



hfma[™] new mexico chapter
healthcare financial management association

NMHiMA
New Mexico Health Information
Management Association

An Affiliate of
AHIMA
American Health Information
Management Association[®]

E-DISCOVERY: AN INTRODUCTION

April 16, 2010

Discovery

- In AHIMA's new legal text, *Fundamentals of Law for Health Informatics and Information Management*, discovery is defined as:
 - “The next pretrial stage after the commencement of a lawsuit, which allows all parties (generally via their legal counsel) to use various strategies to discover or obtain information held by other parties and, subsequently, to assess the strengths and weaknesses inherent in each party's case.” (p. 466)
- The same text defines e-discovery as “The discovery of evidence contained in electronic documents such as e-mails or electronic health records.” (p. 466)

Discovery Fundamentals

- HIM professionals can hearken back to their legal classes when professors discussed that discovery most often begins with the filing of a formal legal complaint. It occurs **before** a lawsuit goes to trial.
- HIM staff have historically routinely copied records for their own and opposing counsels as part of the discovery process.

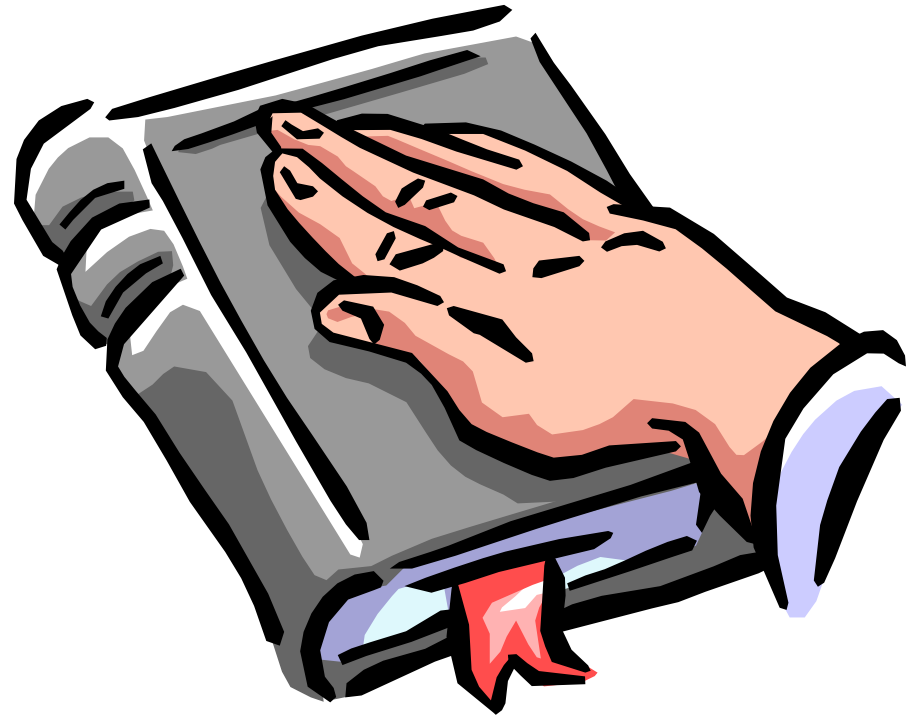
Discovery Definitions

- A *complaint* is a document that is filed with a court in order to commence a lawsuit.
- A *subpoena* is a legal order requiring an appearance in court at a stated time. This device summons witnesses to court. In a *subpoena duces tecum* the subpoena recipient must bring documents and other records with himself/herself to a deposition or to court.
 - From *Fundamentals of Law for Health Informatics and Information Management* (p. 462 & 483)



Discovery Definitions

- A *deposition* is a formal proceeding by which the oral testimonies of individuals are obtained as part of the discovery process



Records Inspection/Records Production

- *Records Inspection Requests* are written notices to inspect records.
- *Record Production Requests* are written orders by the court to produce documents.
- Sample =
<http://www.justice.gov/atr/cases/f0100/0194.htm>

How did we get the “E” in E-Discovery?

