HIPAA Summit West II
~ Case Study ~
Building a Health System HIPAA Compliance Program from the Bottom Up

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

Case Study ~ Baystate Health System

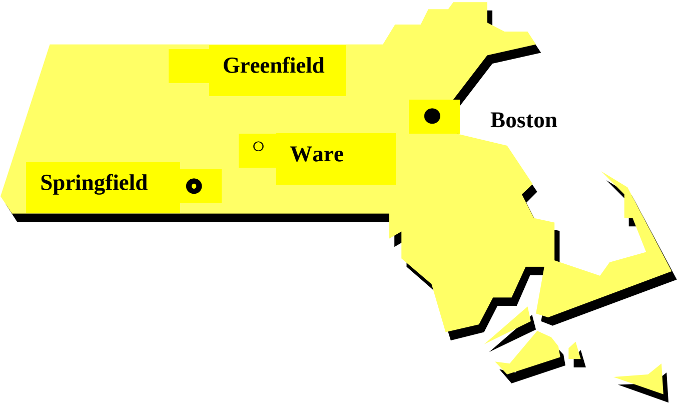
- Baystate ~ Who we are
- HIPAA Project Scope
- Plan for Compliance
- Awareness Efforts
- Project Organization
- Assessment (Gap Analysis) Strategy & Outcome
- Assessment Lessons Learned
- Workplans
- Next Actions
- Conclusion

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 (#39 by SMG Marketing Group).
- 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 and
  - Infusion & Respiratory Services.

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

Baystate's Plan for HIPAA Compliance

- Awareness (Communication Plan)
- We established:
  - Executive Sponsor (Chair of Psychiatry Dept)
  - Steering Committee (VPs and Directors)
  - Project Management Process
- We performed an assessment comparing HIPAA regulations to our current state (gap analysis).
- We'll examine 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.

