Practical Issues in HIPAA Implementation

John Glaser, PhD
Vice President and CIO
Partners HealthCare System

August 20, 2002

Observations

- HIPAA is not “another Y2k”
  - Business consequences are less severe
  - The timetable is not absolute
  - The Board is not anxious
  - The scope is more limited
  - There are “work arounds”
- HIPAA is useful
  - It is causing worthwhile/needed activity
  - Standards have been defined or decreed
  - Common frameworks have been established
  - It raises the privacy stakes

Observations

- The organization's orientation should be one of obtaining value and not one of being a victim
  - Funding, while mindful of the need for compliance, should be "considered"
  - Improving organizational performance, and not passing an audit, should be the focus
- The definition of compliance is not clear
  - The role and approach of the auditors are not fully defined
  - The timetable maybe elastic

Our Philosophy in Preparing for HIPAA

"HIPAA is on the management agenda, but it is not a major diversion of resources….We will make *reasonable* decisions about what to do in security and privacy…..Do we pay attention to HIPAA? Sure. Is it a dominant topic in any given week? Not at all"……..

J. Glaser, CIO Partners Healthcare System
iHealth Beat
California Healthcare Foundation
April 8, 2002

EDI Projected Revenue/Expense Reduction Contribution at Partners

Transaction	Denial Reserve Reduction	Interest on Cash Acceleration	Labor Efficiency	TOTAL ANNUAL BENEFIT		ONE-TIME CASH ACCELERATION
Eligibility Verification	$ 1,995	$ 81	$ 83	$ 2,159		$ 1,008
Referral/Authorizations	$ 4,923	$ 202	$ 55	$ 5,180		$ 2,810
Claims Submission		$ 100	$ 47	$ 147		$ 1,248
Claims Status Inquiry		$ 70	$ 1,136	$ 1,206		$ 874
Claim Remittance			$ 86	$ 86		
Total	$ 6,918	$ 435	$ 1,407	$ 8,778		$ 5,940

Dollars in thousands

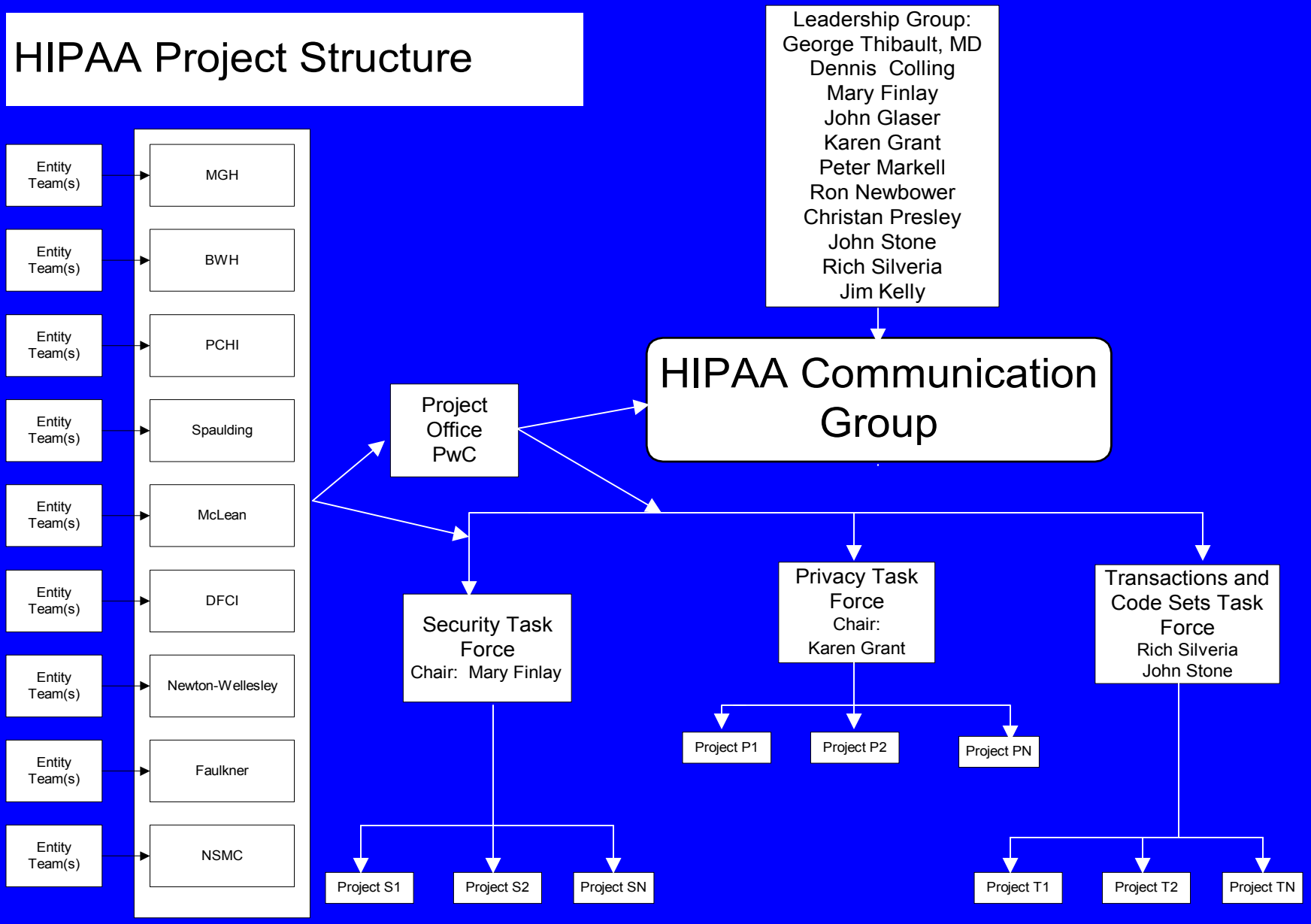
Business Reasons for Security/Confidentiality

