

# EMRs, EHRs and e-Discovery – Positive Strategies for Managing Under the New Paradigm



CHITA Forum 2008/09 Series - "Living with an EMR" #3  
April 22, 2009 – Shoreline, Washington

© 2009 Christiansen IT Law

*John R. Christiansen, J.D.*  
**Christiansen IT Law**  
**Privacy/Security/Compliance**

2212 Queen Anne Avenue North #333  
Seattle, Washington 98109  
206.301.9412  
john@christiansenlaw.net

# Presenter Bio

***John R. Christiansen, J.D. - Christiansen IT Law***

## **Information Technology Law: Privacy, Security, Compliance and Risk Management**

- Chair, ABA Committees on Healthcare Privacy, Security and Information Technology (2004 – 06); on Healthcare Informatics (2000 – 04); and PKI Assessment Guidelines Health Information Protection and Security Task Group (2000 – 2003)
- Adjunct Faculty, University of Washington Information School and Center for Information Assurance and Cybersecurity; and Oregon Health and Sciences University Division of Medical Informatics and Outcomes Research (2000 – 2003)
- Technical Advisor, Health Information Security and Privacy Collaboration (“HISPC”)(2005 – present)
- Publications include ***Legal Speed Bumps on the Road to Health Information Exchange, Journal of Health and Bioscience Law*** (2008); **An Integrated Standard of Care for Healthcare Information Security** (2005); **Electronic Health Information: Security and Privacy Compliance under HIPAA** (2000); etc.

# Our Agenda

- Distinguishing EMRs and EHRs
- Integrating Discovery of Electronically Stored Information (ESI) into EMR Management
- Ensuring EMR ESI Is Admissible in Court
- The Problem of EHR ESI Management

# What's In a Name? EMR

An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff ***within one health care organization.***

- **National Alliance for Health Information Technology, Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms (April 28, 2008)**

# What's In a Name? EHR

An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff ***across more than one health care organization.***

- **National Alliance for Health Information Technology, Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms (April 28, 2008)**

# What's In a Name? EHR

- A repository of consumer health status information in computer processable form used for clinical diagnosis and treatment for a broad array of clinical conditions.
- Must be interoperable with other EHRs
    - **Stark and Antikickback EHR Regulations**

# What's In a Name? EHR

The term “electronic health record” means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

– **HITECH § 13400(5)**

# What's In a Name? Confusion

The Grand Jury discovered three related problems regarding EMR within HHS: (1) there is no formal definition of Electronic Medical Records at any level, (2) communication of goals and strategies to those who will use and be affected by an EMR system is confusing and ineffective, and (3) the County cannot anticipate EMR development costs if there is no understanding of the scope of the project.

- **2006-2007 SANTA CLARA COUNTY CIVIL GRAND JURY REPORT, ELECTRONIC MEDICAL RECORDS: HEALTHCARE COMPLEXITY, LACK OF DEFINITION AND COMMUNICATION CREATES CONFUSION**

# Definition by Control and Use

- EMR: Single provider-controlled, for same provider's use
- EHR: Multiple provider or delegated control, for multiple providers' use

# Evidence in the Traditional Medical Record



# Evidence in the Traditional Medical Record

## Medical Record Basic Requirements

- Appropriate content (per accreditation, regulatory, risk management requirements, etc.)
- Created contemporary with or very soon after care episode
- Accuracy confirmed by responsible professional (physician)
- Signed by responsible professional
- Changes tracked and signed
- Retained per legal requirements, risk management needs

# Evidence in the Traditional Medical Record

## Discovery is (Relatively) Easy

- Medical records are (supposed to be) in the file(s)
- Files are (supposed to be) in the records/file room(s) or checked out to identified individual
- Someone is (supposed to be) managing the records
- Relevant records can be identified, located, reviewed and produced

# Evidence in the Traditional Medical Record

## Documents Admissible as Evidence

- Contents are hearsay, admissible per “business records exception”
- Made in the “regular course of business”
- Contemporaneous or very soon after episode recorded
- Circumstances indicate probable accuracy
- “Wet” signatures (ink or stamp) readily authenticated by visual inspection

# New E-Discovery Rules

Amendments to Federal Rules of Civil Procedure 16, 26, 33 – 37, 45

- Apply to “electronically stored information” (ESI)
  - **Not the same as “document”**
  - **Stored in “information systems” and/or “electronic storage systems”**
  - **Production of discoverable ESI required unless it is “not reasonably accessible”**
- Washington version currently under development by WSBA Court Rules & Procedures Committee
- Existing Washington rules based on Federal, Federal Rules are persuasive authority

# New E-Discovery Rules

## What's “discoverable” ESI?

- Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense — including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. . . . Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.
  - FRCP 26(b)(1)

# Evidence in the EMR

## Human-Generated EMR Content:

- Administrative information
- Clinical observations, progress notes, etc.
- Scanned documents produced internally or forwarded by other providers
- Provider – patient, provider – provider email

# Evidence in the EMR

## System-Generated EMR Content:

- Images and other device output
- Drug interaction and allergy alerts
- Care guidelines
- Reports and prescriptions, ancillary notes
- Metadata

# Evidence in the EMR

## EMRs Presents New ESI Retention Problems

- Washington medical records retention: 10 years or age of majority +3 years.
  - RCW 70.41.190
- Risk management: Until statute of limitations runs on possible professional liability claims
  - Washington: 3 – 8 years from discovery. RCW 4.16.050
- What should be included? Authentication metadata, etc.?
- Can you retrieve and produce ESI from EMR data sources from 2001? From 1988?

