The Sixth National *HIPAA Summit*

~ Case Study ~

Building a Health System HIPAA Compliance Program from the Bottom Up

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

Session # 6.04
March 28, 2003

Case Study ~ Baystate Health System

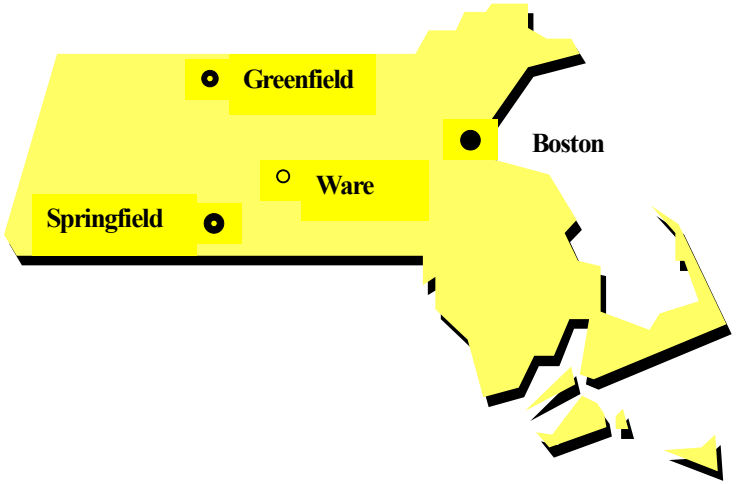
- Baystate ~ Who we are
- HIPAA Project Scope
- Plan for Compliance
- Awareness Efforts
- Project Organization
- Assessment (Gap Analysis) Strategy & Outcome
- Workplans
- Privacy Update
- Next Actions
- Conclusion

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 and include an academic medical center and two community hospitals, numerous outpatient facilities and programs, an ambulance company, home care and hospice services, an 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 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)**
- **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 costs, risks & resource needs.**
- **We developed & implemented workplans to obtain compliance by the various dates.**
- **We are establishing accountabilities and processes to ensure ongoing compliance.**