- Security
  - Increased Internet presence
  - Clinical and operational impact of “impaired” systems
  - Bad press
- Confidentiality
  - Delivery of patient care
  - Basic right
  - Bad press

Organization of the Effort at Partners

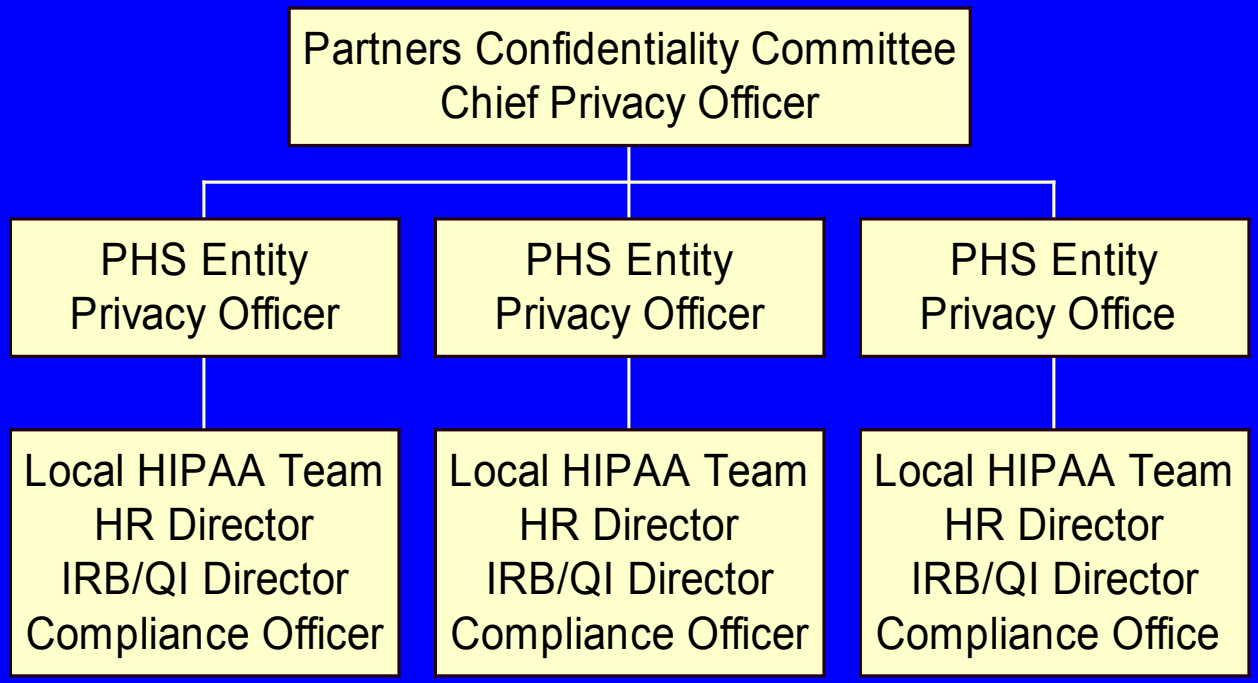
- Broad oversight is provided by the Corporate Compliance Office, Internal Audit and Board Audit Committee
- HIPAA implementation oversight is the responsibility of the Deputy CIO
- Each entity is responsible for its own implementation
- Several committees have been formed:
  - HIPAA Steering Committee
  - HIPAA Communications Committee
  - Security Sub-committee
  - Confidentiality Sub-committee
  - Codes/Transaction Sets Sub-committee

HIPAA Project Structure



Privacy Officer Structure

Corporate Privacy Officer and Entity-Level Privacy Officers



Role of Privacy Officers

Directors of HIS serve as Privacy Officials

1. Provide Leadership and Coordination of privacy issues within the network; they are at point for addressing operational issues and represent their entity at Partners Committees.

