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

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

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

**Entity Team(s)**
- MGH
- BWH
- PCHI
- Spaulding
- McLean
- DFCI
- Newton-Wellesley
- Faulkner
- NSMC

**Project Office PwC**

**Security Task Force**
Chair: Mary Finlay

**Privacy Task Force**
Chair: Karen Grant

**Transactions and Code Sets Task Force**
Rich Silveria
John Stone

**Leadership Group:**
George Thibault, MD
Dennis Colling
Mary Finlay
John Glaser
Karen Grant
Peter Markell
Ron Newbower
Christian Presley
John Stone
Rich Silveria
Jim Kelly
Privacy Officer Structure
Corporate Privacy Officer and Entity-Level Privacy Officers

Partners Confidentiality Committee
Chief Privacy Officer

- PHS Entity Privacy Officer
  - Local HIPAA Team
    - HR Director
    - IRB/QI Director
    - Compliance Officer

- PHS Entity Privacy Officer
  - Local HIPAA Team
    - HR Director
    - IRB/QI Director
    - Compliance Officer

- PHS Entity Privacy Office
  - Local HIPAA Team
    - HR Director
    - IRB/QI Director
    - Compliance Office
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: DeIdentification 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**

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

**Partners Healthcare System**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Modification of Forms, Policies and Procedures as appropriate, for entity use</td>
<td>Ongoing Monitoring and Tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conduct (Entity) Gap Analysis</td>
<td>Conduct (Entity) Risk Analysis and Improvement Plan</td>
<td>Implement Improvement Strategies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conduct Gap Analysis</td>
<td>Conduct Risk Analysis and Improvement Plan</td>
<td>Ongoing Monitoring and Tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2002</td>
<td>Develop Strategy and core module for PHS Training</td>
<td>Conduct Training for PHS Corporate Staff</td>
<td>Ongoing Training, Tracking, and Monitoring Training for Improvement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conduct Entity HIPAA Privacy Training</td>
<td>Entity Privacy Awareness Campaigns/Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Development of Consent and Authorization Forms**

**Pilot, Implement, and Monitor Use of Consent, Authorization, and Privacy Notice**

**Modification of Forms, Policies and Procedures as appropriate, for entity use**

**Define Research Needs**

**Develop Research Policies and Procedures**

**Implement and Monitor Research Policies**

**Conduct (Entity) Gap Analysis**

**Conduct (Entity) Risk Analysis and Improvement Plan**

**Implement Improvement Strategies**

**Conduct Gap Analysis**

**Conduct Risk Analysis and Improvement Plan**

**Develop Strategy and core module for PHS Training**

**Conduct Training for PHS Corporate Staff**

**Conduct Entity HIPAA Privacy Training**

**Entity Privacy Awareness Campaigns/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

## Entity

<table>
<thead>
<tr>
<th>Entity</th>
<th>Original Compliance Date</th>
<th>Proposed Analysis Deadline</th>
<th>Proposed Implementation Deadline</th>
<th>Proposed Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>North Shore</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGH/MGPO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BWPO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N-W</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BWH</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Vendor

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Original Compliance Date</th>
<th>Proposed Analysis Deadline</th>
<th>Proposed Implementation Deadline</th>
<th>Proposed Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTCT- Beta</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PATCOM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meditech</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eclipsys</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BICS/PARS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Payer (as of 5-2-02)

<table>
<thead>
<tr>
<th>Payer</th>
<th>Original Compliance Date</th>
<th>Proposed Analysis Deadline</th>
<th>Proposed Implementation Deadline</th>
<th>Proposed Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fallon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medicaid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPHC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BC/BS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tufts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Timeline

- **Q1 2002**
- **Q2 2002**
- **Q3 2002**
- **Q4 2002**
- **Q1 2003**
- **Q2 2003**
- **Q3 2003**
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>______ to ______</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average Provider Submit Time/Claim (days)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average Provider Submit Time/Claim $ (days) (if possible)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average Payer Turnaround Time/Claim (days)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average Payer Turnaround Time/Claim $ (days) (if possible)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Turnaround Time/Claim (days)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Turnaround Time/Claim $ (days) (if possible)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#/% of Claims Paid in less than/equal to 30 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#/% of Claims Paid in less than/equal to 60 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#/% of Claims Paid in less than/equal to 90 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#/% of Claims Paid in greater than 90 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
## Status of External Audit Findings

<table>
<thead>
<tr>
<th>Audit Findings</th>
<th>Current Year Initiatives</th>
<th>FY03 Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Logging and review of ID’s with high level access privileges</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>• Excessive number of NT Accounts</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>• Develop processes to support firewall implementation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>• Implementation of an intrusion detection system</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>• Monitoring of dial-up and platform level access violation</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
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
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?
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.