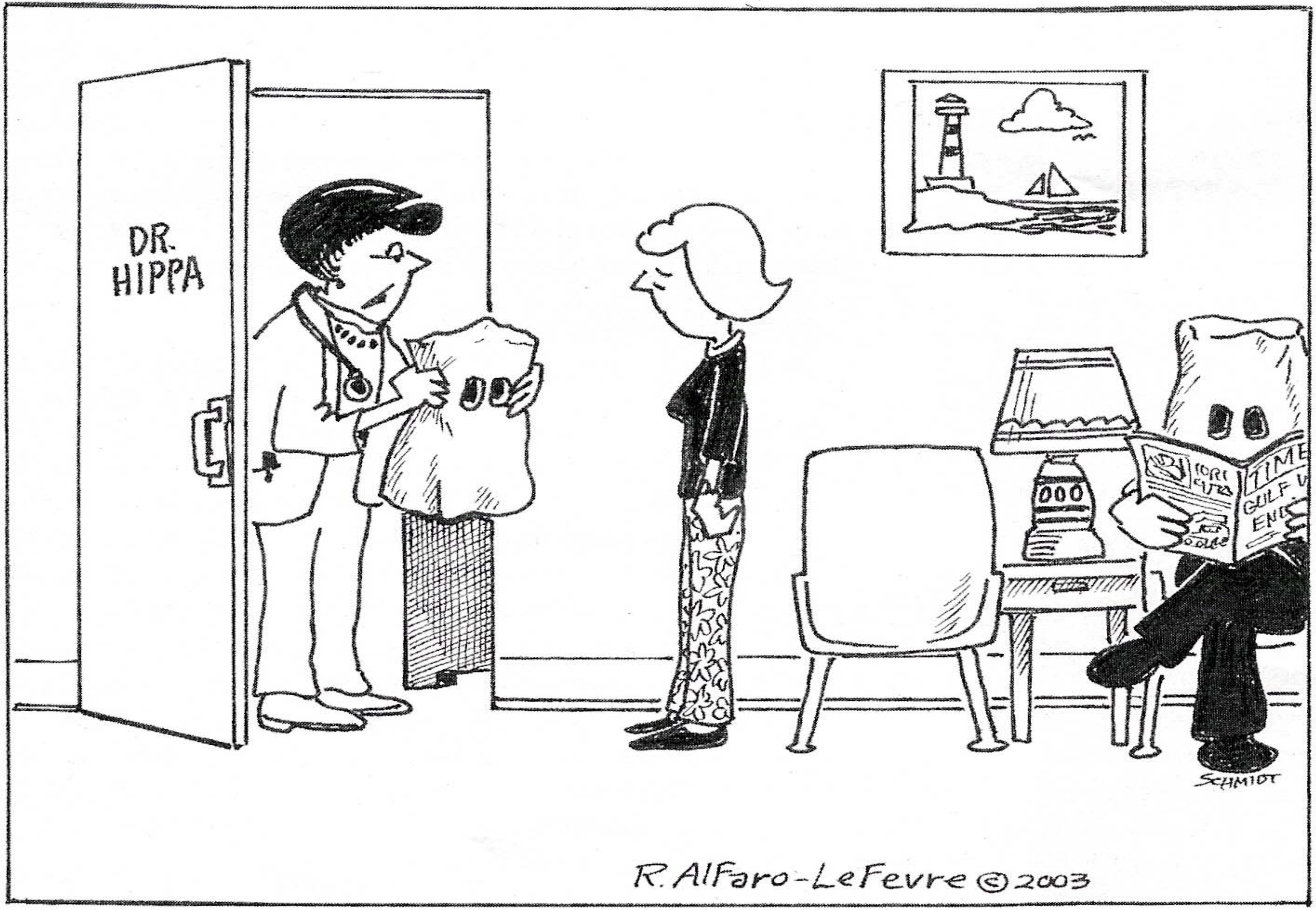
STATEN ISLAND UNIVERSITY HOSPITAL
NORTH SHORE - LONG ISLAND JEWISH HEALTH SYSTEM

Staten Island University Hospital: A Case Study in Effective Monitoring and Reporting Systems for Compliance with HIPAA Privacy Policies and Procedures

Eighth National HIPAA Summit

March 8, 2004

Baltimore Waterfront Marriott, Baltimore, MD



R. AlFaro-LeFevre © 2003

"Take this bag and put it over your head. It's our way of ensuring privacy."

STATEN ISLAND
UNIVERSITY HOSPITAL
SPRING
SPRING

Office of Civil Rights

- As of February 2004 the Office of Civil Rights has received over 4000 complaints averaging 100/week.
- Most common type of complaints include:
  - Impermissible uses of PHI
  - Inadequate safeguards
  - Minimum necessary
  - Denial of access to patient's own Medical Record
- What type of systems do you have in place to monitor complaints and the effectiveness of your Privacy Program?