# Evidence in the EMR

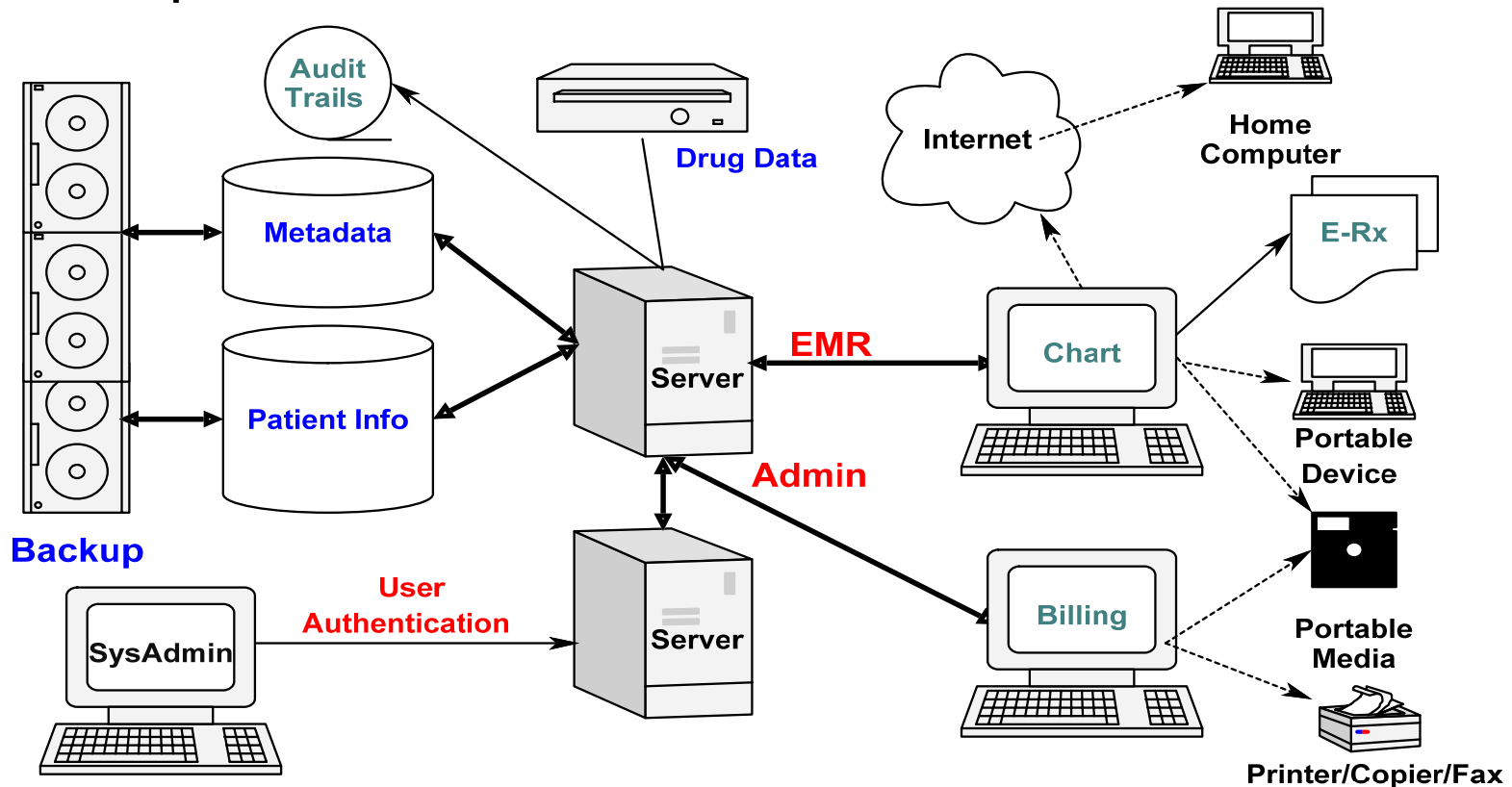
## EMRs Present New Discovery Problems

- Relevant data may reside in multiple locations
- Relevant data may inadvertently be altered or destroyed
- What form should production take?

# Evidence in the EMR

Find the ESI in this picture

- Now produce it.