2. Collaborate with other experts in their entity (HR, Compliance Officers, Patient Advocacy staff) in order to ensure that implementation and ongoing measurement of privacy-related activities occurs.

3. Identify and address privacy issues as they arise, bringing "lessons learned" to Partners for development of system-wide changes for improvement.

Privacy Officer Responsibilities and Measures of Success

- Participate in Partners Operating Committee Meetings, and report on entity-level progress
- Lead entity Confidentiality Committee Meetings, where local implementation efforts are developed, implemented, and monitored
- Conduct meeting evaluations to assess effectiveness and to ensure that opportunities for improvement are addressed
- Complete periodic privacy readiness assessments within their entity

Initial Privacy Projects

- P1: Confidentiality and Security Committee **- establishes a Steering Committee responsible for information privacy**
- P2: Decision Points **- develops a baseline for definitions and standards to ensure consistent implementation of privacy projects**
- P3: Privacy Official **- creates and assigns a privacy official**
- P4: Awareness and Training **- establishes and implements an on-going program to raise awareness and educate staff on privacy and confidentiality guidelines**
- P5: Information Risk Assessment **- identifies current operational and technical risks to information**
- P6: Data Classification **- inventories data to identify confidential information and allows categorization of findings to assist in the implementation of need-based access -**
- P7: Business Partner Inventory **- inventories business partners to identify types of shared information and business partners where contracts may require amendment or changes**

  P8: De Identification of Data **- creates and implements guidelines for the de-identification of data**
- P9: Minimum Necessary Disclosure **- establishes guidelines for minimum necessary disclosure**
- P10: Policy and Procedure Development **- develops and implements formal policies and procedures**
- P11: Information Practice Notice **- updates the process for communicating to patients their rights relating to their health information -**
- P12: Documentation Retention **- creates and implements corporate document management and retention policies**
- P13: Research- **reviews the research as it relates to the new regulations**

Decision Points

Partners Healthcare Systems, Inc.
HIPAA Support
Privacy Project Levels

Project Name	Consistent Implementation	Implementation Advisories	Uniquely Determined
P1: Confidentiality and Security Steering Committee	X		
P2: Decision Points	X		
P3: Privacy Officer	X		
P4: Awareness and Training		X	
P5: Information Risk Assessment			
PHS Systems Information		X	
Entity Specific Systems Information			X
P6: Data Classification			
PHS Systems Information	X		
Entity Specific Systems Information			X
P7: Business Partner Inventory		X	
P8: De Identification of Data	X		
P9: Minimum Necessary Disclosure	X		
P10: Policy and Procedure Development			
Patient's Rights			
Detailed notice of information practices		X	
A patients ability to restrict access to medical records	X		
Protection of deceased patients private health information	X		
Patient access and amendment to private health information		X	
Accounting of disclosures of private health information		X	
Ability to accept and process patient complaints		X	
Information Disclosure			
De-identification of private health information	X		
Access of individuals to PHI		X	
Private health information use and disclosure authorizations	X		
Employee			
Staff training of policies and procedures	X		
Use of home computers for work	X		
Transmitting faxes and leaving voicemail			X
P11: Information Practice Notice		X	
P12: Documentation Retention		X	