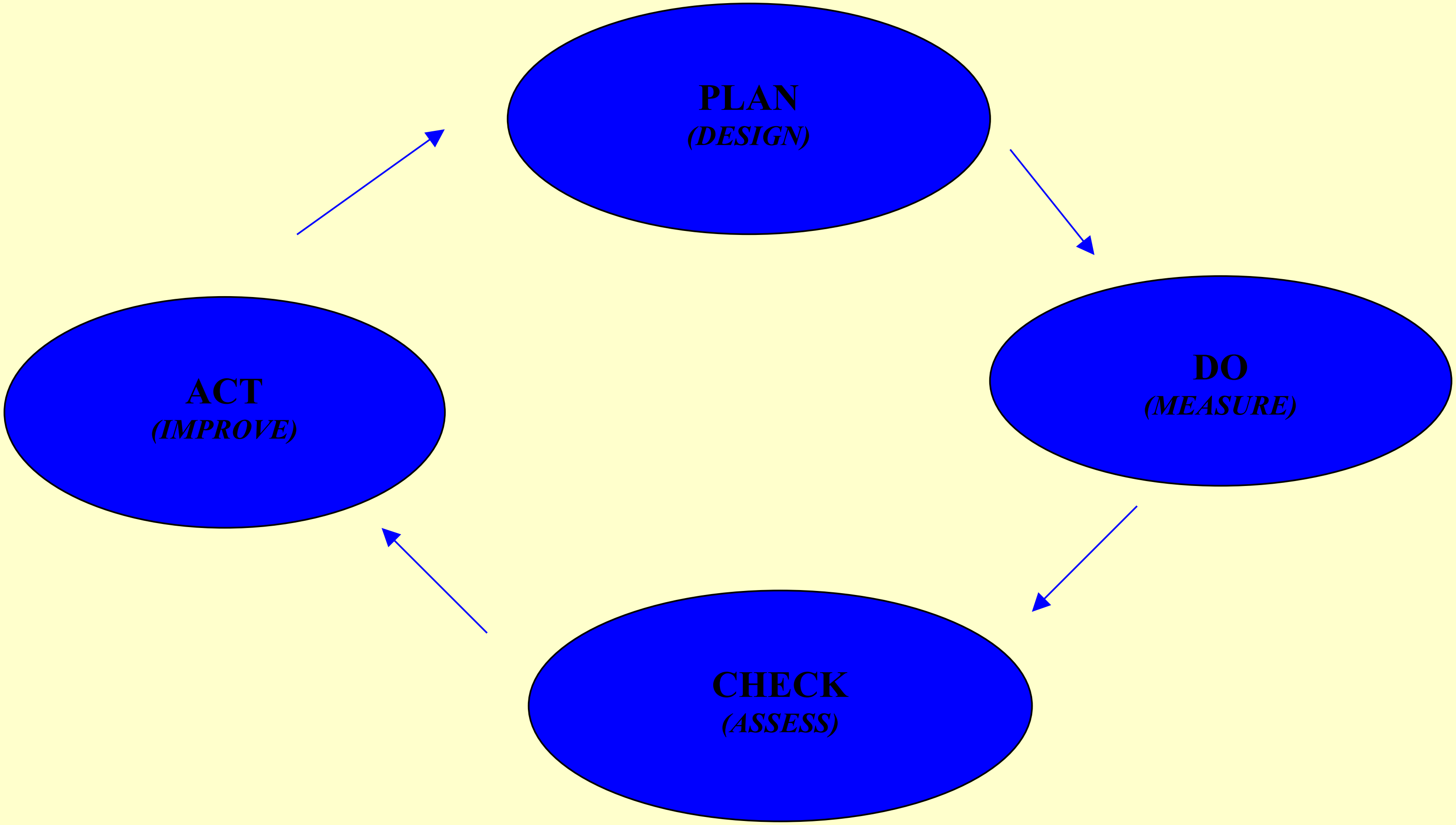
Objectives

Participants will:

- understand how the concepts of Plan-Do-Check-Act can be incorporated to implement an effective Privacy Program;
- enhance their knowledge of monitoring tools for ongoing compliance with organization Privacy polices and procedures;
- gain insight into how to incorporate existing systems to assist in ongoing monitoring of compliance.

Plan-Do-Check-Act Cycle

- **Plan** (Design) - New processes are designed effectively and the design process is concise, systematic, and based on professional organization standards.
- **Do** (Measure) – Implement the Plan and identify methodology to monitor the effectiveness of the Plan.
- **Check** – (Assess) - Analyze the result of data collection and establish a baseline to compare performance overtime.
- **Act** – (Improve) – improvement is a continuous process and usually leads to redesign or modification of existing processes.



