
Wallace, David A.; Hedstrom, Margaret

http://hdl.handle.net/2027.42/78185
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.
Use + Share + 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

- **Public Domain – Ineligible**: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ*
- **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 12 – April 13, 2009

Records and Accountability Environments:
Healthcare Sector
OUTLINE

• Final Session plan
• Overflow from last week...Corporate Sector
• Healthcare Sector
Final Session – Week 13: April 20

- Course summary
- 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
Best Practices Ex.: Computer Forensics

- Critical resource for law enforcement, auditing, Fortune 100 companies
- Uses: assist investigations > computer evidence; discovery; intrusion detection; recovery of temporary and deleted files
- Tool:
  - Enterprise Response, Auditing, and Discovery (ERAD)
    - Noninvasive disk imaging on any disk connected to network
    - Noninvasive KW search and retrieval across network
    - Noninvasive audit and compliance checking re: usage policies via KW search and retrieval (Patzakis)
SOX - Implications for Electronic Records

- Increased awareness of recordkeeping requirements in publicly traded companies
- Increased market for ERM systems
- Jobs for analysts, designers, auditors, and trainers for implementation
- Impact on corporate behavior remains to be seen
Context/Environments

• Context is important
  – Legal/Policy
  – Organizational
  – Functional
  – Technological
Organizational Environment

• Structural
  – Stable hierarchy
  – Laissez-faire
  – Distributed, collaborative, “emergent”

• Cultural
  – Rule-bound / compliant
  – Process / production oriented
  – Innovative, dynamic, re-configurable
Cultural Issues

• Jamaican Bank failures vs. US accounting scandals

• Jamaican Banking RK issues:
  – Missing, incomplete, untrustworthy and inaccurate records
    • damaged operational control (financial management, loan and deposit, risk, fraud)

• US Accounting RK issues
  – Incident reporting; improper destruction; mismanaged retention; falsification...

• Institutional vs. personal motivations
  – Many motivations for alternative / compliant RK reinforces need for control systems
  – Sociotechnical environment: usable..........perfect records
    (Lemieux)
Healthcare
Healthcare
Discussion questions

- What do you know about what can be done with your medical records?
- What control do you have over who uses them?
- What differences might electronic medical records make?
- Are the benefits worth the cost?
- Is medical privacy an illusion?
Healthcare

- Where do recordkeeping and accountability requirements come from?
- How does one locate them?
- What are the specific challenges in the environment?
- How is electronic records management being implemented?
- How are requirements enforced?
Where do recordkeeping and accountability requirements come from?

- 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
Medical Records – Complexity

- Requirements come from many sources
  - Government (federal, state)
  - Private Sector (suppliers, insurance...)
  - Professional standards of practice
Multiple Uses

• Diagnosis and patient care
• Communication among specializations
• Hand offs
• Eligibility and billing
• Performance monitoring and improvement
HIPAA 1...
(PL 104–191, August 21, 1996)

• Privacy provisions
  – Individuals must be able to access their record and request correction of errors
  – Individuals must be informed of how their personal information will be used
  – Individuals “protected health information” (PHI) cannot be used for marketing purposes without the explicit consent of the involved individuals
HIPAA 2...

- Individuals can ask covered entities which maintain PHI about them to take responsible steps to ensure that their communications with the individual are confidential.

- Individuals can file formal privacy-related complaints to the Department of Health and Human Services (HHS) Office of Civil Rights.
HIPAA 3...

- Covered entities must document their privacy procedures, but they have discretion on what to include in their privacy procedure.
- Covered entities must designate a privacy officer and train their employees.
- Covered entities may use an individual’s information without the individual’s consent for the purposes of providing treatment, obtaining payment for services and performing the non-treatment operational tasks of the provider’s business.
HIPAA 4...

- Electronic Data Exchange Standards
  - Security provisions
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards

See also:

http://www.hhs.gov/ocr/privacy/index.html
http://www.hipaa.org/
http://www.cms.hhs.gov/hipaaGenInfo/
Long-term retention of healthcare records

• Medical history
• Prior conditions
• Adverse reactions
• Delayed reactions