IT personnel to locate relevant information? Did the company pay attention to the identification and collection of electronic information during discovery so as to be able to discuss at trial the origin of the information, the reliability of the systems that stored the information and the chain of custody for that information? All of these issues should be considered when devising a defensible records retention program. While this is informative, is there anything about "Best Practices" that we can extract from these cases? Of course, that assumes that companies have to follow "Best Practices" in order to be successful in business and litigation? But is that really necessary?

In August 2005, the Court of Chancery in Delaware issued a decision, not in an electronic discovery case, but in a stockholders' action against corporate directors and officers of Walt Disney Company for breaches of fiduciary duty in connection with the hiring and termination of the corporation's president. While the Court said nothing about electronic discovery, ESI, PHI, EHR or records management policies or programs, it did offer some very useful advice about corporate governance. While the Judge's comments were directed to directors and officers, the guidance is equally applicable to records managers as well . . .

> [T]here are many aspects of [the company's] conduct that fell significantly short of the best practices of ideal corporate governance. Recognizing the protean nature of ideal corporate governance practices, particularly over an era that has included the Enron and WorldCom debacles, and the resulting legislative focus on corporate governance, it is perhaps worth pointing out that the actions (and the failures to act) of the Disney board that gave rise to this lawsuit took place ten years ago, and that applying 21st century notions of best practices in analyzing whether those decisions were actionable would be misplaced.
>
> * * * *
>
> This Court strongly encourages directors and officers to employ best practices, as those practices are understood at the time a corporate decision is taken. But [the] law cannot hold fiduciaries liable for a failure to comply with the aspirational ideals of best practices,
>
> * * * *
>
> [T]he essence of business is risk – the application of informed belief to contingencies whose outcomes can sometimes be predicted, but never known. The decision-makers entrusted by shareholders must act out of loyalty to those shareholders. They must in good faith act to make informed decisions on behalf of the shareholders, untainted by self-interest….
>
> * * * *
>
> That is why … within the boundaries of those duties [decision makers] are free to act as their judgment and abilities dictate, free of *post hoc* penalties from a reviewing court using perfect hindsight. Corporate decisions are made, risks are taken, the results become apparent, capital flows accordingly, and shareholder value is increased.[38]

38 Disney 907 A. 2d 693, 697 – 98.

X. CONCLUSION

Managing ESI and e-PHI in the healthcare industry presents some very unique problems for consumers, providers, health information managers, in-house and outside counsel because the definition of the legal health record is ill-defined and ESI and e-PHI routinely resides in a number of different locations with a myriad of custodians. The custodians many of whom may not be under the control of the primary healthcare provider may not have the requisite technical expertise or the EHR systems to properly provide non-repudiated and authenticated records for litigation and business purposes. In addition, there are substantial regulatory concerns (HIPAA) as well as complex privacy and security issues.

In order to improve health information tools with respect to the routine business needs of ESI contained with the EHR, certain changes need to be made such as:

* Education of health information professionals responsible for procurement, development, enhancements, use and maintenance of health information tools;

* Education of health care professionals to help evaluate functionality of health information tools; and

* Establishment of standards that mandate that healthcare organizational teams support "Best Practices" with respect to information management in the context of litigation preparedness regarding ESI in the L-EHR.

The healthcare industry is just starting to examine those unique e-discovery issues and hopefully this paper will provide a basis for a formative discussion and some framework for future dialogue for addressing issues related to ESI and EHRs in healthcare.