Understanding the Importance of Metadata Management

Presented by Carol Selvey, MHSA, CPHIMS, FHIMSS,
Associate Vice President, Business Development
James Lawson
Associate Vice President, Strategic Integration Services
Iatric Systems, Inc.
August 17, 2010
Agenda

• Healthcare IT Challenges for Information and Records Managers
• Definition and Implications of Metadata
• Metadata versus Audit Logs
• Metadata and Standards
• Legal and Regulatory Considerations
• Metadata Call to Action
Complexity of Current EHR Landscape

- Transition from paper to digital records
  - Changing role from document to data-centric
  - New role as enterprise content and information management

- Significant regulatory activity

- Coordination of Care initiatives requiring cross-enterprise record/information exchange (NHIN)

- EHR spans multiple systems and involves multiple views

- Need for multidisciplinary EHR governance
Metadata & EHR Management

INTEROPERABILITY DATA EXCHANGE

Clinical Document Architecture (CDA)
CCD, CRS, CCR

Record Locator Service/
Enterprise Master Patient Index

HOSPITAL

EMERGENCY/URGENT CARE

PRACTICE/CLINIC

PERSONAL HEALTH RECORD
MICROSOFT/GOOGLE

PATIENT PORTAL

STATE/FEDERAL REPORTING

LONG TERM CARE

AHIMA © 2007
## HIMSS Analytics U.S. EMR Adoption Model

<table>
<thead>
<tr>
<th>Stage</th>
<th>Cumulative Capabilities</th>
<th>2010 Q1</th>
<th>2010 Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 7</td>
<td>Medical record fully electronic; HCO able to contribute CCD as a byproduct if EMR; Data warehousing in use</td>
<td>0.7%</td>
<td>0.8%</td>
</tr>
<tr>
<td>Stage 6</td>
<td>Physician documentation (structured templates), full CDSS (variance &amp; compliance), full RPACS</td>
<td>1.8%</td>
<td>2.6%</td>
</tr>
<tr>
<td>Stage 5</td>
<td>Closed loop medication administration</td>
<td>5.0%</td>
<td>3.2%</td>
</tr>
<tr>
<td>Stage 4</td>
<td>CPOE, CDSS (clinical products)</td>
<td>7.7%</td>
<td>9.7%</td>
</tr>
<tr>
<td>Stage 3</td>
<td>Clinical documentation (flow sheets), CDSS (error checking), PACS available outside Radiology</td>
<td>50.0%</td>
<td>50.2%</td>
</tr>
<tr>
<td>Stage 2</td>
<td>Clinical Data Repository, Controlled Medical Vocabulary, CDSS, may have Document Imaging</td>
<td>16.5%</td>
<td>15.5%</td>
</tr>
<tr>
<td>Stage 1</td>
<td>Ancillaries-Lab, Radiology, Pharmacy- all installed</td>
<td>6.9%</td>
<td>6.8%</td>
</tr>
<tr>
<td>Stage 0</td>
<td>All Three Ancillaries Not Installed</td>
<td>11.4%</td>
<td>11.2%</td>
</tr>
</tbody>
</table>

Data from HIMSS Analytics Database™ 2010

N=5223  N=5217
ARRA Audit Requirement

“The date, time, patient identification and user identification must be recorded when electronic health information is created, modified, accessed or deleted; and an indication of which action(s) occurred and by whom must also be recorded.”

- Standards and Certification Criteria Final Rule, July 13, 2010

What is Metadata?

- Embedded information about the content, context and structure of records
  - When (date and time)
  - Where (patient ID)
  - Who (user ID)

- The key to effective record capture/creation, maintenance/modification, retention, deletion
- “Snapshot” of latest activity (single use)
- Differentiates electronic health records from an audit perspective
What is Metadata?

- Validates and quantifies the authenticity, reliability, usability and integrity of information over time and enable the management and understanding of electronic information
- Varies by organization and within jurisdictions according to:
  a) business needs;
  b) jurisdictional regulatory environment;
  c) risks affecting business operations.
Metadata Sample

- When (date and time)
- Where (file location)
- Who (last changed by)
- What (size, type, name)
EHR Metadata Sample Data Elements

Continuity of Care Record Metadata Sample

小编一起<Attribute><Name>PT_ID</Name><StrValue>21431256</StrValue></Attribute><Attribute><Name>PT_ID_SITE</Name><StrValue>ABC</StrValue></Attribute><Attribute><Name>PT_NAME</Name><StrValue>CCDTEST</StrValue></Attribute>

Site MRN
Site of MRN
Patient Name
Visit/Account #
Sending Facility
Sending Application
Document Name
Document ID
Document Version
Date Created
Purpose of Document-> lab result, medication reconciliation
File size
Metadata versus Audit Logs

- Metadata is defined for each individual file whereas audit logs are defined for multiple records
- Record system and application activity
- Detect security violations, performance problems and application flaws
- Insurance Policy
- Support operations and system administration
Audit Time?
(100 bed facility)

Assuming 52,602 PT Access Daily:

- 1 Auditor spending 5 seconds per audit = 263,010 seconds or 4383 minutes or 73 hours
- 10% of that is **7.3 hours**
- Realistically, it is much higher even into the minutes per audit
- For example: 10% review @ 30 secs per audit review equates to 157,800 seconds or 2630 minutes or **43.83 hours**
Why is Metadata Important for Managing EHR Data?

