The Seventh National *HIPAA Summit*

~ Case Study ~

Health System HIPAA Compliance: TCS, Security and Privacy Clean-Up

(or How to HIPAA-TIZE an entire health system)

Jim DiDonato
HIPAA Project Manager &
Information Security Officer
Baystate Health System
Springfield, Ma.

Session # 1.07
September 15, 2003

Meeting Objectives

By the end of this meeting, you will be able to answer the following questions:

- What is the effect of today's meeting/presentation?
  HIPAAnosis
- What will you most likely say after this meeting?
  HIP- HIPAA-Ray
- What is the disease you get from too much HIPAA?
  HIPAA-titis
- What not to say after April 14th?
  I'm in a HIPAA-trouble
- What do you call a boring person who talks in circles about HIPAA? **HIPAA-Drone**

Case Study ~ Baystate Health System

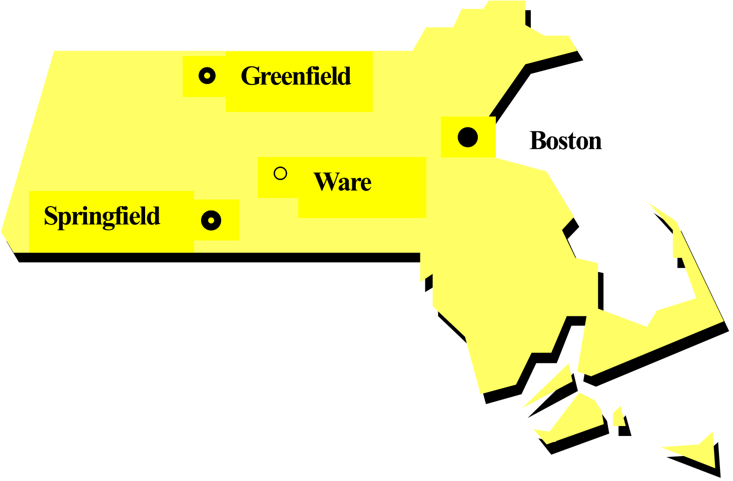
- Baystate ~ Who we are
- HIPAA Project Scope
- Project Organization
- Plan for Compliance
- Initial Assessment Outcome & Project Budget
- Workplans
- Project Updates
  - TCS
  - Privacy
  - Security
- Next Actions
- Conclusion

Baystate Health System ~ Who we are

- **Not-for-profit, hospital-based integrated delivery system (IDS) serving western New England.**
- **Named one of the nation’s leading 100 integrated healthcare networks.**
- **Based in Springfield, Massachusetts.**
- **We include:**
  - **an academic medical center and two community hospitals,**
  - **numerous outpatient facilities and programs,**
  - **an ambulance company,**
  - **home care and hospice services,**
  - **employed primary care provider group with multiple sites and**
  - **other support services.**
- **Majority interest in for-profit HMO with 100,000 lives.**

Baystate Health System ~ Who we are

- **699 – beds**
  - **572 beds @ Baystate Medical Center, Springfield, Ma**
  - **96 beds @ Franklin Medical Center, Greenfield, Ma.**
  - **31 beds @ Mary Lane Hospital, Ware, Ma.**
- **39,885 combined admissions**
- **605,038 outpatient service volume**
- **8,261 employees in Mass, Ct, Vt & NH**
- **$1.4 billion gross revenue**



Baystate's HIPAA Project Organizational Scope

- **In Scope:**
  - Medical practices & ambulatory care services,
  - Administrative support (Marketing, HR, Info Sys, strategic planning and financial services),
  - Ambulance company in two cities,
  - 3 hospitals,
  - Visiting Nurse Association & Hospice,
  - Infusion & Respiratory Services and
  - Employee Health Plan

- **Out of Scope:**
  - HMO (collaboration only)
  - Other Affiliated Organizations (Joint Ventures)