PLAN

(DESIGN)

DO

(MEASURE)

CHECK

(ASSESS)

ACT

(IMPROVE)

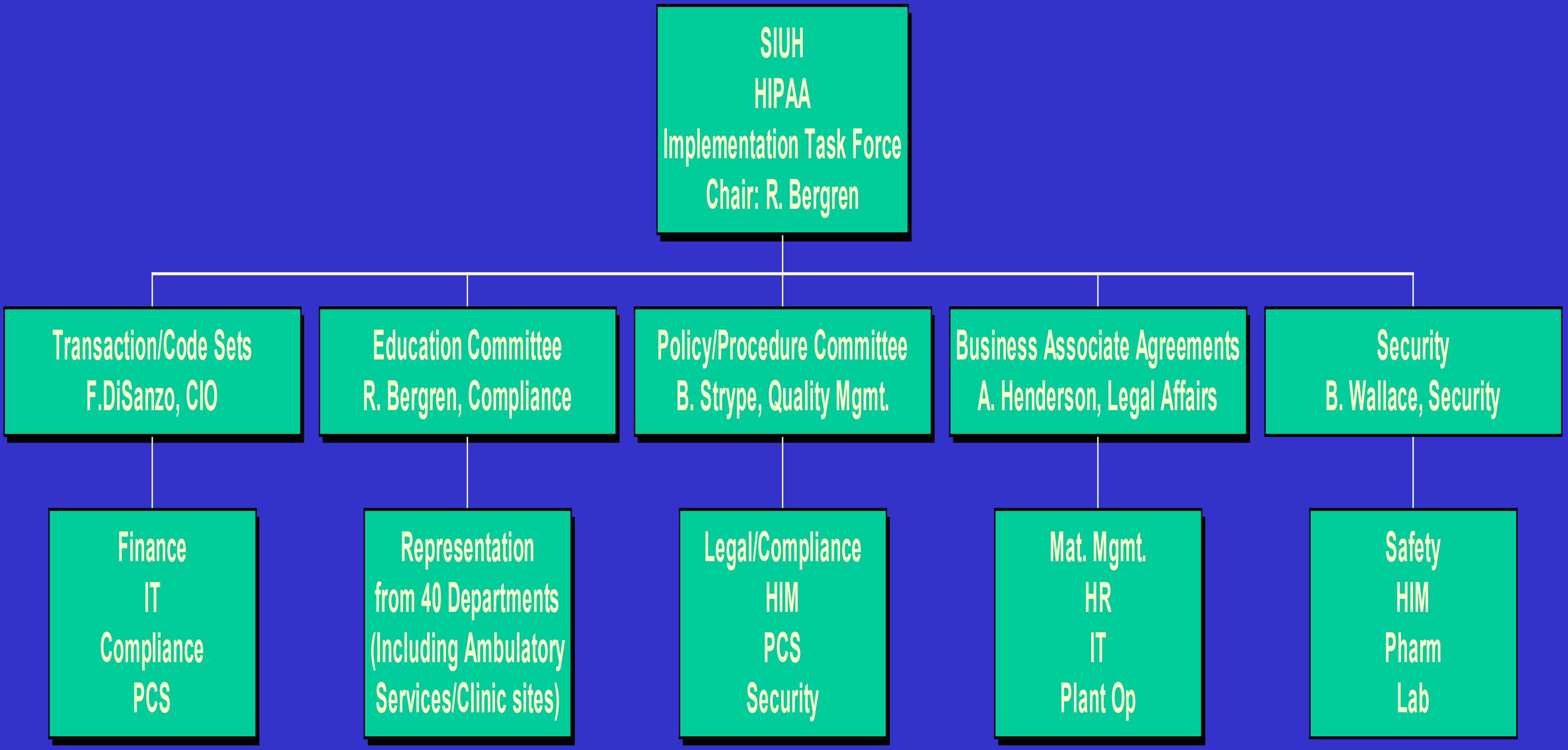
Plan: Design the Process

(before April 14, 2003)

Commitment of Board of Trustees, Executive and Medical Staff

Using the PDCA process a Interdisciplinary team was formed to develop and implement a effective process for compliance with HIPAA Privacy Regulations lead by the Compliance and Privacy Officers.

HIPAA Task Force



SIUH
HIPAA
Implementation Task Force
Chair: R. Bergren

Transaction/Code Sets
F.DiSanzo, CIO

Finance
IT
Compliance
PCS

Education Committee
R. Bergren, Compliance

Representation
from 40 Departments
(Including Ambulatory
Services/Clinic sites)

Policy/Procedure Committee
B. Strype, Quality Mgmt.

Legal/Compliance
HIM
PCS
Security

Business Associate Agreements
A. Henderson, Legal Affairs

Mat. Mgmt.
HR
IT
Plant Op

Security
B. Wallace, Security

Safety
HIM
Pharm
Lab

3/2/2004

Plan: Design the Process

HIPAA Task Force identified key components for HIPAA Compliance:

- ❖ Privacy Education/Training
- ❖ Privacy Policies and Procedures (including Privacy Notice)
- ❖ Business Associate Agreements
- ❖ Transaction/Code Sets
- ❖ Security –lock and key issues, disposal of PHI.

Plan: Design the Process

How to demonstrate compliance with HIPAA regulations?

Task Force met weekly and Committee Chairs reported on their progress with areas identified through the “Gap Analysis” report, their tasks included

- Review of current policies/systems/contracts;
- Review current Complaint process;
- Education/Training process;
- Disposal of patient information/Security;
- Tracking of contracts- Business Associate Agreements.