- Serves as key differentiator between paper and electronic records
- Provides a reference point for large volumes of data and related audit trails
- Maintains essential record to ensure effective data integrity, confidentiality and access/availability
EHR Copy & Paste Auditing

- Review advantages and risks
- Audit plan policy development and testing
- Types of copy functions
  - Paste from outside the EHR
  - Partial duplication inside the EHR
  - Duplication-create new record (duplicate)
- Retrospective analysis (work lists)
- Sample Policy

What Standards Exist for Metadata?

Metadata standardization can be complex, involving a variety of organizations, including the following:

- Standards development organizations (SDOs) that specify details of metadata
- Domain (medical) and business organizations that use the metadata
- Regulatory organizations that enforce adherence to metadata standards
Sample Metadata Standards

American Society for Testing Materials (ASTM)

- **Continuity of Care Record (CCR):** XML-based standard for the movement of “documents” between clinical applications; responds to the need to organize and make transportable a set of basic information about a patient’s health care that is accessible to clinicians and patients.

HL7- CCD (Health Level 7)

- **Continuity of Care Document (CCD):** Result of a collaborative effort between the Health Level Seven (HL7) and to “harmonize” the data format between ASTM’s Continuity of Care Record (CCR) and HL7’s Clinical Document Architecture (CDA) specifications.

IHE (Integrating the Healthcare Enterprise)

- **Audit Trail and Node Authentication (ATNA)**
# How Specific Should Audit Log Requirements Be?

<table>
<thead>
<tr>
<th>Least Restrictive</th>
<th>HIPAA</th>
<th>1. Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information; and 2. Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderately Restrictive</td>
<td>Intra-enterprise audit integration</td>
<td>Construct a continuous audit trail across systems within an organization using ATNA</td>
</tr>
<tr>
<td>Most Restrictive</td>
<td>Cross-enterprise ATNA</td>
<td>Ability for organization in a health information exchange to query another organization's audit trail. This is helpful in maintaining trust because there is a virtual audit trail for the community.</td>
</tr>
</tbody>
</table>
Metadata & EHR Certification


- Access Control
- Audit
- Authentication
- Consent Management
- Consumer EHR
- HIPAA De-Identification
- Data Integrity
- Transmission Security
Support logging to a common audit engine using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile.

Demonstrate System Logging with an Audit Trail worksheet:
• Transaction timestamps
• Systems effected (hardware/software components)
• Event types
• Subject identities (document source, document consumer)
• Outcomes
Why Do Regulatory & Legal Requirements Necessitate Metadata?

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Federal Rules for Civil Procedure (FRCP)
- Sarbanes-Oxley (SOX) Section 404
- Civil False Claims Act
- American Recovery & Reinvestment Act (ARRA/HITECH)
- State Statutes

➢ Case Law Metadata requirement for outputs admitted into legal proceedings
Metadata & HIPAA

- Implement **security measures** to reduce risks and vulnerabilities to a reasonable and appropriate level
- Implement **procedures** to regularly review records of information system activity, such as audit logs, access reports and security incident-tracking reports
- Implement **hardware, software or procedural mechanisms** that record and examine activity in information systems that contain or use electronic protected health information
- Retain documentation for at least **six years** from the date of its creation or the date when it was last in effect, whichever is later
Metadata & the Federal Rules for Civil Procedure: eDiscovery Amendments

- **Rule 16**: Pretrial Conference, Scheduling and Management
  - Define data stores and effective mechanisms for retrieving information in a timely manner

- **Rule 26**: Duty to Disclose; General Provisions Governing Discovery
  - Record retention and destruction policies - ability to locate/retrieve data and know where data is stored

- **Rule 34**: Producing Documents and Electronically Stored Information
  - Deliver data in “reasonably usable form”

- **Rule 37**: Safe Harbor Provision
  - Protection against data loss
Metadata Call to Action

Establish effective EHR governance

- Form interdisciplinary team
- Establish procedures, training and technology solutions
- Develop Policies and Procedures
  - Compliance and e-Discovery Response
    - Discovery and Disclosure
    - Retention and Destruction
    - Litigation hold or preservation order
    - Spoilation
    - Disaster recovery

- Evaluate where ePHI is located and who owns the data
Metadata Call to Action

• Examine effectiveness of EHR security features
  – Audit Trails
    • Perform security risk assessment
    • Test audit availability and accuracy
    • Recognize metadata as a functional requirement
  – Access Controls (role-based access)
  – Data Encryption
  – Patient Consent
Challenges We Face

- Lack of retention standards
- Lack of audit data standards
- Policy has to catch-up!
- Growing volume of data
- Be a part of the strategic planning process
Questions?

Thank you for attending!

To obtain a copy of the bibliography for this presentation, please contact me at:

Carol.Selvey@iatric.com