- The Federal Rules of Civil Procedure (FRCP)
 - Governs procedures for all civil suits in US District Courts
 - Amendment addresses unique aspects of e-discovery
- Who issued this amendment?
 - The Supreme Court (and approved by the US Congress)
 - Effective December 1, 2006
- Who does it apply to?
 - Legal proceedings in the federal court systems (federal cases)
- Most litigation is in the state & local courts – will this have an impact?
 - Yes – the FRCP established a standard that is gradually being adopted in state and local jurisdictions as new e-discovery procedures are adopted
 - <http://www.uscourts.gov/rules/CV2008.pdf>.

E-Discovery Rules: Process and the Quality of the ESI

- The Federal Rules of Civil Procedure (12/1/06) referenced in the last slide govern the *process* for producing *Electronically Stored Information also called ESI*
- A body called the Uniform Law Commission worked concurrently with the Federal committee who produced the amendment to the FRCP and produced *The Uniform Rules Relating to the Discovery of Electronically Stored Information*. These rules are now part of the Federal Rules of Evidence and govern the *quality* of *ESI* produced.
- The Federal Rules of Civil Procedure and The Federal Rules of Evidence establish the rules for litigation in the United States

Electronically Stored Information (ESI)



- Any information in any form relevant to the case is discoverable.
- All electronic information should be treated as potential evidence and the integrity of the information maintained.
- HIM professionals working closely with IT must be knowledgeable about the flows, format and storage of ESI
- It will be critical for HIM and IT to work closely with legal counsel in developing a mutual understanding of the information managed and stored within your organization

E-Discovery: The Process

- Rule 26

- (a)(1)(A) requires the parties in a lawsuit to automatically provide to the other parties copies, or descriptions by category and location, of any ESI in their possession
- (b)(1) sets the *scope* of discovery which can be almost unlimited, barring privileged information
- (b)(2)(B) provides for some relief for ESI that may not be “reasonably accessible”
- (f) Has an emphasis on meeting and pretrial conferences and the development of discovery plans
 - Expected formats for records production are discussed here.

E-Discovery: The Process

- Rule 33
 - Allows interrogatories (*a list of written questions*) to be answered under certain conditions by referring the requesting party to ESI
 - Requesting party reserves the right to make copies

E-Discovery: The Process

- **Rule 34: format**
 - (a) You can be expected to produce records stored in any medium and potentially requiring interpretation
 - (b)(1) The requester must specify the format of production they expect to receive; objections must be reasonable
 - (b)(E) If records cannot be produced in the requested format, a *reasonably useable* format must be provided

E-Discovery: The Process

- Rule 37(e)
 - Provides for lost ESI that is discoverable.
 - Develops the concept of “*good faith practices*”
 - Acceptability of missing information lost as a normal part of operations, i.e. overwriting tapes
 - Distinguishes “lost” from “destroyed”, i.e. ESI deliberately singled out for destruction

E-Discovery: The Process

- Rule 45

- (d)(1)(B)(C) and (D) addresses how to respond to subpoenas for ESI
 - Repeats the concept of *reasonably accessible*
 - Creates the burden of understanding the cost of electronic record production



Imagining an E-Discovery Action



Implications of the Duty to Preserve and Produce

- The duty applies to both hard copy and electronically stored information (ESI)
- There must be people who are knowledgeable about –
 - Retention requirements
 - Back ups, integrity of system data, record tracking, application of legal holds
 - Preservation Notice documentation management
 - *Duty to Preserve slides based on “The New e-Discovery Rule for Legal Proceedings”*
(Michelle Dougherty, RHIA, CHP and Kim Baldwin-Stried (Reich), MBA, MJ, RHIA, CPHQ)



Implications of the Duty to Preserve and Produce

- What information is “reasonably accessible” and what is not and the cost implications of electronic record production
- The ability to produce information in the same form as it existed at the time the ESI was created
- The development and documentation of “good faith” practices including data aberrations or losses documentation

Duty to Preserve



- Relevant Case Law:

- 1. *Silvestri v. General Motors*, 271 F.3d 583, 591 (4th Circuit 2001).

“The duty to preserve material evidence arises not only during litigation but also extends to that period before litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.”

- 2. *Mosaid Technologies, Inc. v. Samsung Electronics Co.*, LTD, 348 F. Supp. 2d 332 (D.N.J. 2004).