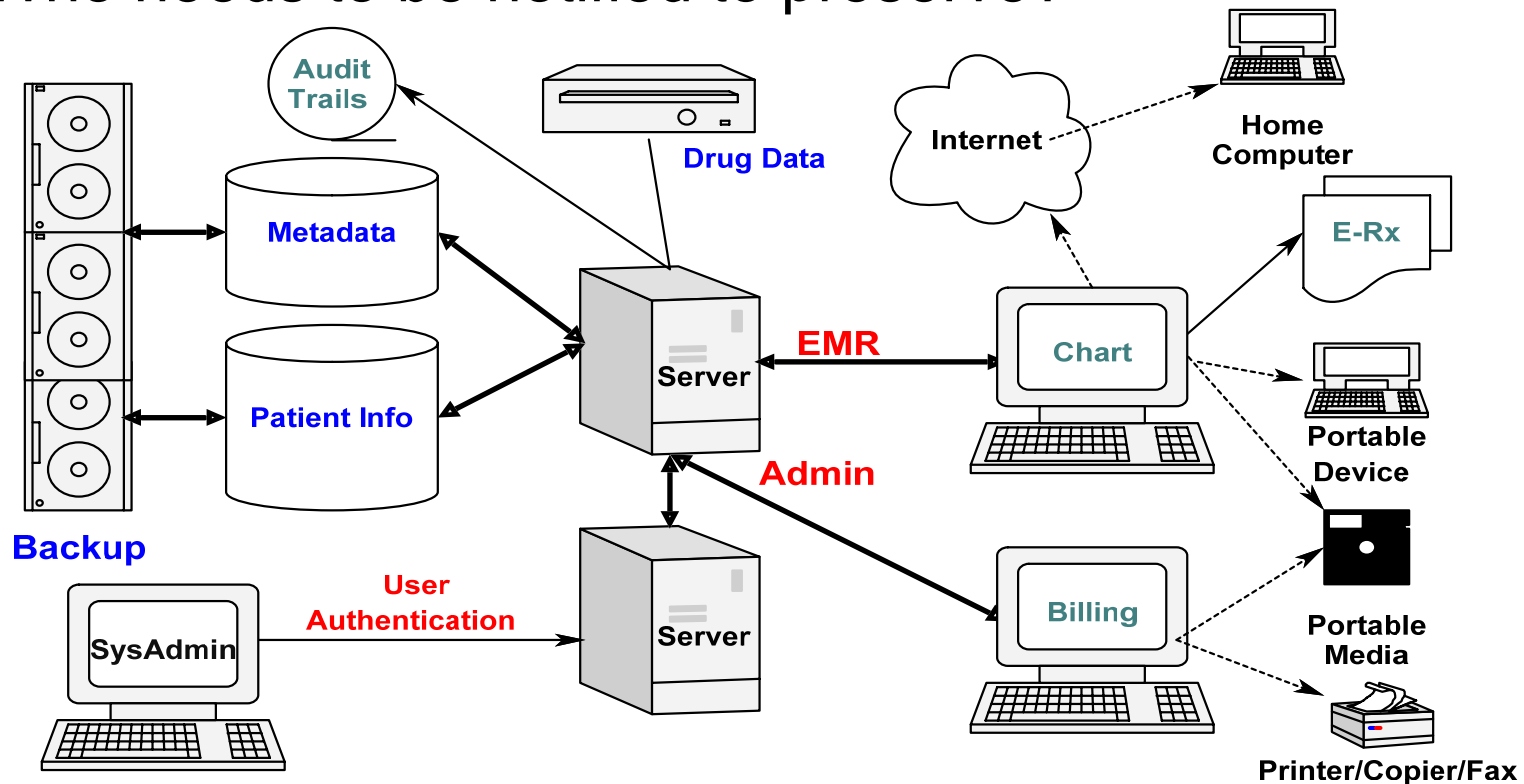
# Potential Spoliation and the “Litigation Hold”

- Knowledge of actual or prospective litigation creates duty to preserve potentially relevant ESI
  - Levy v. Remington Arms Co., Inc. (8<sup>th</sup> Cir. 1987)
  - No “bright line” test
  - “Never” events?
- Culpable intent – willful, reckless, negligent
  - E.g. GTFM, Inc. v. Wal-Mart Stores (SDNY 2000)(attorney’s misunderstanding re length of time records maintained)
- Potentially nasty sanctions
  - Financial penalties, adverse inferences against spoliator, etc.

# Potential Spoliation and the “Litigation Hold”

What data retention policies apply to the ESI in this picture?

- Who needs to be notified to preserve?



# Evidence in the EMR

## EMRs Presents New Admissibility Problems

- Authentication of content
- Authentication of content creators
- Validity of computer-generated content

# EMR Content Integrity

## Electronic Signatures as Authentication

- Signature provides evidence of:
  - **Authorship of record**
  - **Accuracy and completeness of record**
- How do you authenticate the signature?
  - **Presumed valid if made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; was kept in the course of the regularly conducted activity; and was made by the regularly conducted activity as a regular practice.**
    - **Fed. Rule of Evid. 902(4)**

# Electronic Signatures

## Applicable Laws

- Federal Electronic Signatures in Global and National Commerce Act (E-SIGN), enacted 2000, codified at 15 USC. §§ 7001 et seq.
  - **Supersedes inconsistent federal and state laws**
- Uniform Electronic Transactions Act (UETA), adopted in most states
  - **Consistent with, expressly allowed by E-SIGN**
- States without UETA are governed by E-SIGN
  - **Washington for one**