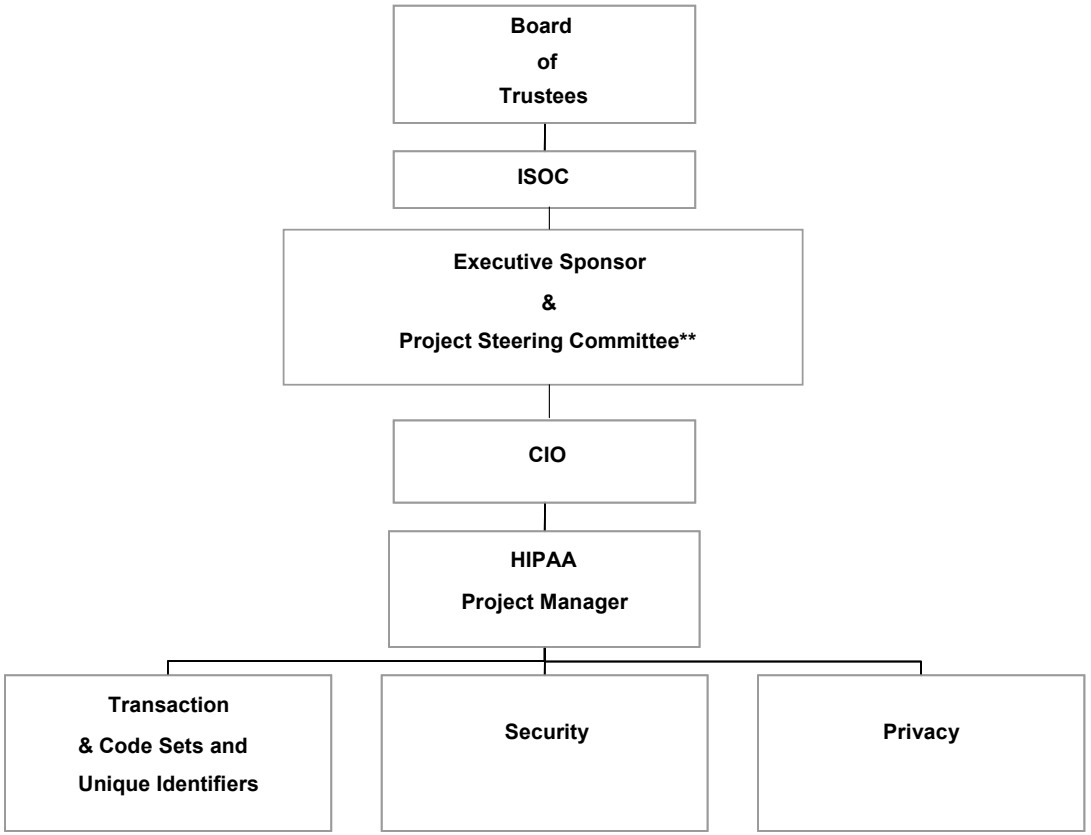
Awareness Efforts

- We describe that the purposes of Administrative Simplification are to:
  - improve the efficiency and effectiveness of the health care system by standardizing electronic data interchange for administrative & financial transactions.
  - enhance the security and privacy protections over patient information.
- We also describe our project organization & schedule.
- Audiences include:
  - Boards of Trustees and the Board Compliance Committee
  - Senior Executives
  - VNAH management team
  - Behavioral Health management team
  - Revenue Management Team
  - Community Hospital Medical Staff
  - Teaching Hospital Surgeons & Residents
  - Community practice managers
  - Others

BHS HIPAA Project Organization

Project Steering Committee **

Director (Risk mgmt/Corp Compliance)
VP (Finance) (2)
Director (Nursing)
Director (Mary Lane Hosp)
VP (HR)
Staff (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 Sys)
VP (Ambulatory Care)
Director (Franklin Med Ctr)



Assessment Strategy

- **Hired consultants for full HIPAA regulation Assessment, but partial Organizational Scope, a train-the-trainer approach that would be a lower cost alternative.**
  - **Consultant would assign 3.5 individuals part-time, including executive leadership.**
  - **BHS Staffing:**
    - **Security & Privacy (6 manager-level individuals – 70 FTE days).**
    - **Transactions (6 manager-level individuals – 35 FTE days)**
  - **All work results would be integrated into a single, cohesive set of assessment deliverables.**

Assessment Outcome – Security and Privacy

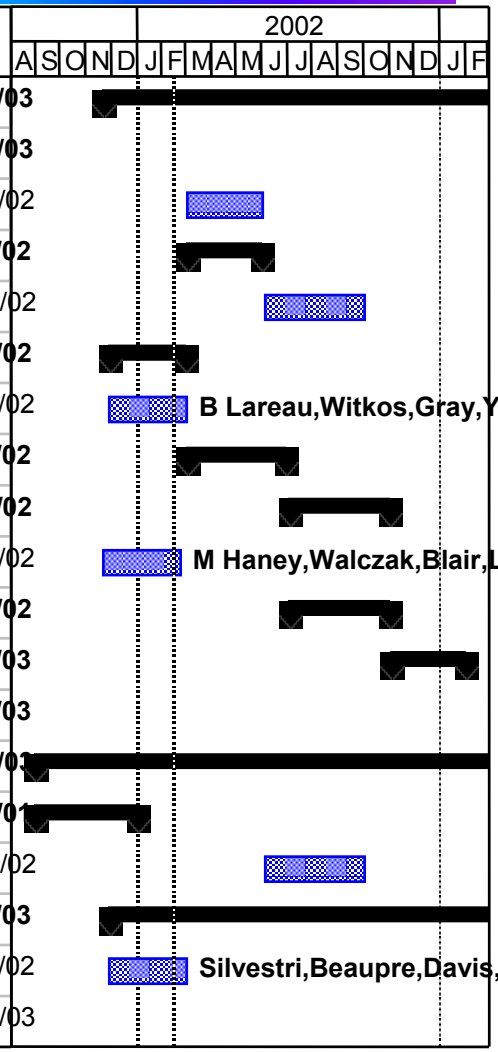
- Contracts not compliant.
- Patient consents and authorization not compliant.
- Patient information found in the trash.
- Patient charts exposed on hospital hallway walls & counters.
- FAX machines & printers left unattended.
- Medical records not adequately secured.
- Computer terminals pointing toward public.
- Employees and physicians not aware of existing policies.
- Need to designate the Security Officer & Privacy Officer.
- Need to conduct Security certification.
- Doors unlocked (medical practices, hospital stairwells, and other ‘secure’ areas).
- Need for new policies (Passwords, Workstation use, etc.)