“If a party has notice that evidence is relevant to an action, and either proceeds **to destroy that evidence or allows it to be destroyed by failing to take reasonable precautions**, common sense dictates that the party is more likely to have been threatened by that evidence.”

Legal Holds

- **Legal Hold**– Generally issued by the court
 - Should be initiated when a duty to preserve is clear
 - Suspends the normal disposition, processing of paper and electronic records.
 - Organizational policy should dictate legal hold policies and procedures
 - After implemented, legal holds should be regularly monitored
 - Failure to initiate a legal hold can lead to adverse inference instructions to jury and sanctions and penalties.

E-Discovery: the Evidence

- The Federal Rules of Evidence determine how evidence is qualified and admitted into court
- **Rules 401 and 402**
 - 401 requires ESI to be relevant evidence
 - 402 determines which ESI is relevant
- <http://www.uscourts.gov/rules/EV2008.pdf>.

Two Types of ESI

- Computer-stored ESI
 - Files whose content is created by a non-computer process
 - E-mail, spreadsheets, word processed documents, presentations, but stored on a computer
 - ESI that is computer output like system-generated logs

E-Discovery: the Evidence

- Rules 801,802, and 803
 - Rule 801 defines hearsay in terms of ESI
 - Rule 802 disallows ESI unless “exceptions” exist
 - Rule 803(6) excepts computer-stored ESI from the hearsay rule “if the record is created and maintained as part of a regularly conducted business process”.
 - Qualified witnesses like Finance, HIM or IT professionals may need to testify about these records and their creation in the ordinary course of business.

E-Discovery: the Evidence

- **Rules 901 and 902**
 - 901(a) requires “knowledgeable testimony or documentation to authenticate ESI”
 - *A description of how the ESI is controlled by a witness who can testify to the data integrity management*
 - *A witness who can testify to the digital format of the file itself along with the metadata inserted into the file by the system or process*

E-Discovery: the Evidence

- Rules 901 and 902

- 901(b)(9)

- *A witness who can testify to how a system or process works to produce an accurate result*

- 901(11)

- *A record of regularly conducted activity can be self-authenticated to the court by a written declaration of its custodian (example: the HIM Director as custodian of the EHR can authenticate its integrity and management by a written declaration)*

E-Discovery: the Evidence

- Rules 1002, 1003, and 1004
 - 1002 requires that original ESI be produced unless there is an exception under the rules – the question of format
 - 1003 and 1004
 - 1003: Duplicate information is acceptable unless there is a question about the authentication of the original
 - 1004: Allows a duplicate of the original information to be admitted into court if the original is “lost or destroyed in good faith (original was not intentionally lost or destroyed)”

The Reality of E-Discovery

- “The reality of electronic discovery is it starts off as the responsibility of those who don’t understand the technology and ends up as the responsibility of those who don’t understand the law.”

- *Craig Ball*

- *Quoted from the Stellant Crescendo conference in 2007.*

Implications of the Amendment to the Federal Rules of Civil Procedure for Finance, HIM and IS

- Are electronically stored data and records available from active and archival media? Are records accessible within pretrial conference timeframes, i.e. 21 days before the first meeting with the opposition?
- Can Finance, HIM and IS accommodate the expected format for record production, i.e. “native format”? What about production of the metadata?
- What are potential costs and delays in record production?
- How can Finance and HIM help IS assess if the information requested is relevant to the claim or to the organization’s defense?

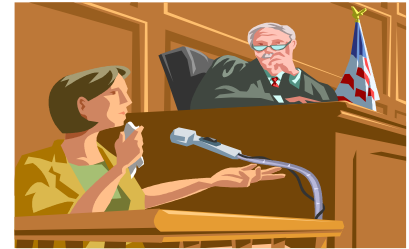
Implications of the Amendment to the Federal Rules of Civil Procedure for Finance, HIM and IS

- Will IS be able to demonstrate that the cost of such record production produces an “undue burden of cost”?
 - Quantify cost of inaccessibility
- Will IS, in conjunction with HIM and Legal Services, be able to establish which types of records can be deemed “privileged” under state law, and, therefore, non-reproducible?
- Can IS provide access to electronic systems confined to the information demanded for viewing in the request for production without jeopardizing other protected health information?