HIPAA Implementation Timeline - Privacy

Partners Healthcare System

2001					2002												2003					
Aug.	Sept.	Oct.	Nov.	Dec.	Jan.	Feb.	Mar.	Apr.	May	June	July	Aug.	Sept.	Oct.	Nov.	Dec.	Jan.	Feb.	Mar	Apr	May	June
Development of Consent and Authorization Forms						Pilot, Implement, and Monitor Use of Consent, Authorization, and Privacy Notice											Ongoing Monitoring and Tracking					
				Development of Privacy Notice																		
						Development of PHS Forms, Policies and Procedures, and Contracts							Pilot, Implement, and Monitor Forms, Policies and Procedures/Contracts				Ongoing Monitoring and Tracking					
							Modification of Forms, Policies and Procedures as appropriate, for entity use															
						Define Research Needs			Develop Research Policies and Procedures					Implement and Monitor Research Policies			Ongoing Monitoring and Tracking					
				Conduct (Entity) Gap Analysis		Conduct (Entity) Risk Analysis and Improvement Plan			Implement Improvement Strategies				Conduct Gap Analysis		Conduct Risk Analysis and Improvement Plan		Ongoing Monitoring and Tracking					
					Develop Strategy and core module for PHS Training			Conduct Training for PHS Corporate Staff									Ongoing Training, Tracking, and Monitoring Training for Improvement					
									Incorporate Core Training into New Employee Orientation													
Entity Privacy Awareness Campaigns/Training									Conduct Entity HIPAA Privacy Training													

Transaction Set Implementation Considerations

- Assessing constituent readiness
  - IS vendors (payer and provider)
  - Clearinghouse
  - Payer and provider remediation plans
- Mechanisms for communication of remediation plans
- What level of contingency planning should be pursued?
  - Cash flow considerations for providers
  - Contractual and legislative remedies?

Examples of Potential Operational Considerations

- **Additional data is required**
  - Vendor compliance with transactions does not necessarily ensure situational logic is sound
- **Use of translation services**
  - Which data will be used in translation? Which data will be ignored? Variation by payers and providers?
  - Will "core" productive capacity really change?
- **Payer specific business logic**
  - Payers only accept a subset of the values associated to a specific data element?
  - Will new required fields drive expansion of related edit logic?
  - Will limitations experienced with previous claims formats be corrected via the utilization of the expanded data sets?
- **Payers mapping rejection reason codes to HIPAA standards**
  - Implications for clarity of processing instruction "rule" sets
  - Impacts on management reporting subsystems
  - Mapping changes consistent for electronic versus paper reports/processes?

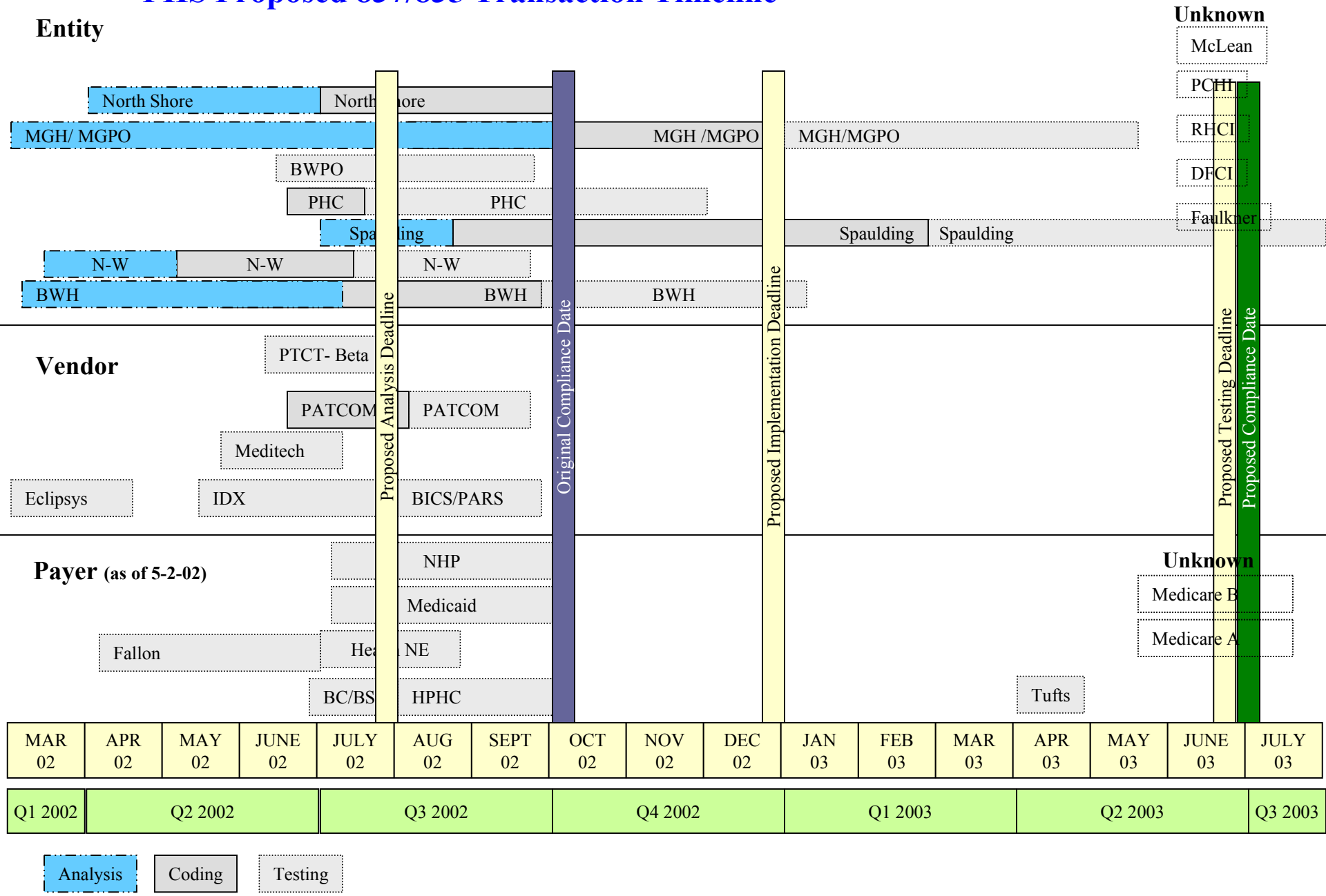
Examples of Additional Provider Claims Data