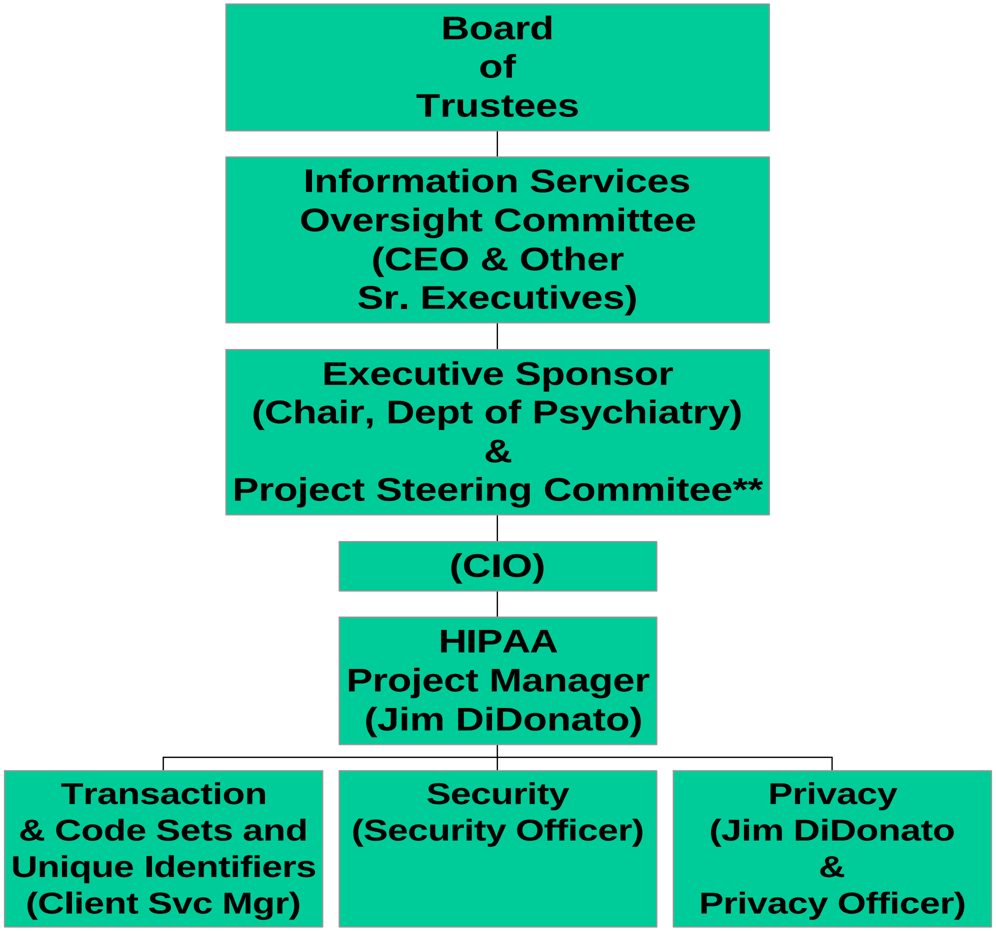
Awareness Efforts

- 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)
Project Manager (Info Sys)
VP (HR)
Staff (Marketing & Communications)
MD (Pediatrician)
VP/CIO
VP/CIO (HMO)
MD (Psychiatry)(Exec. Sponsor)
Director (Facility Security)
VP (Visiting Nurse Assoc)
Director (Patient Acctg)
Director (Physician Billing)
VP (Medical Support Services)
Director (Info Sys)
VP (Ambulatory Care)
Director (Franklin Med Ctr)



Board of Trustees

Information Services Oversight Committee (CEO & Other Sr. Executives)

Executive Sponsor (Chair, Dept of Psychiatry) & Project Steering Commitee**

(CIO)

HIPAA Project Manager (Jim DiDonato)

Transaction & Code Sets and Unique Identifiers (Client Svc Mgr)

Security (Security Officer)

Privacy (Jim DiDonato & Privacy Officer)

Assessment Strategy

- **<u>Option 1:</u> Full HIPAA Assessment, full Organizational Scope with limited Baystate participation:**
  - **Consultant would assign 5 individuals part-time, to the project team (including leadership) & would require:**

    Baystate Info Sys employees - 10 FTE days

- **<u>Option 2:</u> Full HIPAA Assessment, but <u>partial</u> 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 and this option would require a <u>minimum</u> of 4 Baystate employees:**

    Baystate Info Sys employees – 35 FTE days and

    Baystate non-Info Sys employees – 70 FTE days.
  - **All work results would be integrated into a single, cohesive set of assessment deliverables.**

Assessment Strategy ~ Security and Privacy

- Privacy & Security Assessment Phase 1 – Consultant Team:
  - Academic medical center and much of the administrative service entity.
- Privacy & Security Assessment Phase 2 – Baystate Assessment Team:
  - Physician practices and ambulatory care,
  - The remainder of the administrative service entity,
  - Ambulance company,
  - 2 smallest hospitals,
  - Visiting Nurse Association & Hospice,
  - Infusion & Respiratory Services
- Separately we engaged a Big-5 firm to provide a network security assessment.

Assessment Strategy ~ BHS Transaction & Code Set (TCS)

- **TCS Assessment Phase 1 – Consultant Team:**
  - **Inpatient Billing & Patient Management Applications (SMS/SSI)**
- **TCS Assessment Phase 2 – Baystate Assessment Team:**
  - **Physician Billing Office (IDX)**
  - **Retail Pharmacy (Mediware)**
  - **Ambulance**
  - **Infusion & Respiratory Services (HAI)**
  - **Visiting Nurse Association & Hospice (Stat)**
  - **Mary Lane Hospital (SDK)**
  - **Other?**
    - **Medicaid eligibility from 2 sites**
    - **Employee Benefits for enrollment and disenrollment**

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.
- Contingency plans not current.
- Doors unlocked (medical practices, hospital stairwells, and other ‘secure’ areas).
- Need for new policies.

Assessment Outcome - Policies and Procedures

- Workstation use – logoff, direction screens face, use of data bases containing patient information, etc.
- Employee Transfer (modification of access authorization).
- Faxes/printers (transmission & receipt).
- Additional restrictions on use/disclosure of information.
- Notice of information practices.
- Amendments to medical records and disseminating those changes.
- Over minimum necessary information (process and accountability).
- Contingency planning and testing.
- Passwords.
- Accounting for disclosures.
- Audit trails.

Assessment Outcome - Transaction and Code Sets/EDI

- **Claims/Eligibility/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.

- **Claim Status, Referral and Certification, Coordination of Benefits, etc. not typically processed in any of our applications.**
    - To provide this functionality, vendors may be planning major modifications or new product lines.
    - Baystate would redesign operating activities to take advantage of opportunities to automate.