Implications of the Amendment to the Federal Rules of Civil Procedure for Finance, HIM and IS

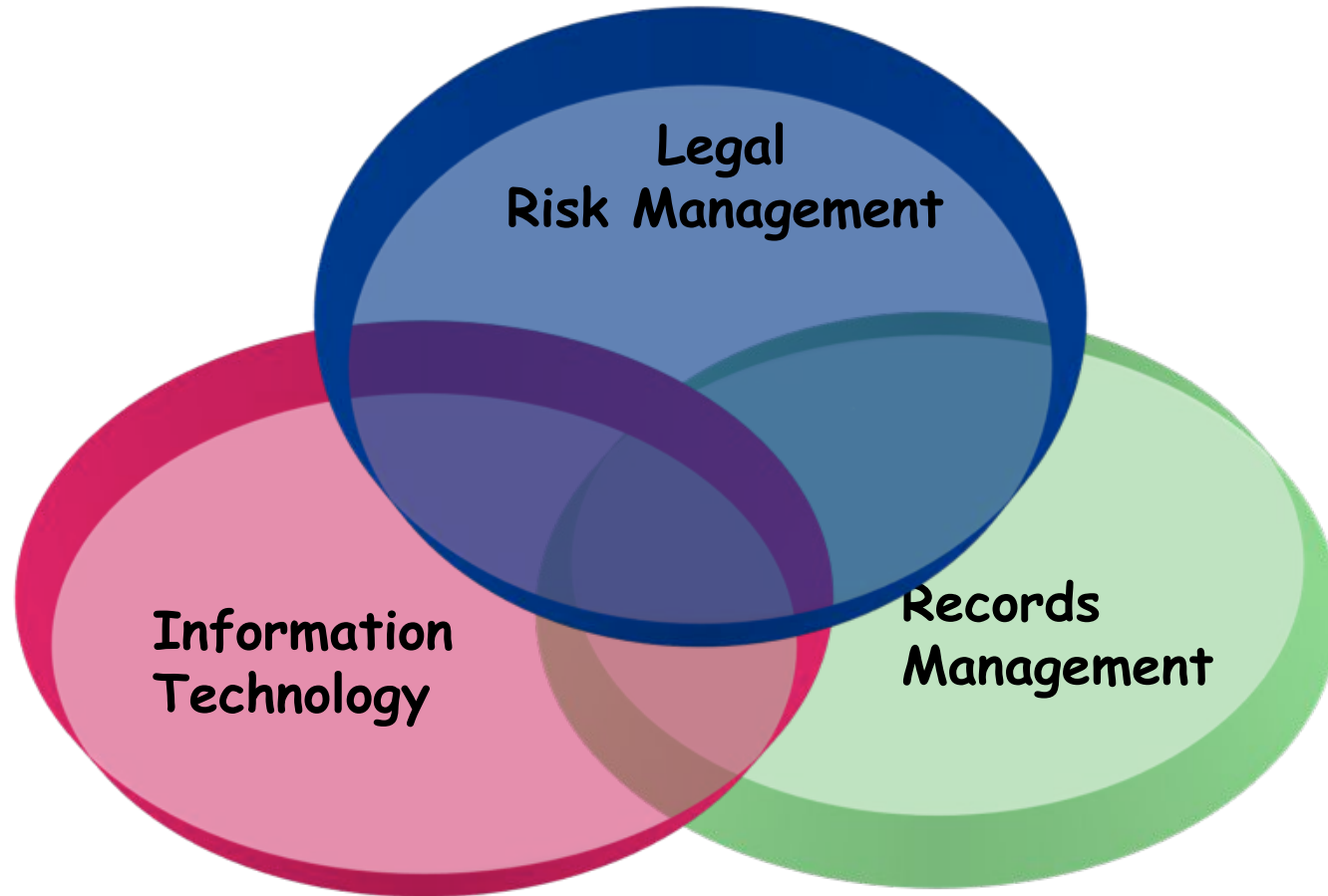
- Can IS testify to the authenticity of records and information stored electronically on their systems? Are there IS staff prepared to be expert witnesses about the “good faith” practices they have established for data management, archival, and destruction?
- Can IS apply a “legal hold” to forestall the destruction of an electronic record or a group of electronic records? Is there documentation to demonstrate valid “data losses” that happened in the “normal course of business”?