- If subscriber is NOT patient
  - Need both patient and subscriber demographic information
  - Need subscriber gender code and birth date
- If patient is pregnant
  - Pregnancy indicator (not necessarily pregnancy services)
- Amounts Paid
  - Estimated & actual amount patient paid
  - Other payer paid amount
- If multiple doctors work on a patient; ALL doctors are reported at claim and service line (if different)
  - Referring Provider
  - Other Provider
  - Attending Physician
  - Operating Physician
  - Rendering Physician

Example: 837 P Elements missing from IDX Standard Charge Entry

- Auto Accident State Code
- Auto Accident Country Code
- For Podiatry Services- Date Last Seen
- Pregnancy Indicator - required if patient is pregnant (not necessarily linked to pregnancy services)
- Date of Last Menstrual Cycle
- Service Authorization Exception Code
- Taxonomy Code
- Insurance Type Code
- Claim Filing Indicator Code
- Rendering Provider
- Purchased Services Provider
- Emergency Indicator
- Special Program Code
- IDE Number
- Copay Exemption Code
- Homebound indicator
- Home Healthcare Information
- Home Oxygen Therapy Information
- DME Information
- Referring Provider Name

PHS Proposed 837/835 Transaction Timeline



Consortium Reports

Claims TAT Analysis

Specifications available

PERIOD COVERED _____ to _____	Paper Claims: Paid	Paper Claims: Denied	Electronic Claims: Paid	Electronic Claims: Denied	All Claims: Paid	All Claims: Denied
Average Provider Submit Time/Claim (days)						
Average Provider Submit Time/Claim $ (days) (if possible)						
Average Payer Turnaround Time/Claim (days)						
Average Payer Turnaround Time/Claim $ (days) (if possible)						
Total Turnaround Time/Claim (days)						
Total Turnaround Time/Claim $ (days) (if possible)						
#/% of Claims Paid in less than/equal to 30 days						
#/% of Claims Paid in less than/equal to 60 days						
#/% of Claims Paid in less than/equal to 90 days						
#/% of Claims Paid in greater than 90 days						

Components of Security Plan

- Physical Security
- Disaster Recovery Plan
- Account Management
- Network Security
- Application Security
- Desktop Security
- Security awareness and training
- Policies

External Audit Review Findings

- As currently designed and implemented, information security controls are inadequate to ensure protection of information assets and to detect security intrusions proactively:
  - Logging and review of IDs with high level access privileges is not performed
  - Dial up and platform level access violation monitoring is not conducted
  - Excessive number of NT accounts
  - No intrusion detection system
  - A firewall has been implemented but no supporting policies that provide structure and guidance
  - Procedure for reviewing firewall logs have not been established

Our Areas of Focus

- Development of a security organization, including a decision making process
- Development of an 18 month plan for security initiatives for each key area of technology
- Incorporation of security focus and standards into new processes of technical architecture, project initiation, product management and solutions delivery
- Hiring of dedicated staff in the areas of network security and disaster recovery efforts to advance these efforts
- Implementation of key policies to support our security measures
- Incorporation of security awareness into privacy training efforts
- Utilization of HIPAA security regulations as framework, despite unclear implementation timeline