Plan (Design the Process) :

Education and Training

- 5800 staff;
- Classroom style training vs. Computer-based training;
- Train the Trainer- representative of 40 departments;
- Used current meeting structures when possible;
- Back-up resource-Staff Development responsible to reach per diem, float staff, night staff;
- Develop and implement a tracking system to monitor compliance.

Plan: (Design the Process):

Through HIPAA Task Force

Individual Departments were given the task of:

- Policies/Procedures- identify/collect all department-specific policies that apply to the receipt, use, disclosure of PHI;
- Identify/collect contracts within the department that may apply to Business Associate requirement;
- Identify sources of PHI;
- Identify users of PHI;
- Identify users of PHI outside the department;
- Identify transfer of PHI within and outside the department.

Plan (Design the Process):
Privacy Policies and Procedures

1. Notice of Privacy Practices
2. Accounting of Disclosures
3. Safeguards to Medical Information
4. Safeguards to Employee’s Patient Information
5. Request for Medical Information
6. HIPAA-compliant authorization
7. Amending PHI
8. Marketing/Fund-raising
9. Minimum Necessary – Need to Know
10. De-identifying PHI
11. Complaint Process
12. Disposal of PHI

Policy	Contents	Existing policy?	Responsible Party
Disclosure/release of information (disclosures that generally do not require a consent/authorization 164.502(f), (g) 164.512 164.514	Who can act as personal representative Verification before disclosure Treatment(examples) Continued treatment (transfer to another provider) Payment(ex of disc. Related to payment) Operations Use/disclosure by students Research, required by law,public health,abuse/vulnerable adult Oversight, judicial proceedings,handling subpoena, court orders, deceased pts,spec gov't functions,others, disclosure of de-identified information		
Marketing/Fundraising 164.514	Limitations to use of PHI for M/F, when PHI can be used w/o authorization for marketing, when auth is required for Marketing, what info can be used for fundraising, what info can be used for fundraising, who can use PHI for fundraising, Opt-out notification process.		
Disclosing Directory Information 164.510(a)	Obtaining permission to disclose What can be disclosed, to whom can it be disclosed, handling calls to receptionist, front desk, nurses station, etc.Directory boards, room numbers.		

Plan: (Design the Process):

Notice of Privacy Practices (NPP)

- Development Team for the NPP was comprised of Legal, Compliance, Regulatory Affairs and Health Information Management;
- Developed a policy and procedure;
- Identified all points of entry into the system;
- Documentation of receipt of the NPP (Receipt tracked electronically through registration database);
- Provided a "script" to registrars distributing the NPP.

Plan: (Design the Process):

Accounting of Disclosures

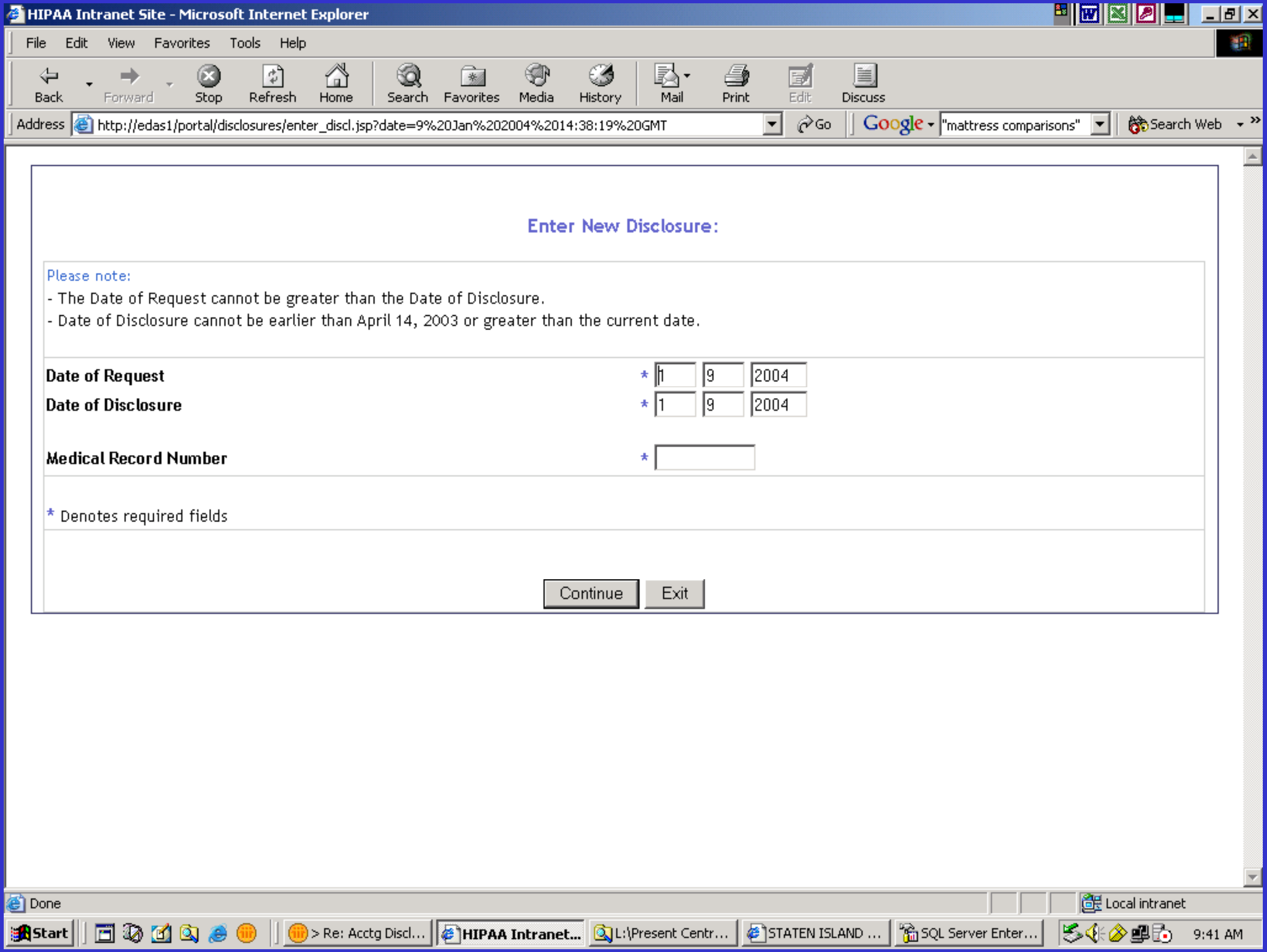
A subcommittee of Policy/Procedure Committee was established;