IT Professionals as Witnesses



- **L.Civ.R. 26.1(d) of the Local Rules of the U.S. District Court, District of New Jersey.**
 - “Prior to a FRCP 26(f) conference, counsel shall review with the client’s information management systems including computer-based and other digital systems, in order to understand how information is stored and how it can be retrieved...including currently maintained computer files as well as historical, archival, backup and legacy computer files.”
(Effective Date 2003)
- **Requires counsel to locate an “IT Witness.”**
 - “Counsel shall also identify a person or persons with knowledge about the client’s information management systems, including computer-based and other digital systems, with the ability to facilitate, through counsel, reasonably anticipated discovery.”

Operational Impact



Effective E-Discovery Involves An Integrated & Collaborative Approach To The Management of Electronic Health Information

Michelle Dougherty, RHIA, CHP and Kim Baldwin-Stried (Reich), MJ, MBA, RHIA, CPHQ

What is a successful Electronic Discovery Response Plan?

- It is built on the same foundation as a traditional discovery response
 - **The same**: analysis of the request, gathering and processing the data, attorney review, and eventual production to the requesting party
 - **The difference**: the technical expertise required to manage electronic discovery efficiently and effectively
 - The need for a collaborative relationship on both legal and technical fronts
 - *Electronic Discovery Response Plan slides developed from an article on discovery on www.lexisnexis.com/discovery.*

Electronic Discovery Response Plan

- The **Scope** of Electronic Discovery
 - Who are the document/record owners and likely key witnesses?
 - Who is knowledgeable about how and where their electronic records are created, stored and destroyed?
HIM's responsibility for the EHR and Finance's responsibility for financial records
- First Response:
 - Development of an organizational chart or grid of all the people who may have created, received, or shared potentially relevant information on their computers (e-mail, etc.)

Unconventional Records



Electronic Discovery Response Plan

- The duty to interview, investigate and disclose potentially responsive electronic information
- The duty to act to preserve electronic information that may be subject to production
 - *An analysis must be conducted to disclose to opposing parties information including a description by category and location of documents and data compilations, i.e. a search must be conducted of electronic systems for relevant information (McPeck v. Ashcroft)*

Sanctions & Penalties

- Relevant Case Law:

- 1. Coleman Parent Holdings, Inc. v. Morgan Stanley & Co., Inc., 2005 WL 679071 (Fla. Cir. Ct, Mar. 1, 2005).
 - An adverse inference instruction to jury for spoliation of evidence contained in emails and back-up tapes.
 - Jury awarded Coleman for over \$604 million compensatory damages and over \$850 million punitive damages.
 - Verdict award in excess of \$1.45 billion
- 2. Phoenix Four, Inc. v. Strategic Resources Corp., 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y.).
 - Failure to produce data timely from a “partitioned section of the hard drive” of a defendants desktop workstation.
 - Defendants and counsel ordered to reimburse Phoenix equally for statutory costs and attorneys’ fees and pay \$10,000 for redepositions of witnesses.

Electronic Discovery Response Plan

- The Gathering of Potentially Responsive Data
 - *The legal and technical teams must work together to prepare a plan for efficient data gathering*
 - When you know the “Who” in terms of data ownership, you can use your technical team to map out the physical location of potentially responsive electronic documents

Electronic Discovery Response Plan

- When you know the data owners and the kind of data at issue, you will need to know:
 - Where does the data reside for what dates?
 - Where is backup data stored? Where are documents saved on the network?
 - Where are e-mail messages kept?
 - Is archive on local drives, removable media?
 - Must deleted files be recovered and produced?
 - In what form must the data be produced?
 - Can existing IS staff handle the workload?

Electronic Discovery Response Plan

- Attorney review(\$\$)
 - Enormous volume of data
 - How will it be sorted? Numbered?
 - What is privileged?
 - Is there an established review protocol for electronic discovery?
 - How can we be certain nothing is omitted or overlooked?
 - What will be the cost of production?



