

Author(s): David A. Wallace and Margaret Hedstrom, 2009

License: Unless otherwise noted, this material is made available under the terms of the **Creative Commons Attribution Noncommercial Share Alike 3.0 License:**
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

We have reviewed this material in accordance with U.S. Copyright Law **and have tried to maximize your ability to use, share, and adapt it.** The citation key on the following slide provides information about how you may share and adapt this material.

Copyright holders of content included in this material should contact open.michigan@umich.edu with any questions, corrections, or clarification regarding the use of content.

For more information about **how to cite** these materials visit <http://open.umich.edu/education/about/terms-of-use>.

Citation Key

for more information see: <http://open.umich.edu/wiki/CitationPolicy>

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }



Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)



Public Domain – Expired: Works that are no longer protected due to an expired copyright term.



Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.



Creative Commons – Zero Waiver



Creative Commons – Attribution License



Creative Commons – Attribution Share Alike License



Creative Commons – Attribution Noncommercial License



Creative Commons – Attribution Noncommercial Share Alike License



GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }



Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }



Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

SI 655

Management of Electronic Records

Week 13 - April 20, 2009

Wrap Up: Towards Transparency,
Accountability, and Governance

Course Themes

- Recordkeeping Requirements
- Trust
- Evidence
- Promoting Accountability
 - Standards and Best Practices
 - Tools and Technology
 - Compliance and Audit
 - Social Demand & Incentives
- Contradictions:
 - FOIA, Privacy, Secrecy
- Records and Accountability Environments
 - Government Accountability
 - International Organizations and Human Rights
 - Corporate Accountability
 - Health Care

Scope of Recordkeeping Requirements

- Creation/Capture
- Content
- Quality
- Structure/Organization
- Retention/Disposition
- Disclosure/Accessibility/Protection

Trust in Electronic Commerce

- Reducing risk
 - Transfer of risk
 - Reduction of liability
- Trustworthy processes
- Traceability
- Intermediaries and Trusted Third Parties
- Endorsements
- Formal Testing and Certification
- Legal Underpinnings and Remedies

Tests for Authenticity

- Forensics
- Diplomatics
- Intellectual Analysis of Consistency and Plausibility
- Evaluation of Truthfulness and Accuracy

Testing for Integrity

- Compare to a known “true” copy
- Check digital signature
- Establish integrity of the digital signature

Trust and Authenticity

- What should technology do?
- What should people do?

Attributes of Trusted Repositories

- Compliance with OAIS Reference Model
- Administrative responsibility
- Organizational viability
- Financial sustainability
- Technological and procedural suitability
- System security
- Procedural accountability

Legal Evidence

(Giordano, 2004)

- Computer Evidence issues
 - Admissibility
 - Authenticity
 - Completeness
 - Reliability
 - Believability

Discovery

- Request by a party to inspect and copy any pertinent records
- E-discovery covers electronic documents and data (email, web pages, word processing files, databases, etc.)
- Preparation
 - Records retention program
 - Employee education (recordness, retention; retrievability after “destruction”; personal emails; spoliation)
 - Format conversion of critical records
 - Catalogs
 - “Persons with knowledge” identified (deposition; interrogatory value)

Sedona Guidelines 1...

- Preserve records in anticipation of litigation
- Proportionality. Balance costs, burden, and need
- Confer early in discovery process
- Discovery requests should be clear and focused
- “Reasonable and good faith effort” does not mean taking “every conceivable step”

Sedona Guidelines 2...

- Responding parties are best able to determine how to comply with requests
- Burden of demonstrating (in)adequacy of production on requesting party
- Access beyond active systems must demonstrate relevancy that “outweigh(s) cost, burden, and disruption”
- Absent demonstrated special need or relevance, respondent not required to “preserve, review or produce deleted, shadowed, fragmented, or residual” ESI
- Respondent to follow “reasonable procedures to protect privileges and objections to production”

Sedona Guidelines 3...

- Electronic tools and processes (sampling, searching, identification criteria) can serve “good faith” obligations
- Production to be in forms/format ordinarily maintained, including metadata to search, retrieve and display
- Review and production costs borne by either requester or respondent depending on “special circumstances”
- Spoliation sanctions mandated only upon finding of “intentional or reckless failure to preserve and produce relevant” information and that such information material to ruling

Federal Rules of Civil Procedure 1...

- Updated and effected December 1, 2006
- Formally align legal process with business reality
- “Electronically Stored Information” (ESI) category. Provides ESI as subject to discovery and production.

Federal Rules of Civil Procedure 2...