- Inventoried all departments using HIPAA Task Force- to identify the type of PHI disclosures made/department;
- Identified staff within departments as point person;
- IT Department designed a program to capture and track this data;
- Database was accessible through intranet site.

The type of disclosure to be tracked for compliance with HIPAA Privacy regulation include any reporting to local, state, or federal agencies for public health purposes, any disclosures of PHI not for TPO (treatment, payment,operations) and any disclosures **not** authorized by the patient/legal guardian.

This inventory will assist the IT Department and Health Information Management in the development/implementation of the "***Accounting of Disclosure***" database currently located on the HIPAA intranet site.

Type of Disclosure: Examples Public health reporting Tumor Registry Court ordered subpoenas abuse/neglect SPARCS, Birth/Death	**Type of Data Disclosed Examples** Demographic, diagnosis, insurance information, Product Recalls, etc.	**To: Examples** NYC Depart. Of Health, Tumor Registry, CDC, Attorney, SPARCS FDA	**Address**	**Freq.** Daily, weekly, monthly, quarterly, etc.	**Department/ Site**	**Contact Person in Department/ phone number**
HIV Surveillance	Demographic, partner notification, diagnosis, date of diagnosis, risk factors	NYS Dept of Health	392 Seguine Avenue	Monthly or as requested	Behavorial Sciences HIV Health Services	Wayne Funk, Manager 2643
Court ordered subpoena	Medical records	Richmond Civil Court	11 Richmond Terrace, SI, NY 10301	Prn	Cardiac Cath	A. Jansen x6849
Abuse/ Neglect	Demographic,diagnosis			If occurs	Behavioral Sciences	Paul Smith RN Asst Mgr @ 2794
Public health reporting	Demographics, diagnosis	NYC dept of Health	125 Worth Street NY NY 10013	Prn	Ante Partum Testing	J. Di Giovanni RN 8197



http://edas1/portal/disclosures/enter_discl.jsp?date=9%20Jan%202004%2014:38:19%20GMT