# Electronic Signatures

## Definitions:

- “Electronic signature:” “An electronic sound, symbol, or process, attached to or legally associated with a contract or other record and executed or adopted by a person with intent to sign the record.”
  - **15 USC § 7006(5)**
- “Record:” “Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.”
  - **15 USC § 7006(9)**

# Admissibility and Credibility of ESI

## Distinguish Admissibility for Different Types of ESI

- Electronically stored/human-generated
- Automatically generated by software

## General Rule on Admissibility:

- Prima facie authentication, sufficient for “reasonable juror” to find evidence is what it claims to be.
  - US v. Tank, 200 F.3<sup>rd</sup> 627 (9<sup>th</sup> Cir. 2000)(chat room log printouts admitted based on testimony of log producer re production processes), citing Fed.R.Evid. 901(a).

# Admissibility and Credibility of ESI

- In re Vinhee (9<sup>th</sup> Cir. 2005): American Express monthly statement entries inadmissible due to inadequate evidence about software used to generate entries
- US v. Jackson (U.S. D. Neb. 2007): “Cut and paste” of chat room documents inadmissible due to altered context
- United States v. Jackson (7th Cir. 2000) Website postings inadmissible due to risk of spoofed authorship
  - See generally AHIMA e-HIM Work Group on Maintaining the Legal EHR, *Update: Maintaining a Legally Sound Health Record - Paper and Electronic*, J.AHIMA 64A - L (November-December 2005) and Imwinkelreid, *Evidentiary Foundations* (5th ed. 2002)

# Admissibility and Credibility of ESI

The 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.

- In re Vinhee, (9<sup>th</sup> Cir. 2005)

# Admissibility and Credibility of ESI

How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions.

- In re Vinhee, (9<sup>th</sup> Cir. 2005)

# Admissibility and Credibility of ESI

How changes in the database are logged or recorded, as well as 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.

- In re Vinhee, (9<sup>th</sup> Cir. 2005)

# Admissibility and Credibility of ESI

The problem . . . is that it [defendant] did not have adequate procedures to maintain the security of intranet passwords, to restrict authorized access to the screen which permitted electronic execution of the arbitration agreement, to determine whether electronic signatures were genuine or to determine who opened individual emails. . . . The Court recognizes that defendants' burden of proof is not absolute certainty, but merely a preponderance of the evidence. At the same time, Dillard's has not demonstrated the efficacy of its security procedures with regard to electronic signatures. . . . [Defendant] has the burden of proof and its evidence that plaintiff executed the arbitration agreement is not persuasive.

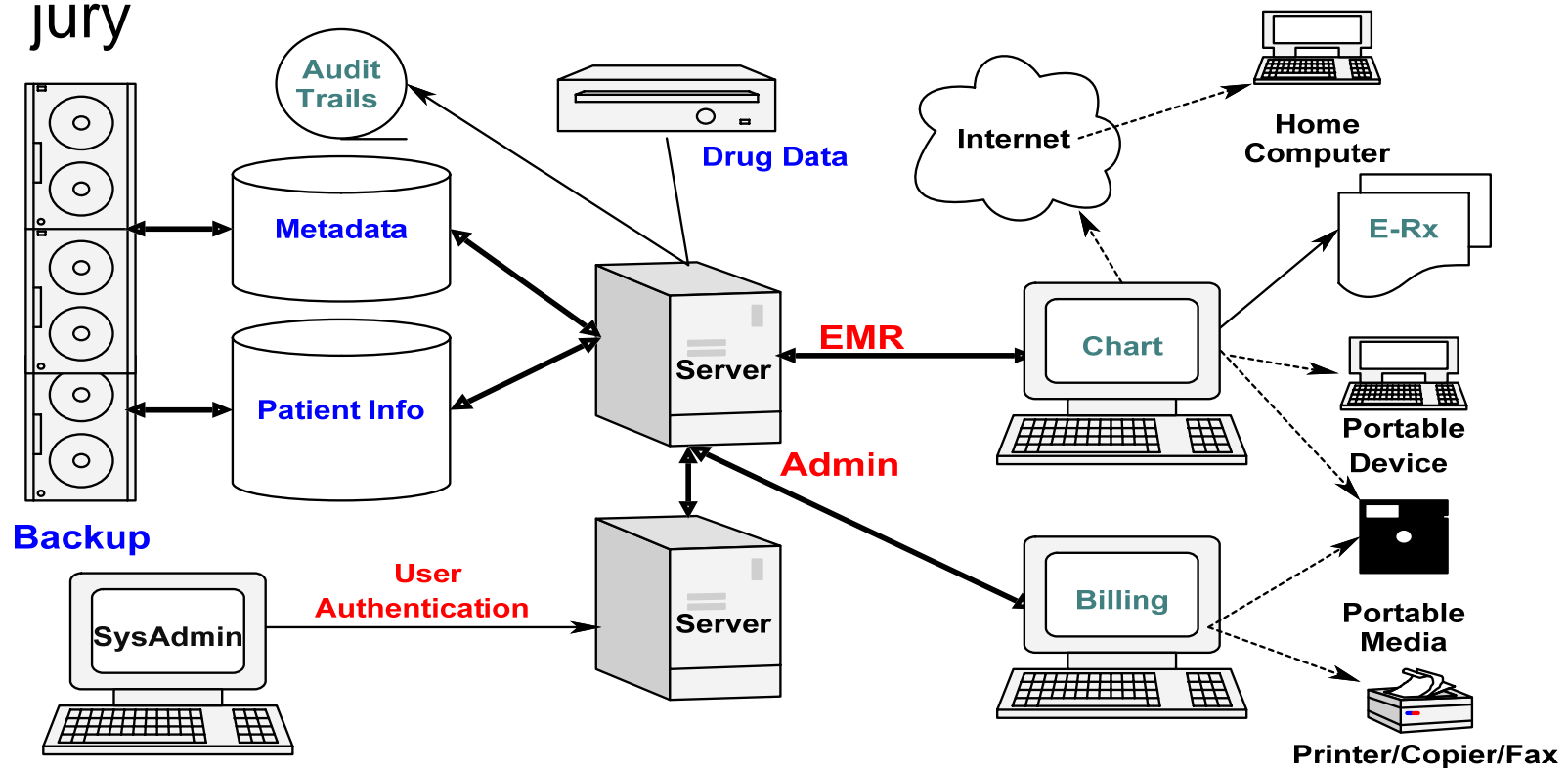
– Kerr v. Dillard Stores, (U.S.D.Ct. Kansas 2009)