- Changes / Issues confronted:
 - Requirement to meet in advance of trial (preserving discoverable information; scheduling discovery)
 - Provide names of holders of relevant information and description of data prior to receipt of discovery request
 - Discovery of information not reasonably accessible (undue burden and cost)
 - Destruction under routine, good faith operations (retention management; safe harbor v. spoliation)
 - Protecting attorney-client / work-product (quick peek; clawback)
 - Subpoenas for ESI

(Spiro; www.axsone.com/pdf/FRCRCP_V8_2007.pdf)

Federal Rules of Civil Procedure 3...

- Implications

- ERM policies and procedures (legal, IT, RM perspectives) essential
- Need to be able to demonstrate suitability and enforcement of policies, procedures, and management of ESI
- IT infrastructure will impact discoverability
- Where and how ESI stored and managed
- Who has ESI and where and how retained
- Abilities to access, search, retrieve ESI in event of litigation

(Spiro; www.axsone.com/pdf/FRCP_V8_2007.pdf)

Standards & Best Practices

- Provide guidance for programs, functions, systems
- Promote interchange, interoperability, longevity
- Provide a basis for monitoring and compliance auditing

SEE:

- ARMA International Standards Development <http://www.arma.org/standards/development/index.cfm>
- ISO TC 46 - Information and Documentation http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=48750

Types of Standards

- Formal vs. De facto
- Open vs. Proprietary
- International, National, Industry, Professional
- Scope: Global process to minute parts
- Abstraction: Model to detailed specification
- Compliance: Mandatory to Voluntary

Electronic Records and Records Management Standards

- System standards
- Software standards
- Metadata Standards
- Process Standards

Some notable (E)RM standards

- OAIS Reference Model
- ISO Records Management Standard
- Various Metadata Standards
- Best (“Good”) Practices