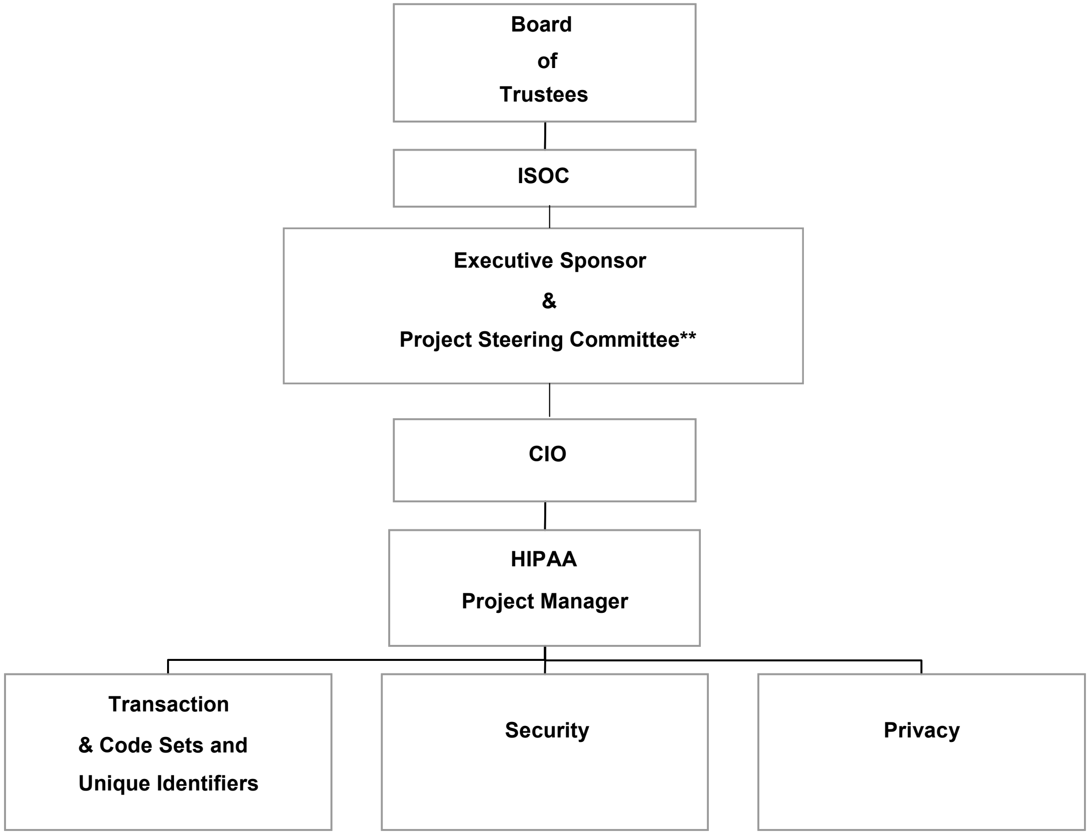
Baystate's Plan for HIPAA Compliance

- Awareness (Communication Plan)
  - Presentations & electronic and printed newsletters
  - Internal & external audiences
- We established:
  - Executive Sponsor (Chair of Psychiatry Dept)
  - Steering Committee (21 VPs and Directors)
  - Project Teams
    - Privacy (20+ people)
    - Security (20+ people)
    - Transactions (20+ people)
- We performed an assessment comparing HIPAA regulations to our current state (gap analysis).
- We agreed on a strategy that examines our compliance options considering <u>costs</u>, <u>risks</u> & <u>resource needs</u>.
- We developed & implemented workplans to obtain compliance by the various dates.
- We are establishing accountabilities and processes to ensure ongoing compliance.

BHS HIPAA Project Organization

Project Steering Committee **

Director (Risk mgmt/Corp Compliance)
Privacy Officer
VP (Finance) (2)
Director (Nursing)
Director (Mary Lane Hosp)
VP (HR)
Mgr (Marketing & Communications)
MD (Pediatrician)
VP/CIO (HMO)
MD (Psychiatry)(Exec. Sponsor)
Director (Facility Security)
VP (Visiting Nurse Assoc)
Director (Patient Acctg)
Director (Physician Billing)
Director (Cancer Services)
VP/CIO
Director (Info Sys)
Asst. Director (Info Sys)
HIPAA Project Manager & Info Security Officer (Info Sys)
VP (Ambulatory Care)
Director (Franklin Med Ctr)


Board of Trustees
ISOC
Executive Sponsor & Project Steering Committee**
CIO
HIPAA Project Manager
Transaction & Code Sets and Unique Identifiers
Security
Privacy

Assessment Outcome

- **Privacy:**
  - Contracts not compliant.
  - Patient consents and authorization not compliant.
  - Patient information found in the trash.
  - Patient charts exposed on hospital hallway walls & counters.
- **Security:**
  - FAX machines & printers left unattended.
  - Computer terminals pointing toward public.
  - Need to conduct Security certification (Evaluation).
- **Transaction & Code Sets:**
  - Claims/Remittances
    - Upgrades or replacement of systems are vendor options.
    - Cost will be dependent on vendor strategy.
      - Part of routine application maintenance (no additional cost)
      - Capital purchase
    - New data gathering requirements.

Project - Budget

Regulation	Impact of New Requirements	Estimated Capital Costs	Estimated Operating Costs
Transaction & Code Sets	Modify billing software & processes	$690,000 (FY 02)	$69,000 (FY 02)
Privacy	Develop new consents & authorizations, contracts, notice of privacy practices, etc.	0	$335,000 (FY 02/ $199,500 FY 03/ $135,500)
Security	Update & enhance contingency plans, audit trails, policies and workforce training, etc.	$120,000 (FY 02)	$450,000 (FY 02/ $67,500 FY 03/ $382,500)
Total		$810,000	$854,000

Project Workplans

- **Transaction & Code Sets:**
  - Consultant support.
- **Privacy:**
  - In-house developed workplan using MS Project
- **Security:**
  - In-house developed workplan using MS Project

Security Workplan

- Much of the workplan comes directly out of the regulation:
  - PHYSICIAL SAFEGUARDS
  - Facility Access Controls
    - Contingency Operations
    - Facility Security Plan
    - Access Control and Validation Procedures
    - Maintenance Records
  - Workstation Use
  - Workstation Security
  - Device and Media Controls
    - Disposal
    - Media Re-use
    - Accountability
    - Data Backup and Storage
- But the workplan needs additional steps such as:
  - Compare HIPAA to JCAHO for consistency & coverage.
  - Results of Risk Assessment.