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

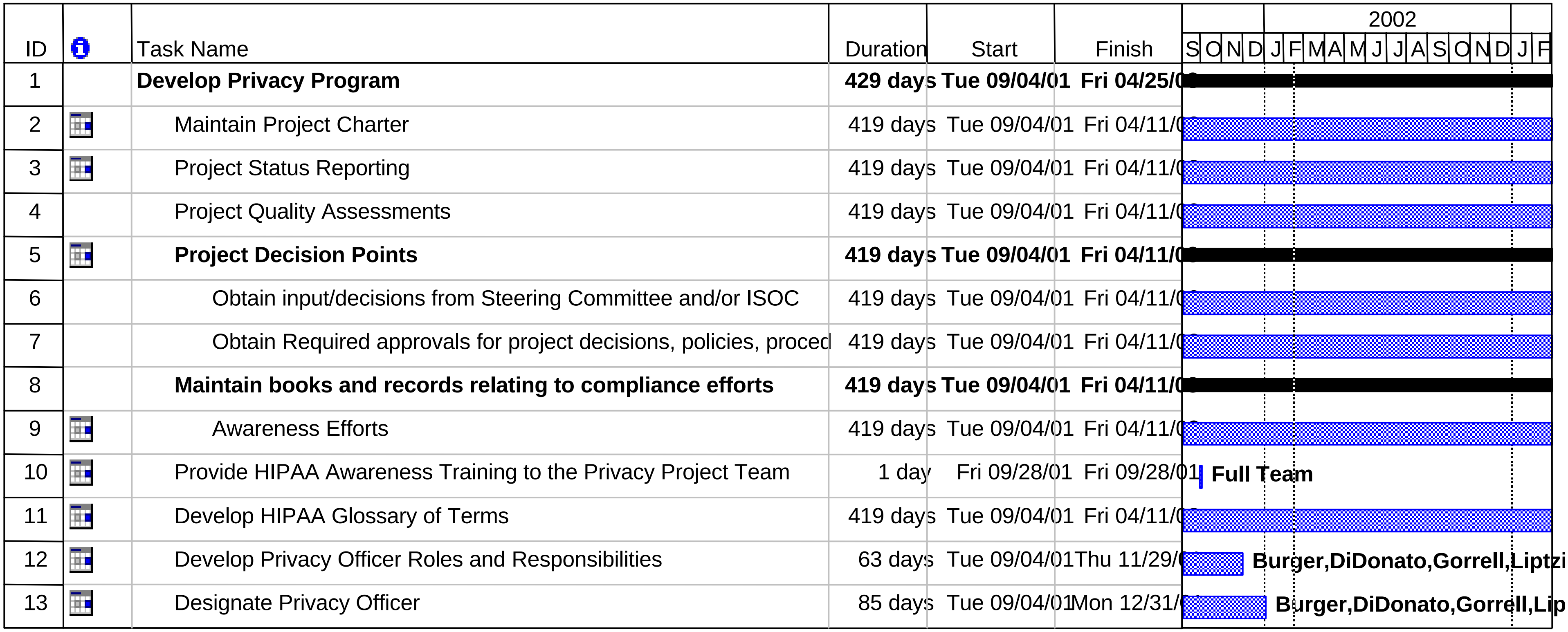
Note: Costs for unpublished regulations could not be considered in our assessment.

Assessment Lessons Learned

- **Project scope management:**
  - Baystate project team (resource contention vs scheduling)
  - Training (the assessment team)
  - Site visits (scheduling conflicts)
  - Analysis & deliverables (meetings/documentation) (under-estimated the follow-up work)
- **Organizational scope - define your organization effectively:**
  - All entities and functions including

    Research,
    Fund raising,
    Marketing.
- **Functional Scope:**
  - EDI preparation and understanding of role
  - Computer applications containing patient information
  - Identify how and where information is disclosed

Privacy Workplan (Draft)