Under UETA, but credibility analysis would apply in WA

# Admissibility and Credibility of ESI

## Answer Vinhee's "logical questions"

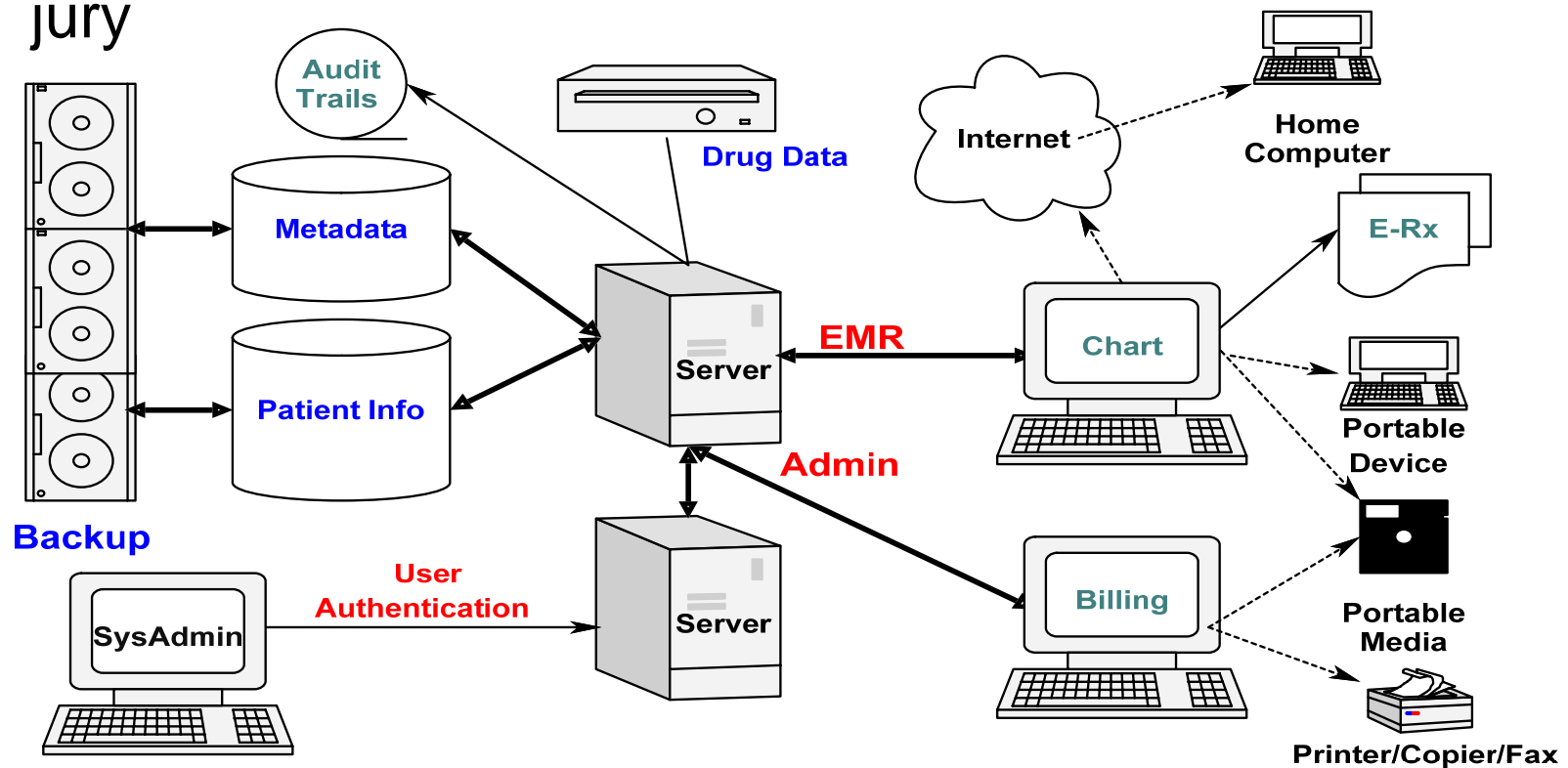
- In plain English, first to the judge and then to the jury