Security Workplan – Task Detail (life-cycle of a task)

1. Task Analysis & Planning (task definition, scope, objectives)
2. Team Staffing
3. Identify Executive Sponsor for Team
4. Develop team training and orientation
5. Task Assignment (conduct team orientation & training)
6. Evaluate addressable specifications
7. Task Effort:
    1. Acquire & Implement Technology
        - Define Required Technology
        - Assess Alternative Solutions
        - Select Preferred Solution
        - Acquire Preferred Solution
        - Install and Test Solution
        - Place Solution into Production
    2. Develop and Implement Draft Policy and/or Procedures
        - Draft Policy and/or Procedures
        - Identify Key Stakeholders
        - Route Draft Policy and/or Procedures to Key Stakeholders
        - Finalize Draft Policy and Review with Project Leadership for Input/approval
        - Present Draft Policy to Designated Approval Committee (ISOC, BAS Exec)
8. Training:
    - Design Training Plan
    - Develop Training Program and Material
    - Implement BHS-wide Training
    - Training Completed
9. Task Complete

Security Workplan – For each Addressable Specification:

- Is the addressable implementation specification reasonable and/or appropriate for Baystate? If yes, then implement the implementation specification.

- If the implementation specification is inappropriate for Baystate, and/or is unreasonable, implement an alternate measure that accomplishes the same end as the addressable implementation specification. In cases where we meet the standard through an alternate measure, document:
  - the decision not to implement the addressable implementation specification,
  - the rationale behind that decision and
  - the alternative safeguard implemented to meet the standard.

Project Update - Transactions & Code Set (TCS)

- In production with some payers for:
  - Pharmacy
  - Practices
  - Ambulance company

- Internal testing underway for all others:
  - Low risk for hospital (except Medicaid – 9% of volume).
  - Low risk for practices with Blue Cross remittances.

Project Update - Privacy

Training continues:

- Leadership Presentations (Heads-up…HIPAA is coming)
- Leadership Train-the-Trainer sessions
  - ‘Phase 1 – HIPAA-Lite’ (20 management teams – 500 managers?)
    - Manager’s Guide (in-house)
    - Handbook for employees (purchased)
    - Quiz (in-house)
    - Video Tape (purchased)
  - ‘Phase 2 –HIPAA Privacy Policies’ (with role-playing)
    - Manager’s Guide (in-house)
    - Handbook for employees (in-house)
    - Intranet
      - Policies & forms
      - Other resources
    - HIPAA Help Line – 4-4722 (H-IPAA)
    - Video Tape (in-house)

Project Update - Privacy (Continued)

- What did we miss?
  - Subpoenas – Ma. state pre-emption
  - Training
- What procedures need additional work?
  - Law Enforcement & the ED
  - Inmates, Disaster relief, Research
  - Information Systems (requests for ad hoc listings of patients)
  - Interface of NPP information to eliminate duplication & costs
  - Automation of Accounting for Disclosures to improve efficiency and effectiveness.
  - Authorizations:
    - Old forms destruction incomplete
    - Too many new forms – need to consolidate
- Gap Analysis - Summer 2003 Follow-up
  - Compliance reviews by 20+ members of Privacy Team & Corporate Compliance.
- Appreciation Celebrations Held

Project Update - Security

- Work began in December 2001 (based upon the proposed Regulation):
  - Various stages of completion – continued to achieve privacy safeguards:
    - Workstation Security
    - Access Control
    - Contingency Planning
    - Business Impact Analysis
    - Disaster Recovery
    - Emergency Mode Operations
    - Passwords
    - Audit
    - Fax
    - Shredding/disposal

Next Actions – TCS

- Complete internal testing of upgraded systems.
- Complete external testing with payers.
- Ensure training of staff and new data gathering as required.
- Finalize contingency plans:
  - Clients order billing forms/supplies and prepare staff
  - Treasury Services plans for bump in cash flow
- Trading Partner Agreements determined to not be necessary.
- Continue documenting good-faith efforts to comply.

Next Actions – Privacy & Security

- **Privacy:**
  - Automation
    - Accounting for Disclosures
    - NPP
  - Gap Analysis
  - TTWP (Tweak, Train and Write Policies)
  - Much of the responsibility to educate patients falls to us.
- **Security:**
  - Teams
  - Scope
  - Timelines