Security Organization

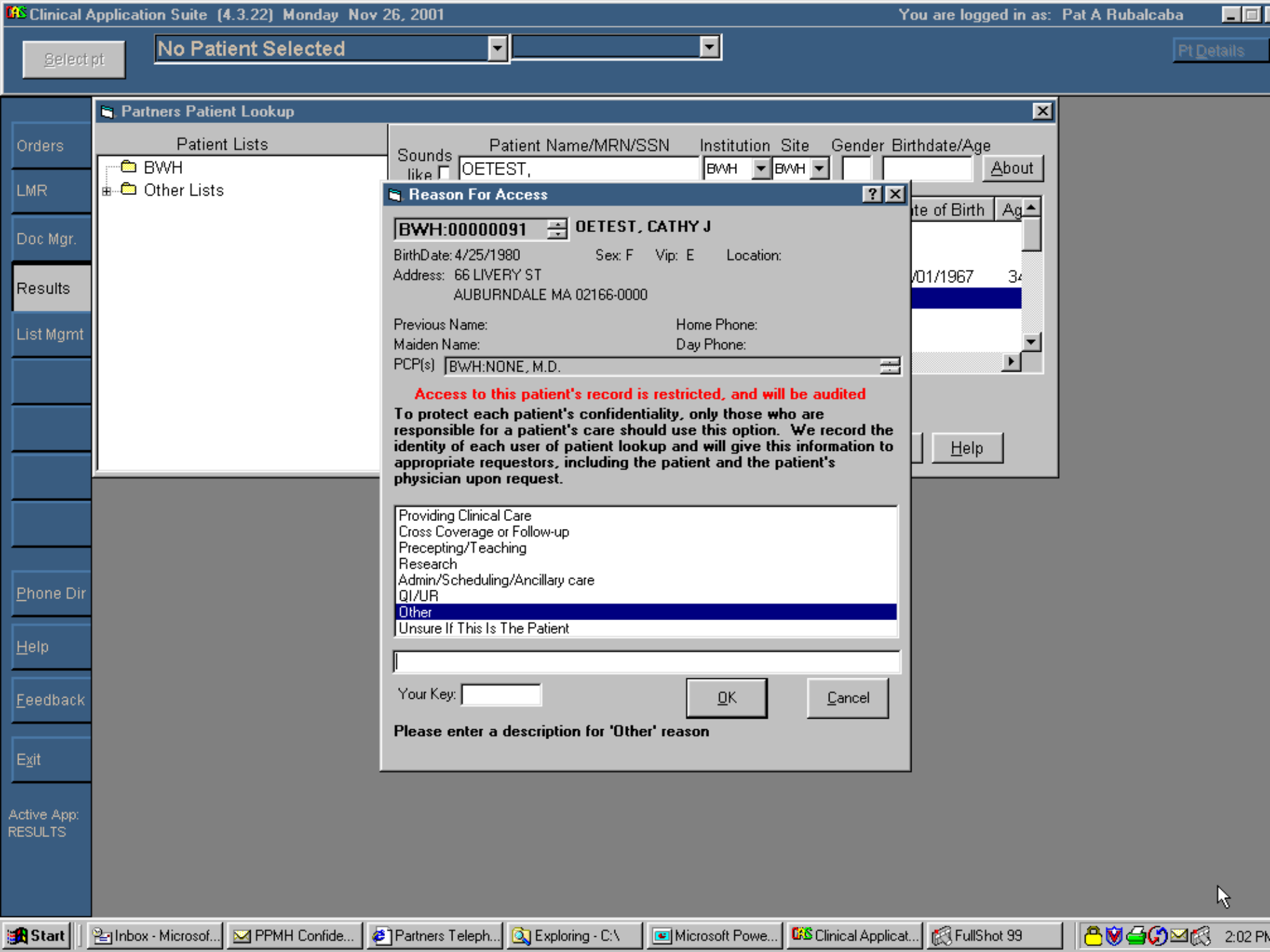
- Security Committee
  - Membership: Senior level IS managers, Internal Audit and Compliance
  - Role: High level direction setting and communication on efforts
- Security Work Group
  - Membership: Senior level functional IS managers
  - Role: Coordination and management of security agenda
- Technical Architecture (TA) Council
  - Membership: Senior level IS managers
  - Role: Establish security standards and ensure adherence to standards through TA process
- PHS Confidentiality Steering Committee
  - Membership: Senior level representation from HIM, OGC, Medical Staff and Information Systems
  - Role: Partner in areas of overlap between security and privacy