# Admissibility and Credibility of ESI

## Answer Vinhee's "logical questions"

- In plain English, first to the judge and then to the jury



# Use Policy to Define Electronic Legal Medical Record (e-LMR)

## Included Information

- Core medical record data: Demographic, clinical etc. per regulatory, accreditation, risk management requirements
- User authentication, including user access and electronic signatures
- Metadata necessary to prove reliability of core medical record data: Audit trails, timestamps, etc.
- Clinical decision support information relied upon in diagnosis/treatment

# Use Policy to Define e-LMR

## Included Hardware

- Identify hardware and devices: Servers, workstations, printers/copiers/fax, laptops and tablets, PDAs, etc.
- Include all under client control: Owned, leased, outsourced, user-owned/client-authorized
  - **No unauthorized devices!**

# Use Policy to Define e-LMR

## Included Software

- Identify applications and operating systems: Some hardware will have multiple applications; some applications may run on multiple servers, etc.
  - **Know your versions! Keep up-to-date!**
- Know what output is automatically generated and be able to explain how
  - **Know your vendors and get their cooperation**
  - **Put evidentiary support requirements in contracts**

# Use Policy to Define e-LMR

## Know Information Storage, Processing and Output Sites

- Databases, servers, backup media, workstations, personal computers, portable devices, portable media, printers, faxes, etc.
- Not just clinical data (“medical record documentation”), but associated non-clinical data and metadata
- **No “private databases!”**

# Use Policy to Define e-LMR

## Identify “Information Life-Cycles”

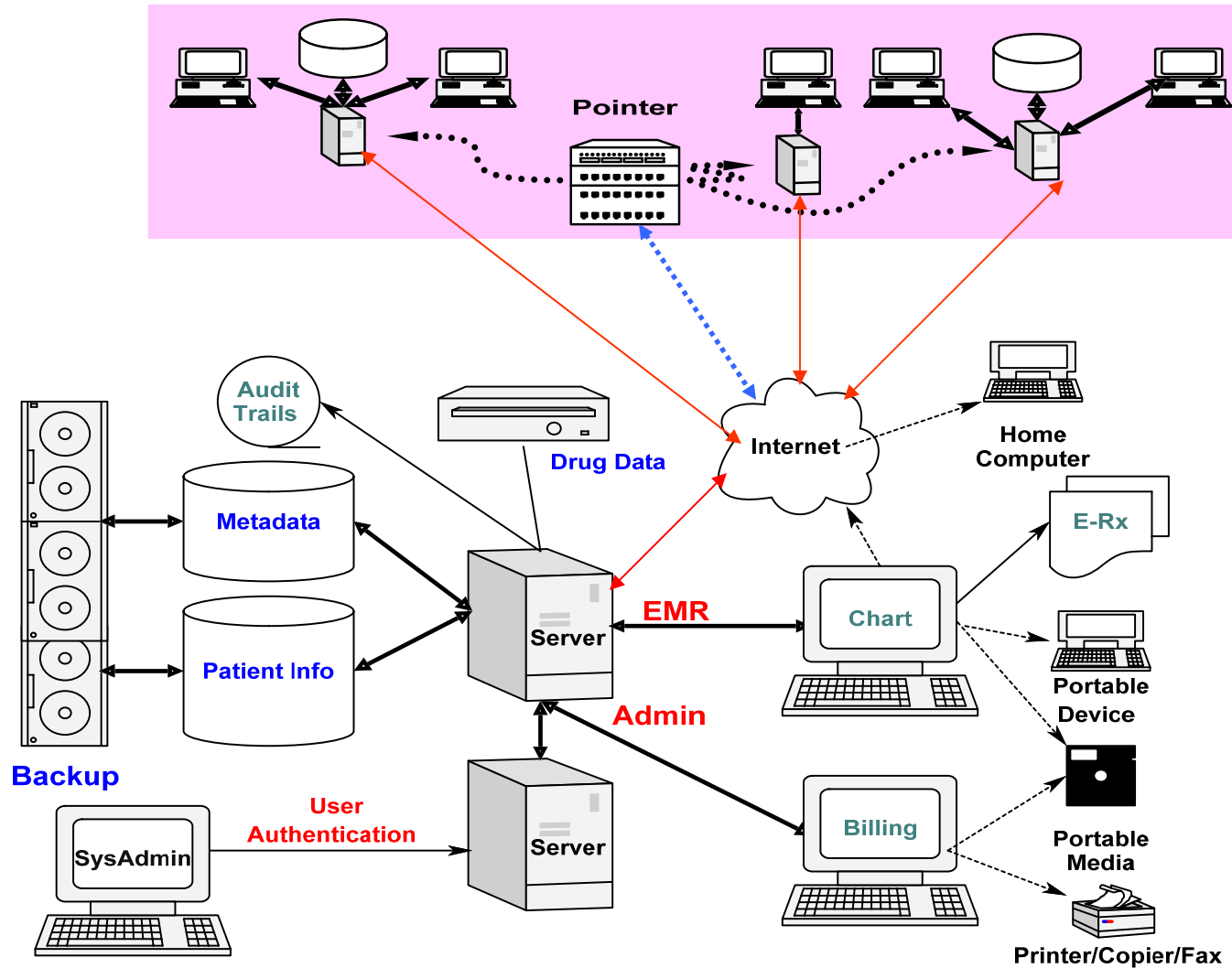
- Intake, processing, operational storage, backup, archiving/retention period, destruction
- Different types of information have different lifecycles
  - **“Medical record” vs. administrative vs. metadata, etc.**
  - **Consider risk management needs to retain information longer than legally required, e.g. electronic signature metadata associated with EMR clinical entries**
- Routine destruction per policy is less likely to count as spoliation