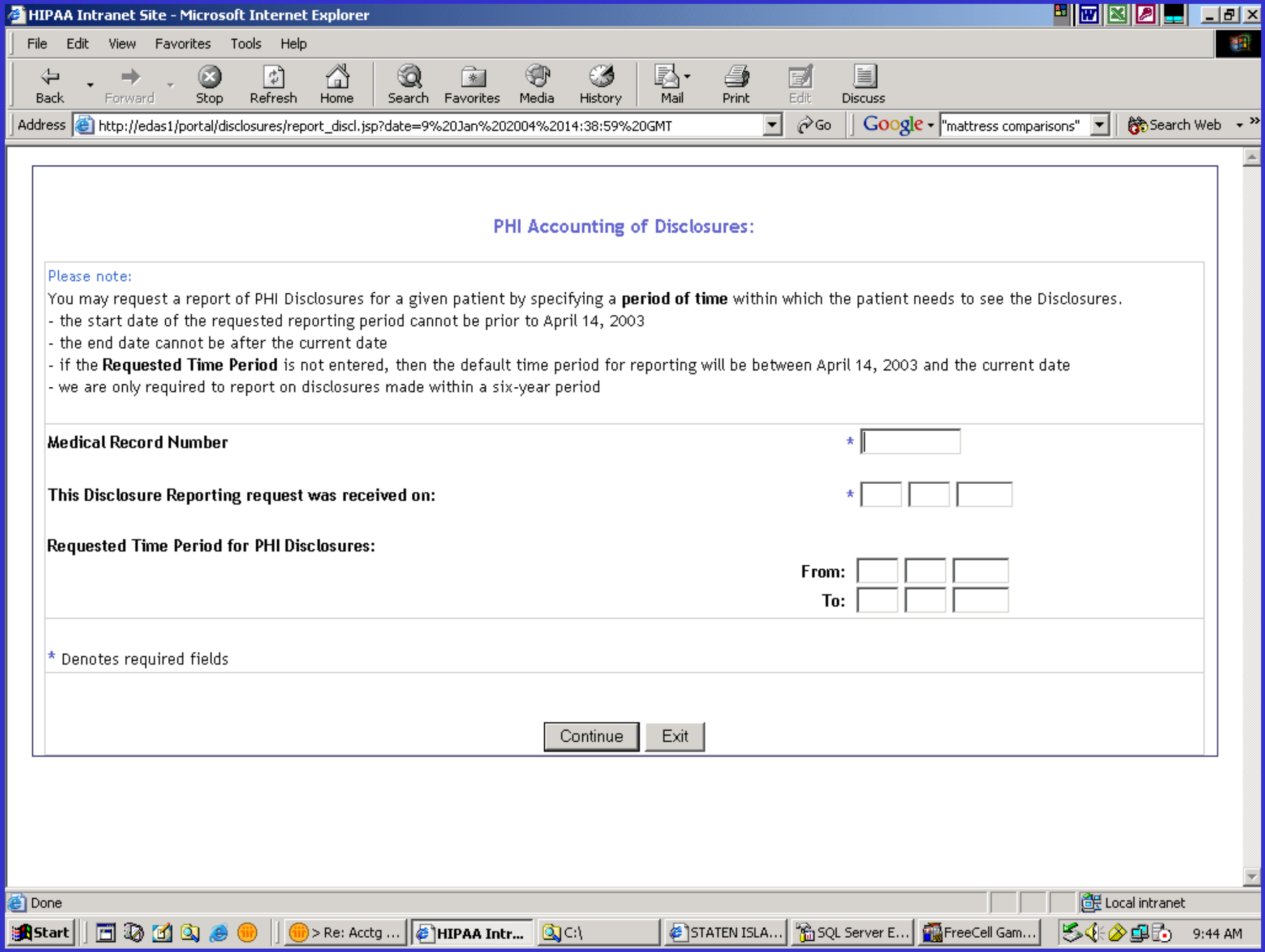
Enter New Disclosure:

Please note:
- The Date of Request cannot be greater than the Date of Disclosure.
- Date of Disclosure cannot be earlier than April 14, 2003 or greater than the current date.

Date of Request	*	1	9	2004
Date of Disclosure	*	1	9	2004
Medical Record Number	*			

* Denotes required fields

Continue Exit


HIPAA Intranet Site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss
Address http://edas1/portal/disclosures/report_discl.jsp?date=9%20Jan%202004%2014:38:59%20GMT
Go
Google "mattress comparisons" Search Web
Done
Local intranet
Start
> Re: Acctg ...
HIPAA Intr...
C:\
STATEN ISLA...
SQL Server E...
FreeCell Gam...
9:44 AM

PHI Accounting of Disclosures:

Please note:

You may request a report of PHI Disclosures for a given patient by specifying a **period of time** within which the patient needs to see the Disclosures.
- the start date of the requested reporting period cannot be prior to April 14, 2003
- the end date cannot be after the current date
- if the **Requested Time Period** is not entered, then the default time period for reporting will be between April 14, 2003 and the current date
- we are only required to report on disclosures made within a six-year period

Medical Record Number * ▭

This Disclosure Reporting request was received on: * ▭ ▭ ▭

Requested Time Period for PHI Disclosures:

From: ▭ ▭ ▭

To: ▭ ▭ ▭

* Denotes required fields

Continue | Exit

Do: Implement,Monitor and Measure

- HIPAA Task Force- continued to meet on a weekly basis until May;
- Over 100 HIPAA Privacy training sessions were provided to staff from February through April, in addition to computer-based training program;
- HIPAA Privacy training was incorporated into Orientation Training Program April 7, 2003;
- Policies and Procedures were approved and distributed:
  - Each department was instructed to prepared a manual specific for Privacy Policies and document review with staff;
- Notice of Privacy Practices was approved and distributed.

Do: Implement,Monitor and Measure

Education and Training

HIPAA Intranet Site

- Accessible for all staff with a computer –included all managers
- Link to Computer-based training program
- Approved privacy policies and procedures were posted
- Approved forms were posted and available to staff
- Notice of Privacy Practice booklet printed/posted
- Privacy Survey Tool was posted
- Links to OCR website (FAQs from OCR website) and Accounting of Disclosure site.