ID	🛈	Task Name	Duration	Start	Finish
1		**Develop Privacy Program**	**429 days**	**Tue 09/04/01**	**Fri 04/25/0**
2	▦	Maintain Project Charter	419 days	Tue 09/04/01	Fri 04/11/0
3	▦	Project Status Reporting	419 days	Tue 09/04/01	Fri 04/11/0
4		Project Quality Assessments	419 days	Tue 09/04/01	Fri 04/11/0
5	▦	**Project Decision Points**	**419 days**	**Tue 09/04/01**	**Fri 04/11/0**
6		Obtain input/decisions from Steering Committee and/or ISOC	419 days	Tue 09/04/01	Fri 04/11/0
7		Obtain Required approvals for project decisions, policies, proced	419 days	Tue 09/04/01	Fri 04/11/0
8		**Maintain books and records relating to compliance efforts**	**419 days**	**Tue 09/04/01**	**Fri 04/11/0**
9	▦	Awareness Efforts	419 days	Tue 09/04/01	Fri 04/11/0
10	▦	Provide HIPAA Awareness Training to the Privacy Project Team	1 day	Fri 09/28/01	Fri 09/28/01
11	▦	Develop HIPAA Glossary of Terms	419 days	Tue 09/04/01	Fri 04/11/0
12	▦	Develop Privacy Officer Roles and Responsibilities	63 days	Tue 09/04/01	Thu 11/29/0
13	▦	Designate Privacy Officer	85 days	Tue 09/04/01	Mon 12/31/0

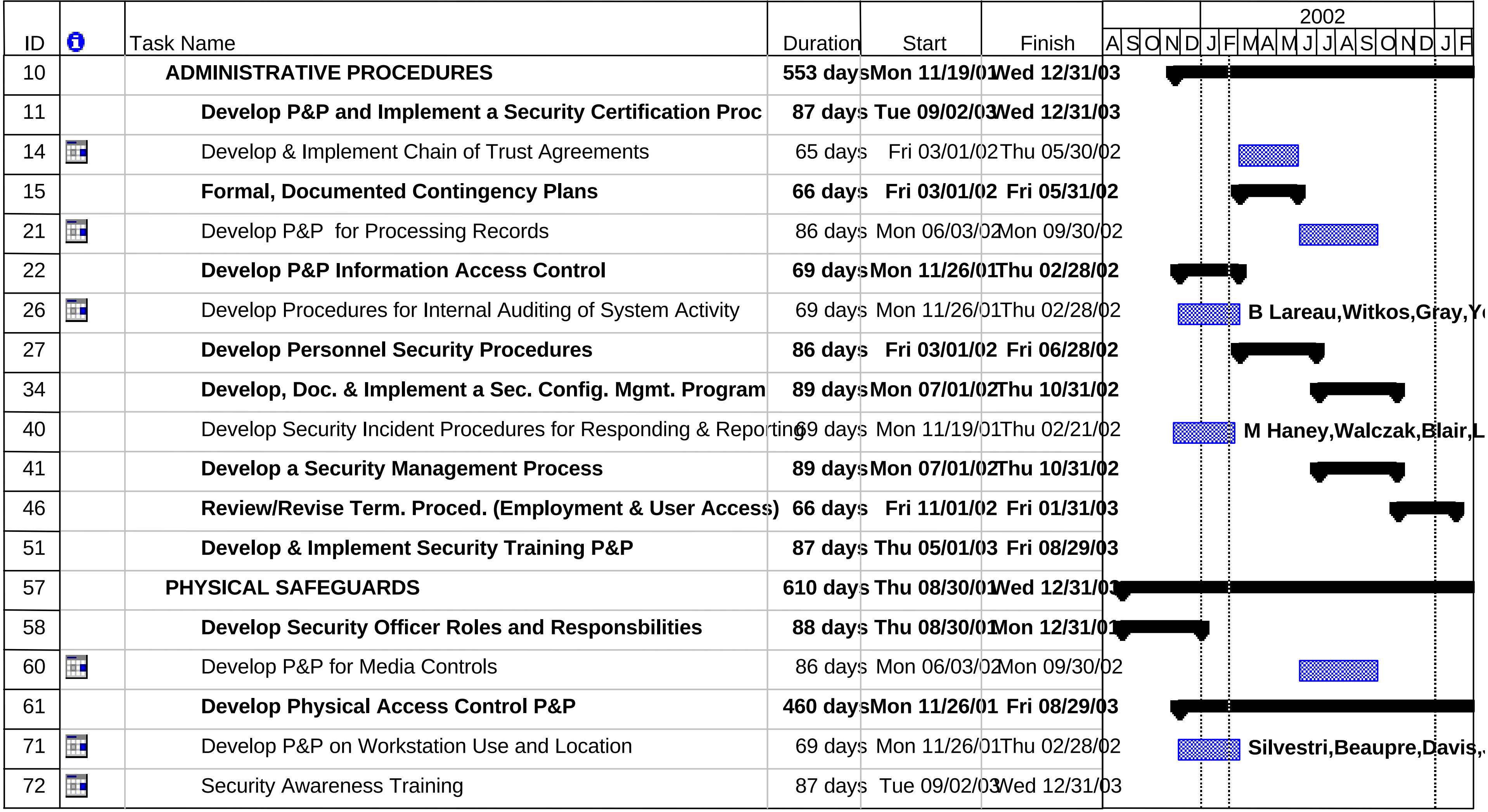
2002
S O N D J F M A M J J A S O N D J F
Full Team
Burger,DiDonato,Gorrell,Liptzi
Burger,DiDonato,Gorrell,Lip