Assessment Outcome - 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

Security Workplan

ID	Task Name	Duration	Start	Finish
10	**ADMINISTRATIVE PROCEDURES**	**553 days**	**Mon 11/19/01**	**Wed 12/31/03**
11	**Develop P&P and Implement a Security Certification Proc**	**87 days**	**Tue 09/02/03**	**Wed 12/31/03**
14	Develop & Implement Chain of Trust Agreements	65 days	Fri 03/01/02	Thu 05/30/02
15	**Formal, Documented Contingency Plans**	**66 days**	**Fri 03/01/02**	**Fri 05/31/02**
21	Develop P&P for Processing Records	86 days	Mon 06/03/02	Mon 09/30/02
22	**Develop P&P Information Access Control**	**69 days**	**Mon 11/26/01**	**Thu 02/28/02**
26	Develop Procedures for Internal Auditing of System Activity	69 days	Mon 11/26/01	Thu 02/28/02
27	**Develop Personnel Security Procedures**	**86 days**	**Fri 03/01/02**	**Fri 06/28/02**
34	**Develop, Doc. & Implement a Sec. Config. Mgmt. Program**	**89 days**	**Mon 07/01/02**	**Thu 10/31/02**
40	Develop Security Incident Procedures for Responding & Reporting	69 days	Mon 11/19/01	Thu 02/21/02
41	**Develop a Security Management Process**	**89 days**	**Mon 07/01/02**	**Thu 10/31/02**
46	**Review/Revise Term. Proced. (Employment & User Access)**	**66 days**	**Fri 11/01/02**	**Fri 01/31/03**
51	**Develop & Implement Security Training P&P**	**87 days**	**Thu 05/01/03**	**Fri 08/29/03**
57	**PHYSICAL SAFEGUARDS**	**610 days**	**Thu 08/30/01**	**Wed 12/31/03**
58	**Develop Security Officer Roles and Responsbilities**	**88 days**	**Thu 08/30/01**	**Mon 12/31/01**
60	Develop P&P for Media Controls	86 days	Mon 06/03/02	Mon 09/30/02
61	**Develop Physical Access Control P&P**	**460 days**	**Mon 11/26/01**	**Fri 08/29/03**
71	Develop P&P on Workstation Use and Location	69 days	Mon 11/26/01	Thu 02/28/02
72	Security Awareness Training	87 days	Tue 09/02/03	Wed 12/31/03



Security Workplan

ADMINISTRATIVE PROCEDURES

- Develop Policies & Procedures and Implement a Security Certification Process
- Develop & Implement Chain of Trust Agreements
- Formal, Documented Contingency Plans
- Develop P&P for Processing Records
- Develop P&P Information Access Control
- Develop Procedures for Internal Auditing of System Activity
- Develop Personnel Security Procedures
- Develop, Document & Implement a Security Configuration Management Program
- Develop Security Incident Procedures for Responding & Reporting
- Develop a Security Management Process
- Review/Revise Termination Procedures (Employment & User Access)
- Develop & Implement Security Training P&P

PHYSICAL SAFEGUARDS

- Develop Security Officer Roles and Responsibilities
- Develop P&P for Media Controls
- Develop Physical Access Control P&P
- Develop P&P on Workstation Use and Location
- Security Awareness Training

Privacy Workplan

- Define Designated Record Set Policy
- Develop Minimum Necessary policy and procedures
  - Develop High-level Policy
  - Develop Department-head level Procedures
  - Develop Matrix tool for Department-head Decision-making
  - Develop Policy for use of PHI for Transcription
  - Coordinate with HIPAA Security Project Team/System Administrators
- Review/revise Email policy (in conjunction with Security Team task)
- Develop/revise Consent forms, policy and procedures
  - Develop forms, policy and procedures
  - Develop Organized Healthcare Arrangement
  - Determine Affiliated Entities & Obtain Corporate Resolutions
  - Develop Policy over Patient Refusal to Sign Consent
    - Waiver of Rights can not be required in order for patient to obtain treatment
- Review & Revise Medical Staff Bylaws
  - Review/Revise Physician Sanctions
- Develop/revise Authorization forms, policy and procedures
- Develop Opportunity to Agree or Object forms, policy and procedures
  - Hospital Directory & Clergy
  - Individuals Involved in Care
  - Disaster Relief

