HIPAA Implementation Case Studies: Hospitals and Health Systems

Rita Aikins

Information Security/Privacy Officer

Providence Health System, Oregon Region

Providence | Health System

A caring difference you can feel

Organizational Strategy Questions

- What makes sense for your organization
- Complexity of your environment
- What worked and what didn't work with Y2K
- Improving organizational performance

Providence | Health System

A caring difference you can feel

Executive Sponsor

- Executive Management Approval and Appointment of Sponsor
  - CIO, CEO, CFO
- Executive Sponsor duties include:
  - Liaison to top executives and the Board
  - Review and approve overall HIPAA compliance strategy
  - Political issue resolution
  - Continuous support for operational business process changes
  - Budget

Providence | Health System

A caring difference you can feel

HIPAA Project Manager/Coordinator

- Overall HIPAA project responsibility
- Awareness/education training
- Strategies
  - Compliance
  - Communication
  - Vendor/Business Partner
- Compliance monitoring

Providence | Health System

A caring difference you can feel

HIPAA Standard Project Managers

- Operational impact
  - People
  - Systems
  - Processes
- Compliance strategy
- Implementation strategy
- Validation/Testing
- Compliance Sign-off

Providence | Health System

A caring difference you can feel

Operational Project Team

- Ancillary
- Audit
- Bio-Medical
- Business Office
- Clinics
- Finance
- Health Plan
- Home Health
- Human Resources
- Information Services
- Legal
- Long Term Care
- Medical Records
- Nursing
- Physicians
- Quality Management
- Research
- Security – Physical

Providence | Health System

A caring difference you can feel

Oversight/Steering Committee

- Strategic oversight
- General guidance
- Resolve political challenges

Providence | Health System

A caring difference you can feel

HIPAA
EDI & Code Sets

Providence | Health System

A caring difference you can feel

EDI/Code Set Timeline

- Final rule passed on 8/17/2001
  - Compliance date 10/16/2002
  - Small health plans have until 10/2003 for compliance

Providence | Health System

A caring difference you can feel

EDI Standards

- Industry (not government) based standards
- ASC X12N is the standard protocol adopted for most EDI transactions

Providence | Health System

A caring difference you can feel

EDI Must Use Provision

- Health plans must use the standards when transmitting the standards
- Health plans may no longer require providers to support proprietary formats or plan specific implementation
- Health plans are required to accept and process without delay all transactions that are presented in a standard format

Providence | Health System

A caring difference you can feel

EDI

- Identification of systems impacted
- 837 – X12 data mapping
  - 72 data elements to review
  - Crosswalk between UB and 1500
- Process changes to collect new data
- Vendor compliance

Providence | Health System

A caring difference you can feel

Code Sets

- Identification of systems impacted
- Local codes go away
- HCPCS J codes replaced by NDC codes
- HCPVS D codes replaced by CDT-2
- Vendor compliance

Providence | Health System

A caring difference you can feel

HIPAA
Security Standard

Providence | Health System

A caring difference you can feel

Security Standard

- Scalable
- Technology neutral
- Does not speak to the intent that one must implement requirements
- Guideline to set a minimum baseline for compliance
- Organizations must assess information security risks and implement appropriate mitigation

Providence | Health System

A caring difference you can feel

IT Asset Inventory

- HIPAA requirement
- Y2K inventory as a foundation
- Asset Inventory:
  - Catalog of applications, operating systems, interfaces, databases, hardware, biomedical equipment
  - IT supported and not supported
- Process to maintain the inventory

Access to Healthcare Information

- Building/maintenance/tracking of access
- Role based
- Need to know
- Confidentiality/Non-Disclosure agreement signed
- Process for non-employees
- Physicians and office staff

Providence | Health System

A caring difference you can feel

Policy/Procedure Development

- Major requirement of HIPAA security standard compliance effort
- Foundation for best practices of information security
- Opportunity to bring policies current with organizational business practices
- Opportunity to eliminate redundancy in policies
- Consistency in message policy is sending

Providence | Health System

A caring difference you can feel

Data Hunting

- Data flow outside and inside
  - Validation
    - Of need to know
    - Minimum information necessary
  - Chain of Trust Agreements
  - Business Associate Agreements

Contract Management

- Inventory of contracts
  - Verbal and written
- Identify contracts needing review for HIPAA/Privacy verbiage
- Legal review

Providence | Health System

A caring difference you can feel

Vendor/Business Partner Agreement

- Information gathering mailing
  - Registered
  - Logged
  - Tracked
  - Readiness status

Providence | Health System

A caring difference you can feel

Risk Management Methodology

- Organizational Assessment
- Departmental Assessment
- Threat Assessment
- Mitigation
- Final Report
- Mitigation Follow-up

Providence | Health System

A caring difference you can feel

HIPAA
Privacy Rule

Privacy Timeline

- Final rule passed on 4/14/2001
  - Compliance date 4/14/2003

Providence | Health System

A caring difference you can feel

Privacy Rule

- State law preemption
- Privacy notice
- Consent and authorization
  - Ability for patient to revoke
  - Ability to track

Providence | Health System

A caring difference you can feel

Privacy Rule

- Marketing and fundraising
  - Ability for patient to opt out
  - Ability to track
- Business Associates
- Minimum necessary
- Policies and procedures

Providence | Health System

A caring difference you can feel

Common Questions

- How much will it cost to implement HIPPA?
- Who should do the work?
  - Do it yourself
  - Consultants
- Do I need an Information Security Officer and a Privacy Officer?

Providence | Health System

A caring difference you can feel

Sustaining Compliance

- Integration of compliance into business strategy?
- Integration of HIPAA with new initiatives
- Evaluation of compliance
- Maintaining compliance
- Where does responsibility fall?
- Who is responsible?

Providence | Health System

A caring difference you can feel