HIPAA Implications: Implementation in a Health System

Clay J. Countryman, Esq.
Roedel, Parsons, Koch, Frost, Balhoff & McCollister, A L.C.
Heather C. Jahnke, Ph.D.
HIPAA Project Manager, General Health System
Presentation Overview

• Legal and regulatory requirements peculiar to a Health Care System

• Organization and HIPAA implementation strategies for a Health Care System
Health Care System

- Single Entity Health Care Delivery System that includes:
  - Acute Care Hospital(s)
  - Physician Component
  - HMO/Insurance Entity
  - Nursing Home(s), Physical Therapy, etc…

- Single Entity that Includes a Health Care Component
Presentation Background: Regulatory and Operational Requirements

- Working relationship of legal counsel and Health Care System Employees
- Distinct Roles
  - Educational Awareness
  - Assessment Tool
  - Drafting and/or Reviewing Policies and Procedures
  - Assistance in Training
  - Working Through Scenarios
Legal Counsel and Implementation Issues

- Identify applicable state laws and regulations
- Legal analysis of application of HIPAA regulations
- Participate on HIPAA oversight committee meetings
- State law preemption identification and analysis
Legal Counsel and Implementation Issues cont’d

• Business Associates (Identify Business Associates, draft contract language, negotiate/amend existing contracts)

• Drafting/Reviewing policies, authorizations, consents, etc…
Requirements That Affect Health Care Systems in the Final Privacy Standard

- § 164.504 (a)- (c) Health Care Component
- § 164.504 (d) Affiliated Entities
- § 164.504 (e) Business Associates
- § 164.504 (f) Group Health Plans
- § 164.504 (g) Multiple Covered Function Entities
Privacy Rules for Health Care Component

• Applies to “Hybrid Entities” who are a Covered Entity, but whose covered functions under the Privacy Standards are not the entity’s primary functions (e.g. school with an on-site health clinic and an employer that self-administers a sponsored health plan)
Privacy Rules for Health Care Component cont’d.

• Health care component requirements apply only to the health care components of the Hybrid Entity
• Safeguard requirements (ensure compliance with privacy standards within Hybrid Entity, oversee non-health care component Business Associate functions, and shared workers within the Hybrid Entity)
Privacy Rules for
Health Care Component cont’d.

- Covered Entity responsibilities (ensure compliance with privacy standards, develop privacy policies and procedures, designate health care components)
Affiliated Covered Entities § 164.504(d)(1)

• Legally separate covered entities that are affiliated may designate themselves as a single Covered Entity.

• Criteria for designation:
  – Must be under common ownership or control
  – Designation must be documented (§ 164.530j)
Affiliated Covered Entities cont’d

• Safeguard requirements for an Affiliated Covered Entity (compliance with Privacy Standards, compliance with § 164.504(g) for Multiple Covered Function Entities)

• May adopt a single shared notice of information practices and a consent form
Affiliated Covered Entities cont’d

• Requirements of a Covered Entity also apply to an Affiliated Covered Entity

• Each Covered Entity of an Affiliated Covered Entity is separately subject to liability under the Privacy Standards
Multiple Covered Function Entities § 164.504(g)

- Applies to single legal entities that have any combination of the functions of a health care provider, health plan, or health care clearinghouse
Multiple Covered Function Entities cont’d.

- Must comply with the Privacy Standards that apply to that particular type of Covered Entity when it functions as that entity (e.g. when a health care component functions as a health care provider it must meet the Privacy requirements for a health care provider)
Multiple Covered Function Entities cont’d.

- May not use or disclose the PHI of an individual that is not involved in a particular Covered Entity function, and must segregate PHI from any joint information systems (e.g. Health Care System cannot share information about a patient in its hospital who is not a member of its health plan)
HIPAA Project Organization

Oversight Committee

HIPAA Project Manager

Hospital Ops  Health Plan Ops  Non-Acute Ops  Corporate Ops
Oversight Committee Membership

- President / CEO System
- Sr. VP Non-Acute
- CEO – Health Plan
- VP – Behavioral Health Managed Care
- Director, Practice Management
- VP Risk Management
- VP - Marketing
- Corporate Compliance Officer
- VP Finance - Hospital
- VP Finance - Corporate
- HIPAA Project Manager
- Information Services
Oversight Committee Responsibilities

- Ensure compliance with regulations is met by required dates.
- Provide a decision making and approval forum on recommended changes and implementation strategies.
- Break down barriers and identify / provide resources to operational teams.
Hospital Ops Team Membership

- Manager, Health Information Mgmt
- Director, Admissions / Scheduling
- Manager, Patient Care: Behavioral
- VP, Patient Care: Med/Surgical
- JCAHO Coordinator
- Administrator, Residency Program & Clinic
- Manager, Business Office
- Information Services
- HIPAA Project Manager
Health Plan Ops Team Membership

- Director, B.H. Managed Care
- Manager, Provider Relations
- Supervisor, Case Management
- Director, Benefit Services / Claims
- Director, Govt. Affairs & Compliance

- Director, Quality Management
- Director, Customer Service
- Manager, Contract Management
- Director, Care Management
- Manager, Provider Relations
- Information Services
- HIPAA Project Manager
Non-Acute Ops Team Membership

- Director, Nursing Homes
- Director, Behavioral Health Services
- Director, DME / Pharmacy
- Manager, Physician Clinic
- Administrator, Home Health
- Manager, Business Office
- Information Services
- HIPAA Project Manager
Corporate Ops Team Membership

- Corporate Compliance Officer
- Director, Managed Care Contracting
- VP, Vendor Contracting
- Director, Professional Services Contracting
- Director, Internal Audit
- Director, Decision Support
- Administrator, Human Resources
- Manager, Accounting Services
- Information Services
- HIPAA Project Manager
Ops Teams Responsibilities

- Assess current state of compliance
- Identify opportunities for improvement and changes needed
- Develop recommendations for new processes and policies
- Report activities to Oversight Committee
- Implement approved changes
Action Plan

- Raise awareness
- Educate on standards
- Assess risk / opportunities
- Develop action plan
- Implement & test
- Ongoing monitoring
Assessment

Transaction Standards:

- Identified applicable ones
- Identified systems
- Vendor contact & monitoring
Assessment

Privacy:
• Developed tool
• Educated along the way
• Ops Teams identified applicability and sources
• Prioritize results
• Develop action plan to address gaps
Assessment

Security:

- Subgroup w/Information Services
- Identified Operations, Technical, or Both
- Developed tool
- Educated along the way
Top Five Tips

• Executive Buy-In
• Awareness & Education
• Know your Resources & Use Them
• Know your Organizational Culture & Use It
• Know your Potential Pitfalls