OAIS Reference Model

Type

- Formal
- Open
- International
- Model
- Voluntary

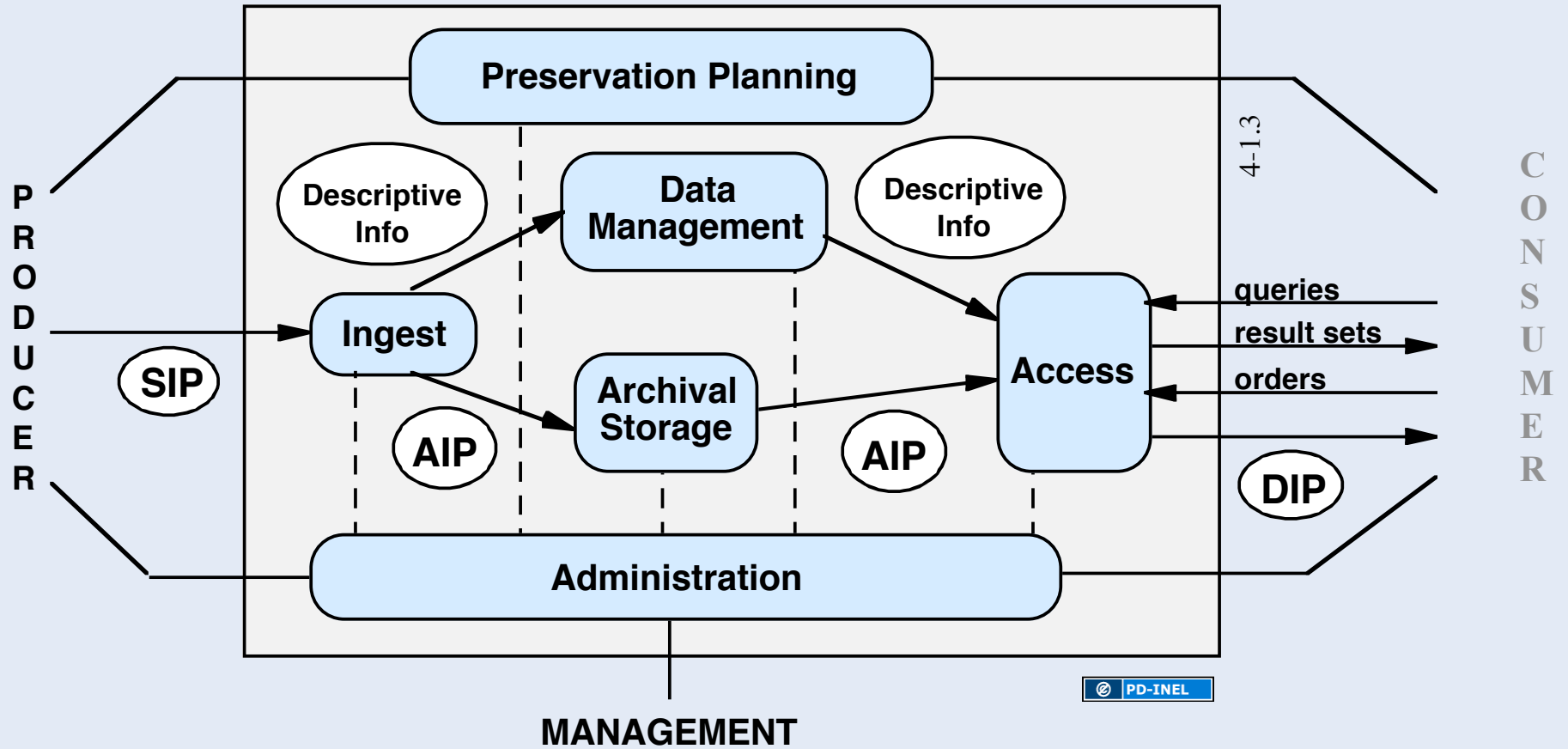
Functions

- Ingest
- Archival Storage
- Data Management
- Administration
- Access
- Preservation Planning

SEE: OCLC Digital Archive

- <http://www.oclc.org/digitalarchive/>

OAIS Functional Entities



SIP = Submission Information Package
AIP = Archival Information Package
DIP = Dissemination Information Package

Records Management Standards

- International Records Management Standard ISO 15489
- Type
 - Formal
 - Open
 - International
 - Program and Processes
 - Voluntary

ISO 15489 Content

- Scope of the Standard
- Benefits of Records Management
- Regulatory Environment (specific to each organization)
- Policies and Procedures (of RM Program)
- Requirements
- Design and Implementation
- Processes & Controls
- Monitoring & Auditing

Requirements

- Determining records needed for each business process
- Formatting and media selection
- Establishing metadata and links
- Managing records retrieval and distribution
- Managing risks (business continuity)
- Managing preservation of records
- Managing security of records
- Managing retention of records

Design and Implementation Methodology

- Preliminary investigation
- Analyze business activity
- Identify recordkeeping requirements
- Assessment of existing systems
- Identify strategies for satisfying records requirements
- Design recordkeeping system
- Implement recordkeeping system
- Post-implementation review

CMS (Content Management Systems)

- E-CMS: Enterprise-wide
- Web Content Management Systems
- Digital Asset Management Systems (DAMS)
- Document Imaging Systems
- Document Management Systems (EDMS)
- Records Management Systems (ERMS/ERKS/RMA)

Records Management Applications

- Separate application that manages paper and electronic records
- Focus on records integrity, retention and disposition
- Records repository (read-only) separate from live applications
- Case Study: Hummingbird in an NGO

DoD: 5015.2-STD RMA DESIGN CRITERIA STANDARD

- requirements based on operational, legislative and legal needs that must be met by records management application (RMA) products
- Compliance testing and evaluation program
- “2. The DoD standard and commercial RMA software packages *are not "out-of-the box" easy or quick solutions* for managing your electronic records. RMA software *only operates in the context of an agency's records management program, policies, and procedures.*”

© FAIR USE

(NARA memo to agencies - www.archives.gov/records-mgmt/memos/nwm03-99.html)

- www.dtic.mil/whs/directives/corres/pdf/501502std.pdf
- Compliance Testing: <http://jitc.fhu.disa.mil/recmgt/>

Sedona Guidelines

- Develop sound and defensible processes to manage ER via law, IT and RM lenses
- Voluntary
- Best Practices
- General
- Scope
 - Creation/Capture
 - Content
 - Quality
 - Structure/Organization
 - Retention/Disposition*
 - Disclosure/Accessibility/Protection*

Risk Assessment & Management

- identifying risks
- assessing magnitude and probability of occurrence
- deciding on an appropriate response (risk avoidance, acceptance, reduction...)