# Use Policy to Define e-LMR

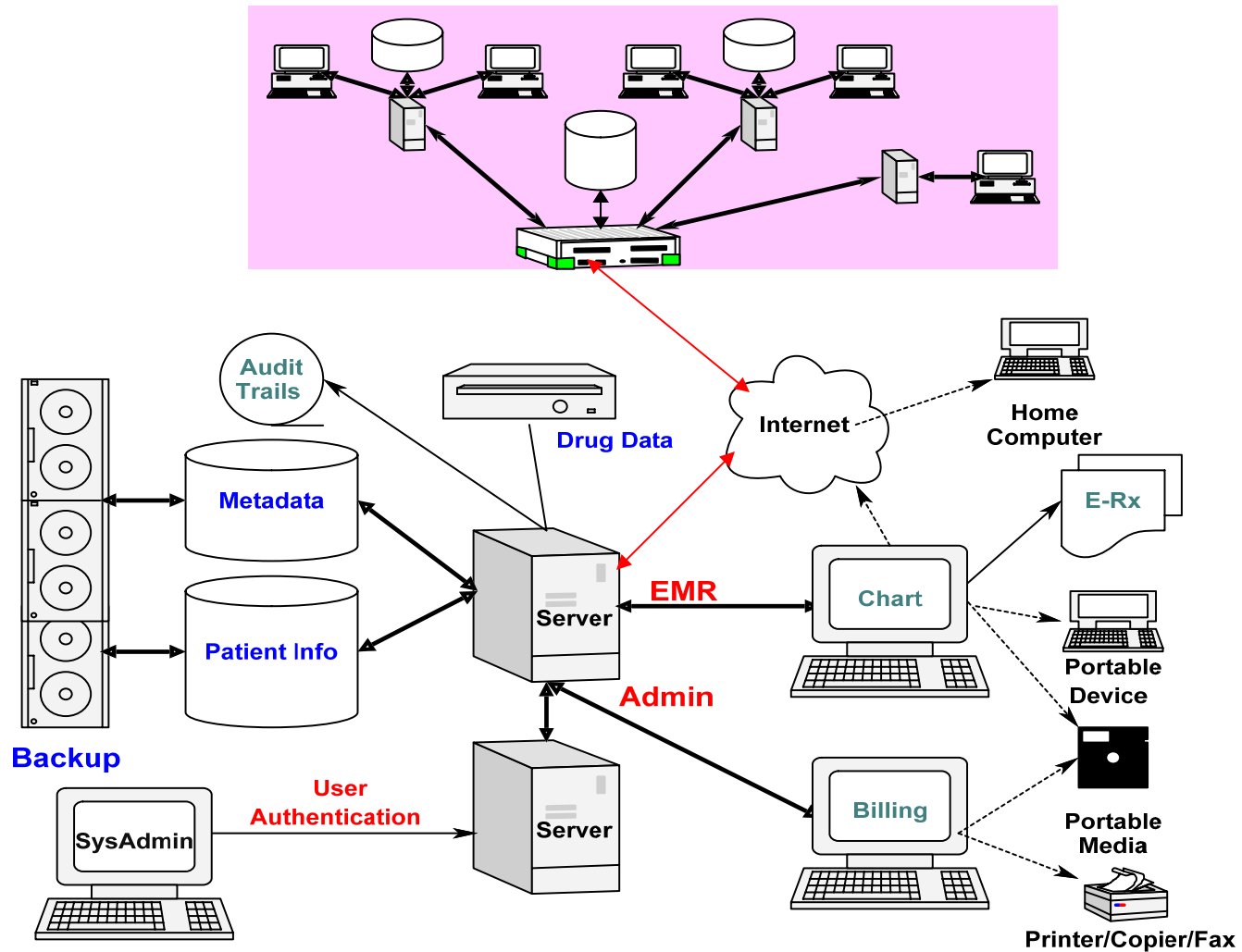
## Define Relationships Among Responsible Offices