Do: Implement,Monitor and Measure

Security- Lock and Key/Disposal of PHI

- Reviewed current security policies;
- Reviewed paper disposal process for the system:
  - hospital- trash compacted on site
  - off-site-shred;
- Provided a checklist for departments to educate staff and monitor adherence to policies.

Check: Assess the results

(after April 14, 2003)

- Education and Training Program
- Complaints
- Privacy Rounds (incl. receipt of NPP)
- Effectiveness of policies:
  - Accounting of Disclosures
  - Amending PHI
  - Opting Out of the Directory.

Check: Assess the results

Education Training Program

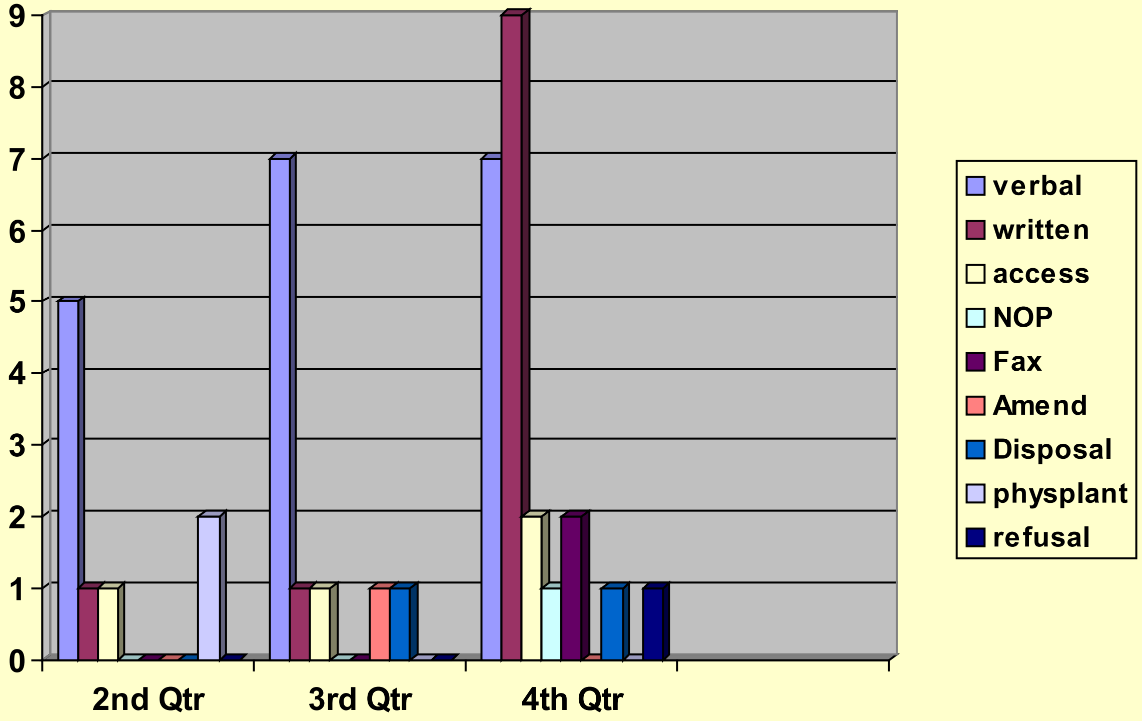
- A review of HR Training database for the hospital revealed only 30% of the departments had documented receipt of training.
- A review of Privacy Officer log/sign-in sheets/access database revealed 78% of the staff had completed HIPAA Privacy training.