(Gable 2005)

2007: Sea change (2005: The tide is turning)

- **Retention**

- Inadequate programs (consideration; performance; record creating technologies; backups; responsibilities) irregularly followed; ignore ER

- **Litigation/Regulation**

- Increases in hold orders responsiveness but many ignore ER; difficulty complying w/ discovery requests

- **Preservation**

- Inadequate/absent migration plans; IS/IT unaware of eventual migrations

- **Life Cycle Management**

- Inadequate RM responsibility for ER; IS/IT unaware of "lifecycle"; heightened awareness over meeting litigation challenges; heightened belief in accuracy, reliability and trustworthiness over time

(Cohasset/AIIM/ARMA 2007)

Risk Impact Scale

| LABEL | VALUE | DESCRIPTION |
|--------------|-------|-----------------------------------------------------------------------------------------------------------|
| Catastrophic | E | Complete, irreversible loss of data. Data cannot be drawn from other sources—print, artifact, or digital. |
| Very Serious | D | Partial, irreversible loss of data. Data cannot be drawn from other sources. |
| Serious | C | Complete loss of data. Data can be fully reconstructed from other sources. |
| Significant | B | Partial loss of data. Data can be fully reconstructed from other sources. |
| Minor | A | Complete or partial loss of data. Data can be copied from other data files. |

© PD-INEL

Appendix A: *Risk Management of Digital Information* (CLIR, 2000)

Compliance

- Compliance generally consists of three activities:
 - persuasion
 - monitoring
 - enforcement (Archives New Zealand 2001)
- Performance of policies, procedures, RK, technologies, training, audit
- RM outcomes?: more automated record declaration, classification; retention (Gable 2005)

Compliance Tools

- Performance Reporting
- Incident Reports (failures that lead to remedies)
- Self-Assessment
- External Audits
- Inspections

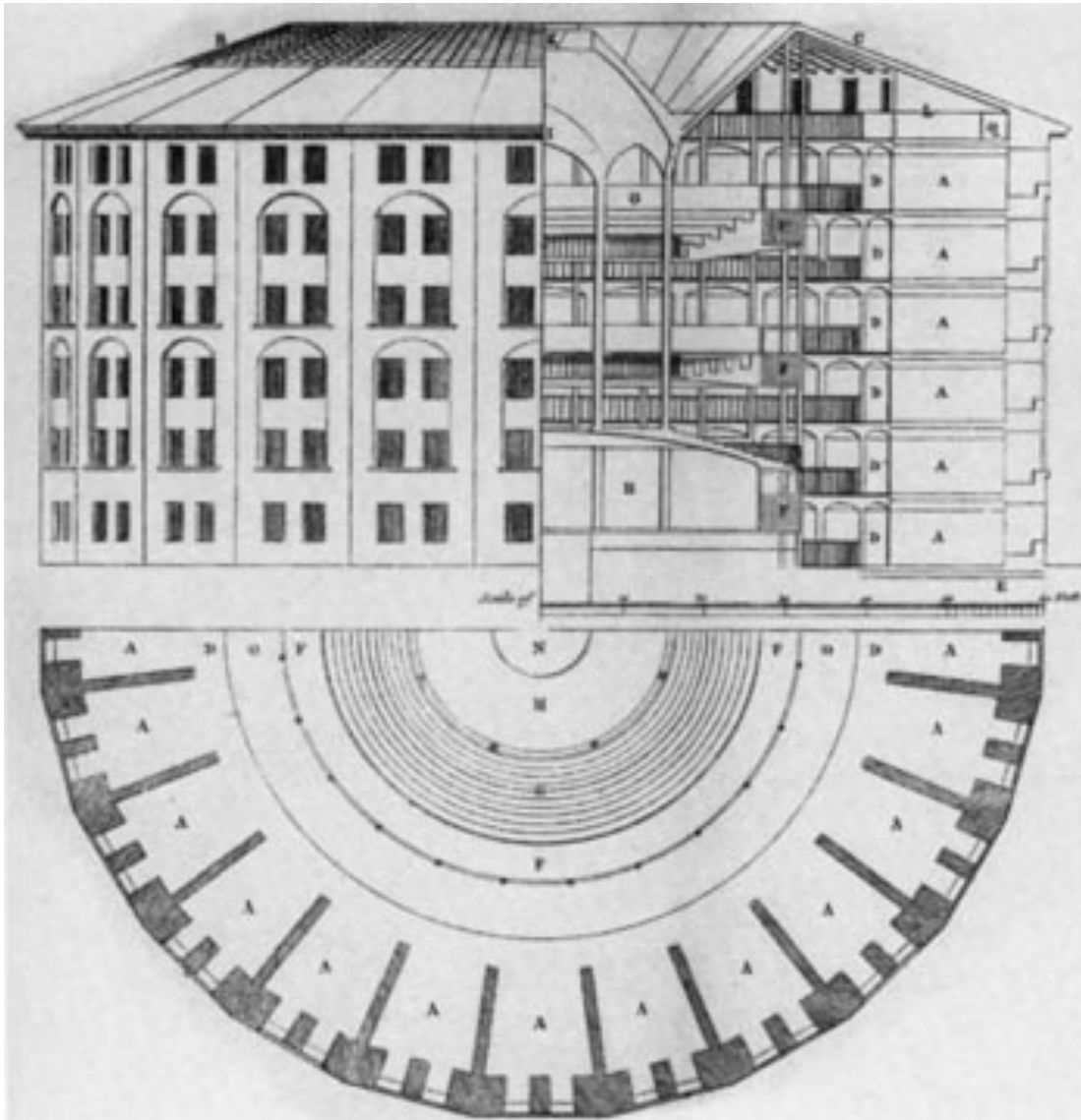
Transparency/Accountability 1...