- Information policy development, implementation and enforcement
- Change review and management
- Information custodians (“owners”)
- Litigation hold issuance and execution responsibilities
- HIM and IT staff trained and available to help with discovery and qualified to testify
  - **Coordinate HIM, legal and IT!**

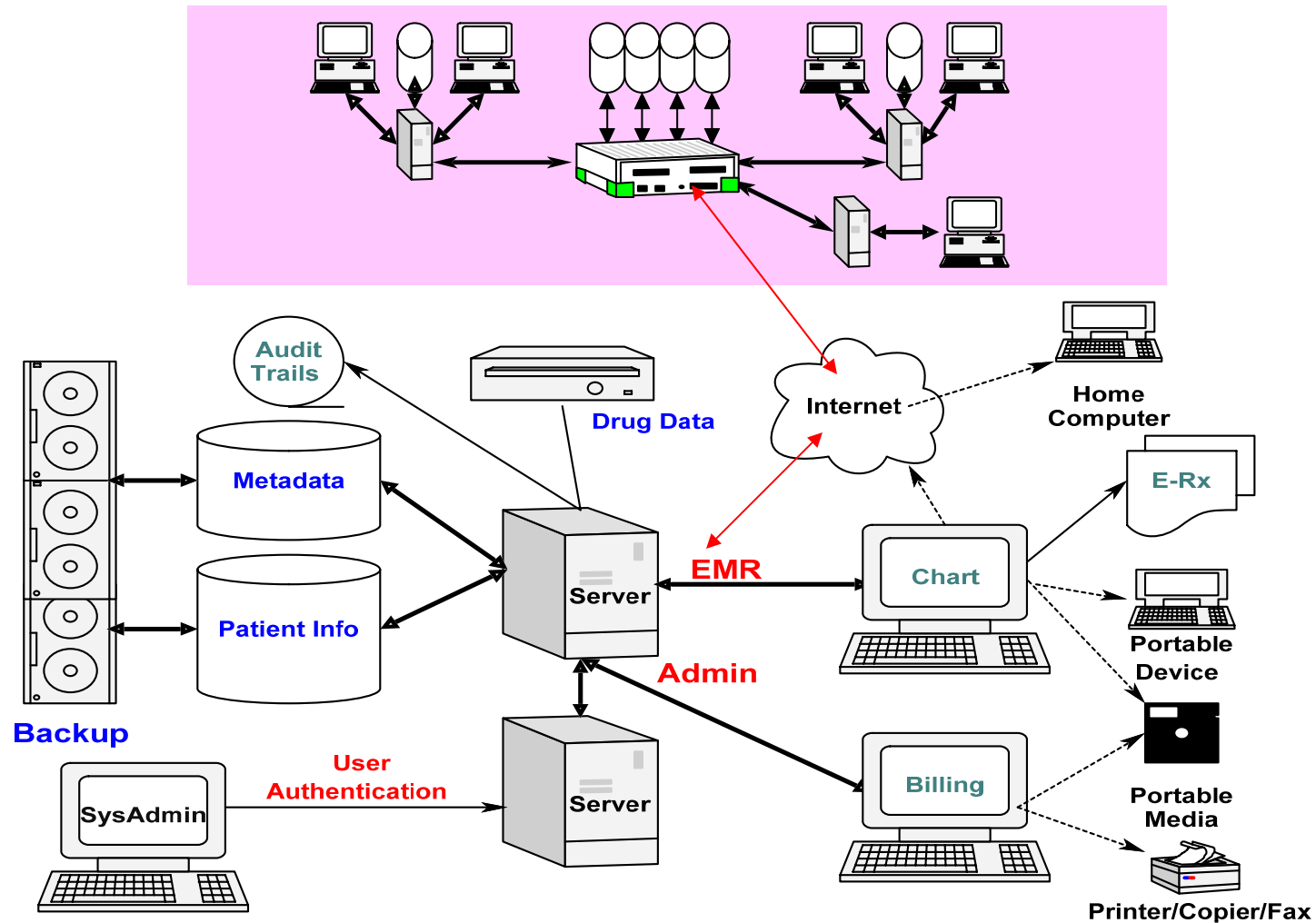
# Integrating Peer-to-Peer EHR Into e-LMR?



# Integrating Centralized EHR Into e-LMR?



# Integrating “Warehouse/Silo” Into e-LMR?



# Integrating EMRs and EHRs

Lots of questions, few answers

Policies to consider:

- **What has to be imported into the e-LMR for legal, risk management purposes?**
- **How is information authenticated?**
- **How are content creators authenticated?**
- **What kinds of ancillary information is created and maintained?**
- **What should be rejected as unreliable? How should rejection be documented?**
- **What are the information life-cycles?**
- **Who is responsible for e-discovery?**

# *Questions? Thanks!*

*John R. Christiansen, J.D.*

**Christiansen IT Law**

**Privacy/Security/Compliance**

**2212 Queen Anne Avenue North #333**

**Seattle, Washington 98109**

**206.301.9412**

**john@christiansenlaw.net**