Health Information Exchange Organizations (HIEs / HIOs)

6th Annual Conference Hosted by OCR & NIST
Safeguarding Health Information:
Building Assurance through HIPAA Security
May 22, 2013

Ruth Anne Carr, J.D., LL.M.

HIEs / HIOs under HITECH

- HITECH Act of 2009 defined Business Associates (BAs) to include "Health Information Exchange Organizations" that provide data transmission of PHI to a covered entity or BA and that require routine access to PHI.
- HIEs / HIOs that are Business Associates must comply with the HIPAA Security Rule and are subject to the Enforcement Rule.

Historical Models for HIEs

- **“Elevator,” “Capacity Builder,” “Orchestrator,” “Public Utility”**
  - Early models varied from a mere Conduit (with no transmission or routine access) to a statewide exchange with data storage, record locators, master patient index, provider directories, etc.
- Models called “**Centralized**,” “**Federated**,”etc.
- NIST HIE Contexts “**Ad Hoc**,” “**Regional**,” “**Multi-Regional**,” “**Nationwide**”

Security Rule: Special Issues for HIEs/HIOs

- Is the HIE / HIO a Business Associate
  - Transmit e-PHI?
  - Require routine access to e-PHI?
  - Have routine access to e-PHI?
- Continuous monitoring and adaptation to changes
  - Dynamic, evolving environment
  - Business models and services change
  - Priorities and operations change
  - Innovations in technology

Special Issues – cont'd

- Changes in Business - More services, more entities
  - Expansion of Shared Services, Value Added
    - Cloud hosting
    - Clinical utilization review, quality improvement
    - Patient safety activities, Personal Health Record
  - Addition of participants / stakeholders
    - Hospitals
    - Physicians
    - Labs
    - Health plans
    - Patients and Families

Special Issues – cont'd

- Administrative Safeguards: Document
  - Access Management: multiple locations, entities, users
  - Security Awareness & Training: continuous
  - Security Incident Procedures: reporting, response
- Physical Safeguards: Implement
  - Facility access controls; workstations may be mobile
  - Device and media controls, BYOD practices
- Technical Safeguards: Monitor
  - Technology and policies & procedures
  - ENCRYPTION: See NIST and HHS Guidance

Challenges

- Lack of agreement on security policies and operating policies
- Lack of agreement on exchange mechanisms
- Concerns about legal liabilities
- Needs:
  - Common set of business practices: organizational, trust, operations, technical = Governance Framework
  - BA Agreements to define access and use
  - More than ever, Collaboration

Resources

- OCR: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
  Risk Analysis Guidance:
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

- NIST: HIPAA Security Rule Toolkit http://scap.nist.gov/hipaa
  NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html

- OCR and NIST Security Rule Guidance:
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

- ONC: State HIE Program http://statehieresources.org
  HIE Governance: http://www.healthit.gov/HIEgovernance