- Re-establishing legitimacy of institutions following series of scandals and malfeasance
- Globalization and the ineffectiveness of national sovereignty mechanisms
- Pressure from consumers and some investors for socially responsible policies and practices

Transparency/Accountability 2...

- Who is held accountable? For what?
- How do we create/enforce effective mechanisms for accountability?
- What are the limits on transparency?

Panopticon revisited: accountability through transparency? technotyranny?



PD-EXP

Jeremy Bentham ([Wikimedia Commons](#))

<http://www.searchsystems.net/>
<http://www.choicepoint.com/>
<http://www.narus.com/> <http://verint.com/>

Emerging Accountability Mechanisms

- Market-oriented
 - Contract and purchasing requirements
 - Labeling and certification
 - Boycotts
- Regulatory & Legal
 - Standards and Protocols (Koyoto Protocol)
 - Inspections and Treaties (IAEA)
- Voluntary
 - Open reporting movement
 - Self regulation / persuasion
 - Codes of conduct / certification / peer accountability
 - Reputational orientation (brand)

Accountability Enhancers

- Voluntary Reporting
 - Global Reporting Initiative
 - Voluntary Posting of Information
- 3rd Party Reviews (e.g. Consumer Reports)
- Posting or dissemination of information required by law (adverse drug reactions, truth in advertising, “this call may be monitored”)
- Rights and procedures to request access to information (investor profiles, FOIA)
- Technological, organizational, and institutional safeguards (Meijer)

Government Information

- Freedom of Information Act (FOIA)
- Privacy Act
- Federal Register (Administrative Procedures Act)
- Open Meetings Laws (FACA; Sunshine in the Government Act)
- Conflict of Interest Statements
- Financial Disclosures for Political Appointees and some Civil Servants (Ethics in Government Act)
- Whistleblower Protection Act of 2007
- Classification - Declassification
- Patriot Act

Government: sources of requirements

- Specific Requirements: Establish requirements for documentation and recordkeeping around specific programs and functions
- Tens of thousands of laws and regulations that define which records have to be kept and for how long
- Retention and disposition schedules

Accountability and Human Rights

- Dynamic environment
- Absence of jurisdiction
- Language and Semantics
- Priorities / Money
- Enforcement / Compliance

Corporate Accountability: U.S. Legal and Political Context

- Goal: restore faith (trust) in financial markets
- Means: Act of Congress (easy to change / revoke)
- Methods: Record-based compliance
- US Accounting RK issues - SOX
 - Incident reporting; improper destruction; mismanaged retention; falsification...

Healthcare Accountability: Where do recordkeeping and accountability requirements come from?

- HIPAA
- Long standing practice
 - Information need for medical practice
 - Tracking interventions
 - Protocols for best practice
 - Division of labor and hand-offs
 - Research
 - Cumulative record

Special Challenges

- Complexity (language, volume, multiplicity of actors)
- Conflicts of interest
- Mobility of patients
- Privacy
- Integration with practice

Healthcare Accountability: Multiple Uses

- Diagnosis and patient care
- Communication among specializations
- Hand offs
- Eligibility and billing
- Performance monitoring and improvement

Long-term retention of healthcare records

- Medical history
- Prior conditions
- Adverse reactions
- Delayed reactions

Summary

- Accountability
 - Is real and can be measured
 - Is a social “glue” holding society together
 - Is increasing in importance in social, organizational, and governing contexts
 - RK a cornerstone locus of accountability
 - ESI increasingly a locus of accountability
 - ERK/ERM provides tools, methods, processes, standards, best practices for enhancing, enabling, and ensuring accountability

Course Project discussion

- Investigate environment for accountability
 - laws, rules, regulations, and/or policies that were broken or are alleged to have been broken.
- Identify consequences of inadequate rk for
 - Principals directly involved in the case,
 - Victims of the failure of recordkeeping systems
 - Public at large.
- Identify potentiality for rk mitigation via
 - Policies
 - Technologies
 - Tools
 - Best practices