Baystate Health System

Privacy Workplan (Continued)

ID	ℹ	Task Name	Duration	Start	Finish	2002 N D J F M A M J J A S O N D J F M A
14	▦	Define Designated Record Set	74 days	Mon 11/19/01	Thu 02/28/02	Houlihan,Bowers-Kane,Starling
15		**Develop Minimum Necessary policy and procedures**	**95 days**	**Mon 11/19/01**	**Fri 03/29/02**	
16	▦	Develop High-level Policy	95 days	Mon 11/19/01	Fri 03/29/02	Kiah,B LaRue,Pasini,Wroth
17	▦	Develop Departmenthead-level Procedures	95 days	Mon 11/19/01	Fri 03/29/02	Kiah,B LaRue,Pasini,Wroth
18	▦	Develop Matrix tool for Departmenthead Decision-making	95 days	Mon 11/19/01	Fri 03/29/02	Kiah,B LaRue,Pasini,Wroth
19	▦	Develop Policy for use of PHI for Transcription	95 days	Mon 11/19/01	Fri 03/29/02	Kiah,B LaRue,Pasini,Wroth
20	▦	Coordinate with HIPAA Security Project Team/System Administrators	95 days	Mon 11/19/01	Fri 03/29/02	Kiah,B LaRue,Pasini,Wroth
21	▦	Review/revise Email policy (in conjunction with Security Team task)	74 days	Mon 11/19/01	Thu 02/28/02	A. Girard,Fogg,Gerstle
22		**Develop/revise Consent forms, policy and procedures**	**95 days**	**Mon 11/19/01**	**Fri 03/29/02**	
23	▦	Develop forms, policy and procedures	74 days	Mon 11/19/01	Thu 02/28/02	Faulkner,Hansen,Lavallee,Ten
24	▦	Develop Organzied Healthcare Arrangement	74 days	Mon 11/19/01	Thu 02/28/02	Faulkner,Hansen,Lavallee,Ten
25	▦	Determine Affiliated Entities & Obtain Corporate Resolutions	95 days	Mon 11/19/01	Fri 03/29/02	Faulkner,Hansen,Lavallee
26		**Review & Revise Medical Staff Bylaws**	**29 days**	**Tue 02/19/02**	**Fri 03/29/02**	
27	▦	Review/Revise Physician Sanctions	29 days	Tue 02/19/02	Fri 03/29/02	Faulkner,Hansen,Lavallee
28		**Develop Policy over Patient Refusal to Sign Consent**	**74 days**	**Mon 11/19/01**	**Thu 02/28/02**	
29	▦	Waiver of Rights can not be required to obtain treatment	74 days	Mon 11/19/01	Thu 02/28/02	Faulkner,Hansen,Lavallee,Ten
30	▦	Develop/revise Authorization forms, policy and procedures	74 days	Mon 11/19/01	Thu 02/28/02	Carty,Guzik,Wellington
31		**Develop Opportunity to Agree or Object forms, policy and procedures**	**74 days**	**Mon 11/19/01**	**Thu 02/28/02**	
32	▦	Hospital Directory & Clergy	74 days	Mon 11/19/01	Thu 02/28/02	Coffelt,Creswell,Dubreuil
33	▦	Individuals Involved in Care	74 days	Mon 11/19/01	Thu 02/28/02	Coffelt,Creswell,Dubreuil
34	▦	Disaster Relief	74 days	Mon 11/19/01	Thu 02/28/02	Coffelt,Creswell,Dubreuil

Security Workplan (Draft)



ID	ℹ	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

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.**
- **Develop, review/revise workplans.**
- **Continue weekly/monthly status reporting.**
- **Continue to examine compliance options considering costs, risks & resource needs.**
- **Develop/conduct training.**
- **Establish accountabilities and processes to ensure ongoing compliance.**
- **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 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.**