Privacy Update - Policies

- **Policy Approval Process – Defined by Steering Committee**
  - Medical Exec Committees (at 3 hospitals)
  - Patient Care Policy Committee
  - Hospital Administrative Support Group
  - Hospital Exec Council
  - Baystate Medical Practices
  - Visiting Nurse & Hospice manager's team
  - Information Services Oversight Committee (Email)
  - BHS Exec Committee
  - Foundation Board (Fundraising)
  - Corporate Entity Boards (OHCA & Affiliated Entity agreements)
  - Human Resource Sr. VP (Sanctions)
  - Marketing VP (Marketing
  - IRB (Research)

Privacy Update – Policies (continued)

- BC # 6.800 EMAIL POLICY
- BC # 7.010 PRIVACY POLICY
- BC # 7.020 PATIENT PRIVACY COMPLAINT PROCESS
- BC # 7.030 SANCTIONS POLICY
- BC # 7.110 ACCOUNTING FOR DISCLOSURES
- BC # 7.120 NOTICE OF PRIVACY PRACTICES POLICY
- BC # 7.130 REQUESTING RESTRICTIONS OF INDENTIFIABLE HEALTH INFORMATION AND REQUESTING ALTERNATIVE METHODS OF COMMUNICATION
- BC # 7.140 PATIENT REQUEST TO AMEND DESIGNATED RECORD SET
- BC # 7.150 RIGHT TO INSPECT AND COPY AND AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION (PHI)
- BC # 7.210 DISCLOSURE OF MEDICAL INFORMATION TO FAMILY MEMBERS AND OTHERS INVOLVED IN THE PATIENT'S CARE

Privacy Update – Policies (continued)

- BC # 7.220 PATIENT DIRECTORY OPPORTUNITY TO AGREE OR OBJECT
- BC # 7.310 BUSINESS ASSOCIATE AGREEMENTS
- BC # 7.320 USE OF DE-IDENTIFIED INFORMATION AND LIMITED DATA SETS
- BC # 7.330 BAYSTATE HEALTH SYSTEM DESIGNATED RECORD SET POLICY
- BC # 7.340 PRIVACY MITIGATION POLICY
- BC # 7.410 FUNDRAISING
- BC # 7.420 CORPORATE MARKETING TO PATIENTS POLICY
- BC # 7.605 RESEARCH
- HR-122 NON-RETALIATION AND NON-RETRIBUTION FOR REPORTING ACTUAL OR POTENTIAL WRONG-DOING
- HR-106 CONFIDENTIALITY

Privacy Update - Training

- **Leadership Presentations (Heads-up…HIPAA is coming)**
- **Leadership Train-the-Trainer sessions**
  - **'Phase 1 – HIPAA-Lite' (20 management teams – 500 managers?)**
    - **Manager's Guide**
    - **Handbook for employees**
    - **Quiz**
    - **Video Tape**
  - **'Phase 2 –HIPAA Privacy Policies' (with role-playing)**
    - **Manager's Guide**
    - **Handbook for employees**
    - **Intranet**
      - **Policies & forms**
      - **Other resources**

Privacy Update - Implementation

- **Implementation (the rubber meets the road!)**
  - New procedures/processes
  - Information System modifications?
    - Hospital directory,
    - Notice,
    - Confidential Communications and
    - Accounting for Disclosures
- **April 14th Modifications**
  - What did we miss?
  - What procedures aren't working?
  - Modifications/Tweaking (to policies, procedures & processes)
- **Fall 2003 Follow-up**
  - Compliance Reviews (by 20+ members of Privacy Team)
  - Modifications/Tweaking (to policies, procedures & processes)

Baystate's Next Actions

- On-going Steering Committee decisions on recommended policies and other corrective actions (decision points).
- Continue to identify funding requirements based on those decisions.
- Revise TCS and Security workplans.
- Continue status reporting.
- Continue to examine compliance options considering costs, risks & resource needs.
- Develop/conduct training.
- Establish accountabilities and processes to ensure ongoing compliance & modify as necessary
- Maintain Communication Plan: Baystate-wide Awareness.

Conclusion

- **Baystate recognizes that:**
  - **HIPAA is a combination of several sets of regulations, totaling thousands of pages.**
  - **The regulations will be defined and become effective over several years.**
  - **HIPAA is more than a technology issue, it is also a major cultural & operational issue impacting our operations and the way we interact with our patients.**
- **Our approach to comply with the regulations includes:**
  - **Technology solutions,**
  - **New/revised policies and procedures,**
  - **New/revised contracts,**
  - **Workforce training programs, and**
  - **On-going maintenance and reinforcement.**