Network Security

- Leader, Scott Rogala, Corporate Manager of Network Engineering
- Scope of Effort
  - Develop network security plan to ensure we are protected from intrusions and viruses
  - Facilitate secure access methods to our network
- Status
  - Wireless Security-solution in place by August, 2002
  - Security Zones-project plan to be done by end of May; implementation in phases during remainder of FY02 and during FY03
  - Upgrade of VPN/PKI access method-implementation planning underway for Q1FY03 implementation.
  - Anti-virus e-mail hub-vendor selected; FY03 funding requested

Account Management

- **Inactive User Accounts deleted**
  - **2,000 February 2001**
  - **3,700 October 2001**
  - **Maintain as an ongoing process**
- **Added requirements when creating accounts**
  - **Name, sex, date of birth, primary site, employee flag, and numeric id**
- **PeopleSoft /HR as source system for account management**
  - **Initiate PeopleSoft -->NT User Account interface**


Clinical Application Suite (4.3.22) Monday Nov 26, 2001
You are logged in as: Pat A Rubalcaba
Select pt
No Patient Selected
Pt Details
Partners Patient Lookup
Patient Lists
BWH
Other Lists
Sounds like
Patient Name/MRN/SSN
OETEST,
Institution
Site
Gender
Birthdate/Age
About
Reason For Access
BWH:00000091
OETEST, CATHY J
BirthDate: 4/25/1980
Sex: F
Vip: E
Location:
Address: 66 LIVERY ST
AUBURNDALE MA 02166-0000
Previous Name:
Maiden Name:
Home Phone:
Day Phone:
PCP(s)
BWH:NONE, M.D.
Access to this patient's record is restricted, and will be audited
To protect each patient's confidentiality, only those who are responsible for a patient's care should use this option. We record the identity of each user of patient lookup and will give this information to appropriate requestors, including the patient and the patient's physician upon request.
Providing Clinical Care
Cross Coverage or Follow-up
Precepting/Teaching
Research
Admin/Scheduling/Ancillary care
QI/UR
Other
Unsure If This Is The Patient
Your Key:
OK
Cancel
Please enter a description for 'Other' reason
Help
Orders
LMR
Doc Mgr.
Results
List Mgmt
Phone Dir
Help
Feedback
Exit
Active App: RESULTS
Start
Inbox - Microsof...
PPMH Confide...
Partners Teleph...
Exploring - C:\
Microsoft Powe...
Clinical Applicat...
FullShot 99
2:02 PM

Status of External Audit Findings

Audit Findings	Current Year Initiaives	FY03 Initiative
• Logging and review of ID's with high level access privelages	X	
• Excessive number of NT Accounts	X	
• Develop processes to support firewall implementation	X	
• Implementation of an intrusion detection system		X
• Monitoring of dial-up and platform level access violation		X

PHS Training Modules
Draft, 5/8/02

HR/Occup Health
* Policies and procedures for *
* Occupational Health, EAP staff
* Uses and disclosures of PHI
* Accounting of disclosures
* Self-insured policies and procedures

Contracting/Materials Management
* BA Agreements
* Uses and Disclsoures of PHI
* Accounting of disclosures

Admitting/Registration/ED/ Financial Counselors
* Consent, Privacy Notice
* Verification of ID of person requesting information
* Limited Access/VIP/Directory Policies

Marketing/QA/Fundraising
* Consent, Authorization, Privacy Notice
* Definitions policies (QA, DM, Marketing)
* Policies and Procedures related to Fundraising/Marketing
* Defintion of "operations"

Finance (Patient Accounts, Credit Collections, Customer Service)
* Consent policy (definition of "operations"
* Disclosing PHI for QA/UR purposes
* State Laws related to disclosure of PHI

Research
* De-identification policy
* IRB Policies/Informed Consent
* Authorization, when needed

Core Module
* What is HIPAA?
* Why Privacy is Important
* How HIPAA will impact patients/patient rights
* How HIPAA will impact you as an employee/your responsibilities
* What you should do to report a breach
* What you should tell a patient or family member that wants to complain about a privacy issue

HIS Staff
* HIS Policies and Procedures:
  - authorization, disclosure, release of information
  - amendment policies
  - accounting of disclosures
  - disclosing PHI for QA/Research
  - verification of ID of individuals requesting information
* Federal, state laws, regs

Mental Health Clinicians (in addition to info listed under MD/ Nursing):
* Psychotherapy notes policy
* Limited Access Policies

Medical Staff/Residents/Medical Students
* Consent, Authorization, and Privacy Notice
* De-identification Policy (incl. presentations)
* Personal Database Policy
* Using and disclosing PHI for treatment purpos
* Protecting passwords
* Protecting privacy in public areas and/or whe using wireless technology
* "Core" Research Policies
* Limited Access Policies
* Fundraising and Marketing Policies