Challenge: Record Production with New Legal Requirements

- Subpoenas, search warrants, summons for records on multiple media
- Class action suits that cross multiple organizational lines
- Requests for the content behind records: metadata, policies and procedures, process documentation

The Federal Rules of Civil Procedure:

Records Management & Security

- Mapping of all known Data Sources for the Enterprise- *“Where does all organizational content live?”*
- Lifecycle record management - *tying all content to a mandated organizational retention schedule*
- Identification and affidavits regarding security & mapping of systems

The Federal Rules of Civil Procedure: Records Management & Security

- Software acquisition requirements
- Decommissioning of systems - “system retirement”
 - Where does the content live now?
 - On what media? Who manages it?
- Ability to apply “legal holds” on individual electronic records or groups of electronic records

The Federal Rules of Civil Procedure:

Records Management & Security

- Record Production
 - The ability to supply the metadata for records when record production is required
 - The ability to demonstrate “best practices” in terms of data management and integrity
 - The ability to determine when electronic records were destroyed compliant with a retention schedule
 - If a failure to produce records is encountered, the organization must **prove cost was prohibitive**

Rules of Civil Procedure: The Federal **Records Management & Security**

- The ability to supply “good faith” process documentation -
 - Consistent measurements, practices and expectations
 - How will the organization demonstrate that the evidence from our computers has been properly preserved, authenticated and retrieved?
 - How will the organization demonstrate that measures are taken to preserve documents/records when there is a duty to preserve? (**Business Continuity, Disaster Preparedness**)

The Management of Unconventional Records

- E-Mail
 - Categorization
 - Retention
 - Destruction
 - Documentation
- Image Management
- Voice Management



HIPAA Security Expansion and What About ARRA?

- Extension of the Security Incident Response Team's role
 - Documentation of data incidents and losses
 - Audit trail management
 - PHR and HIE considerations
 - Development of the ability to “hold” data in each system in the Systems Inventory database (Configuration Management system)
 - Management of the decommissioning of systems of the EHR and others

LEHR Defined: The Model

- Hybrid record definition
- Definition of each source system
- Definition of all the metadata in the systems
- Definition of the native formats of all data/ records in the LEHR
- Disclosure Data Set – Clinical & Health plan
- Grid of Data Owners defined

Controlling the Cost of Electronic Discovery

- Implementation of Retention Management
- Develop early access/understanding of the possible scope of evidence
- Decrease storage costs through retention and capacity management
- Increase knowledge through the ability to find information more easily

E-Discovery Readiness Checklist

- ✓ 1. Establish A Litigation Response Team
 - Risk Management/Legal, IT, HIM
- ✓ 2. Review/Revise/Develop Information Management Plan
 - Define Your Records Management Program
 - Identify Custodians of Records
- ✓ 3. Review Legal Hold Practices
 - Also called: Litigation Hold, Preservation Orders, Preservation Requests
 - Determine Under What Conditions a Legal Hold Can Be Lifted
- ✓ 4. Develop Methodologies to Determine Actual Costs of Production of electronic records
- ✓ 5. Email Management Practices
 - Discourage PHI via E-mail
 - Privileged – Secure Server

E-Discovery Readiness Checklist

- ✓ 6. Review Records Storage, Retention and Destruction Practices
 - Costs, Locations, Schedules
- ✓ 7. Understand Features & Functionality of E-Discovery Systems
- ✓ 8. Back-Up Tapes and Legacy Systems
 - Categorize and Identify True Value In Retaining
 - If No Legal Duty or Business Use – Consider Destruction
- ✓ 9. Ensure electronic records are Being Appropriately and Effectively Managed to Avoid Sanctions and Penalties
- ✓ 10. Educate and Train Management and Staff
 - Monitor for Compliance With Established Policies
 - Provide Testing

Resources

- Summary of the Report of the Judiciary Conference Committee
 - <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf>
- AHIMA Practice Brief & Article
 - The New Electronic Discovery Civil Rule
 - http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031860.hcsp
 - E-Discovery and HIM: How Amendments to the Federal Rules of Civil Procedure Will Affect HIM Professionals
 - http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032032.hcsp?dDocName=bok1_032032
- The Sedona Conference Resources
 - Legal Think Tank
 - www.thesedonaconference.com