Nursing/Patient Care Services (Rehab Therapists, Technologists)
* Consent, Authorization, and Privacy Notice
* De-identification Policy (incl. presentations)
* Personal Database Policy
* Using and disclosing PHI for treatment purposes
* Protecting passwords
* Protecting privacy in public areas and/or when using wireless technology
* Verification of ID of person requesting PHI
* "Core" Research Policies
* Limited Access Policies

Information Systems
* Security policies and Procedures
* Personal Database Policy
* Disclosing PHI for QA/Research
* Use of wireless technology

Why is HIPAA Important to Partners Healthcare?

- **It supports our mission**

Partners is committed to serving the community. We are dedicated to enhancing patient care, teaching, and research, and taking a leadership role as an integrated health care system.

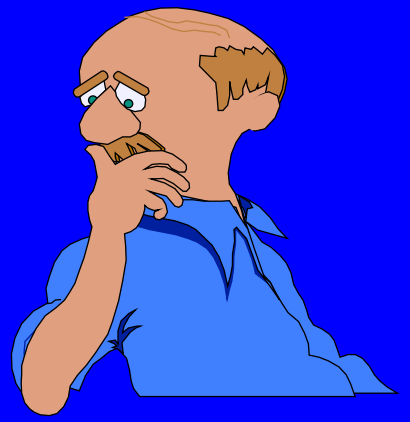
We recognize that increasing value and continuously improving quality are essential to maintaining excellence.

Why is HIPAA Important to Partners Healthcare?

- Maintaining patients' trust in their caregivers is critical to obtaining a complete history, medical record, and carrying out an effective treatment plan
- It's the right thing to do

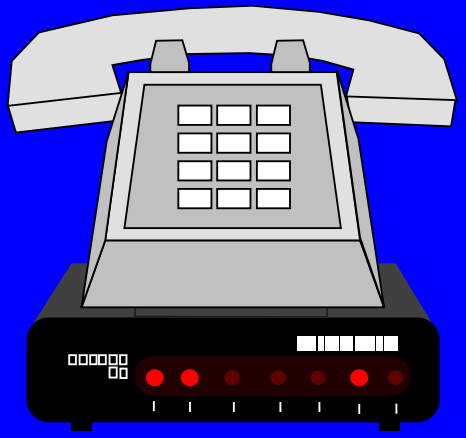
Failure to Protect Patient Privacy Can Have Dire Consequences

- It has been documented that failure to protect patient privacy has caused patients to:
  - Lose Jobs
  - Be Victims of False Rumors
  - Lose Insurance Coverage
  - Become Estranged from Friends and Family
  - Lose Custody Battles
  - Be harassed by the Media



Some examples…….

How to Report a Privacy Concern or Breach



Contact the Compliance Hotline: (617) 724-1177

or

To Report Anonymously: 1-800-856-1983

Q&A: Privacy

- What are examples of the “minimum necessary” rule in your daily work; do changes in practice need to be made?
  - Whiteboards, patient lists in public view
  - Patient names at bedside
  - Reports

Answer

- Whiteboards and patient lists are permitted, although they should be out of public view, when feasible
- Patient names at bedside are permitted as part of hospital operations
- Identifiable information in reports should be limited to the minimum necessary for their purpose, and should be distributed only to those who have a need to know

Q&A: Privacy

- **HIPAA allows identifiable health information to be shared among Partners-owned (or "controlled") entities on a need-to-know basis for certain purposes (without obtaining a signed authorization). What are these reasons?**

Answer

Identifiable health information may be shared among Partners entities for TPO:

- **Treatment**
- **Payment**
- **Healthcare Operations (QA/QI, Utilization Review, Disease Management, Credentialing, Auditing, Accreditation, etc.)**

Training the Workforce

- **Central Responsibilities**
  - Development of "core" training slides and identification of role-based modules
  - Reviewed and compiled list of training resources that meet defined criteria
  - Development of HIPAA intranet (P&P's, Forms, Q&A's, Training Resources)
- **Entity Responsibilities**
  - Develop role-based modules
  - Plan training budget
  - Implement and track training

Summary and Conclusions

- A HIPAA philosophy and orientation need to be determined
- HIPAA is no different than other initiatives; organization, governance structures, project plans and resources need to be put in place
- Implementation of HIPAA does require that a wide range of practical issues be identified and addressed
- Ongoing sharing of HIPAA experiences, lessons learned and re-usable “stuff” is critical