Check: Assess the results

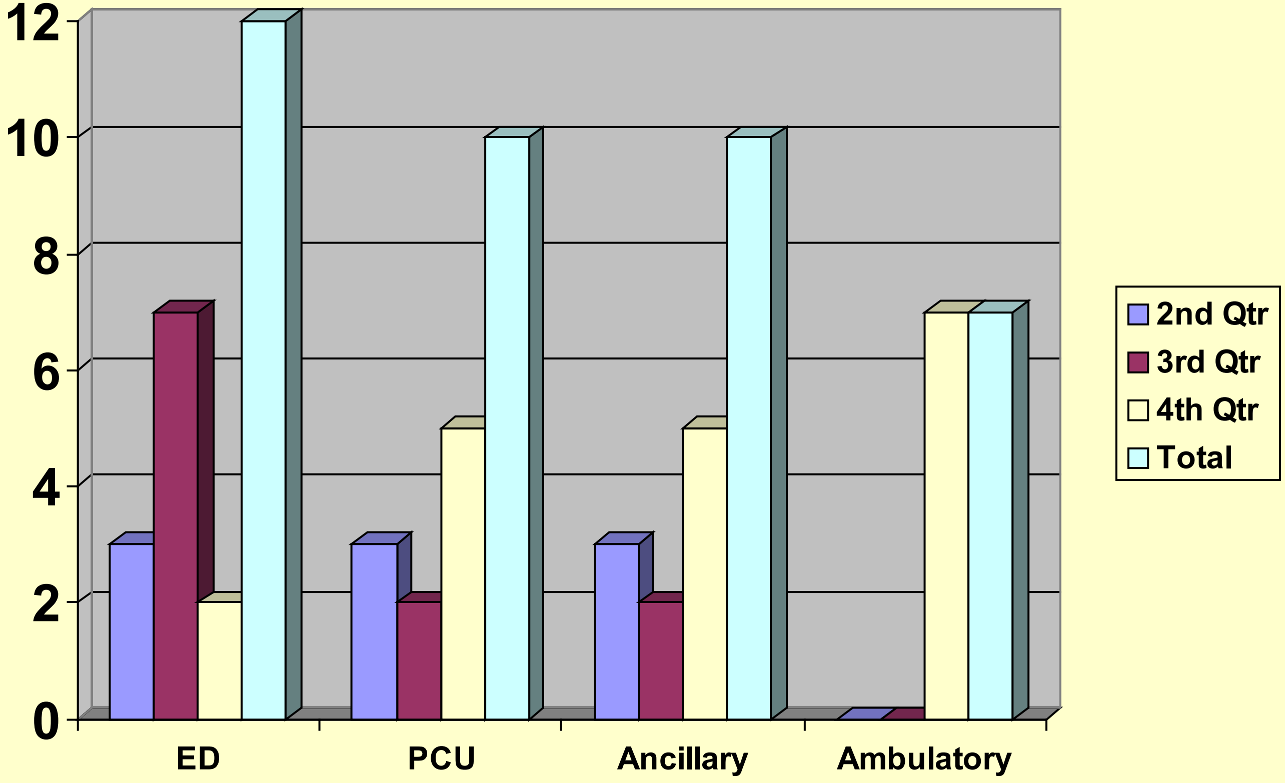
Complaint Process:

- Initially the majority of issues were reported through Patient Representation and Employee Suggestion Program;
- Hotline was operational;
- Identified complaint by type and specific departments/areas with issues;
- 39 complaints/concerns received for 2003.

Complaint/Concern Type



Privacy Complaints by Departments 2003



Check: Assess the results

Notice of Privacy Practice

- Ambulatory: Monitored by Compliance staff for Ambulatory sites (sample review of 30 files per clinic);
- Inpatient: 10 charts were monitored per unit during Privacy Rounds;
- A "glitch" in capturing the date NPP was received was identified.

Sample review by Compliance Staff					
Review of Current Procedure	HIPAA CITATION	Guidelines for Policy Adherence	CLINIC COMPLIANT/ YES/NO	CORRECTIVE ACTION/TIMEFRAME	RESPONSIBLE PARTY
Is the patient provided with a copy of the clinic's Notice of Privacy Practices describing the practice's uses and disclosures of PHI?	164.520 (c)	The clinic should make available a Notice of Privacy Practices statement to each patient. A copy off the entire notice must be posted in the waiting room or other prominent area, and should be available upon request to patients and non-patients. Where necessary, NOP should be available in English, Russian, and Spanish.			
Is the CLINIC'S Notice of Privacy Practices posted?	164.520 (c)(2)(A)	The DEPARTMENT must post a Notice of Privacy Practices in an area that is easily visible to patients.			
Staff has patient's document receipt of the Notice of Privacy Practices in the medical record and staff document receipt in the IBAX Registration screen.	164.520	Receipt documented on either: "Notification of Advance Directives" or "Acknowledgement" form – for patients not eligible for Advance Directives.			

Check: Assess the results

Privacy Rounds

- Revised current tools for Environmental, JCAHO, and Compliance rounds to include Privacy issues;
- Privacy Officer conducted unannounced rounds periodically at both hospital and ambulatory sites;
- Results of rounds were discussed with Managers/staff to identify areas for improvement;
- HIPAA Task Force was informed of results of rounds during quarterly meetings.

Unit/Area Peri-Operative Areas	Administrator/ Manager	Date of Review	Physical Plant issues/ Computer issues	Security Disposal PHI Access to PHI	Policy/Procedures reviewed/clarified w/staff				Corrective Action/Comments
Sample Privacy Rounds Report 2003					**Incidental. Disclosure**	**Min. Necc**	**safeguards**	**Authorizations**	
1). PAST-North	C Griffiths	5/6/03	X	X	x	x	x	O	Re-enforced policies of incidental disclosure, using discretion when speaking with patients, leaving minimum necessary information on voice mail, staff reminded to maintain PHI in folders and turn identifying information toward wall when in chart holder on wall. Review current process for registering patients. Currently there can be more than 2 patients in the registration area waiting to register. Look at possibility of implementing a sign-in sheet and call patients in to register to eliminate congestion/privacy breach in Registrar's Area.
2). PAST-South	C. Griffiths	5/7/03	O	X	X	X	X	O	Staff advised patients can be called by first/last name. Private area, no privacy issues identified.
3). Ambulatory Surgery-South	C. Griffiths	5/7/03		X	X	X	X	O	OR schedule to be placed in a folder/chart cover. Security advised only 1 visitor/patient due to congestion @ nurses station and easy access from elevator. Computer in Nurses Station re-positioned to limit viewing of screen.

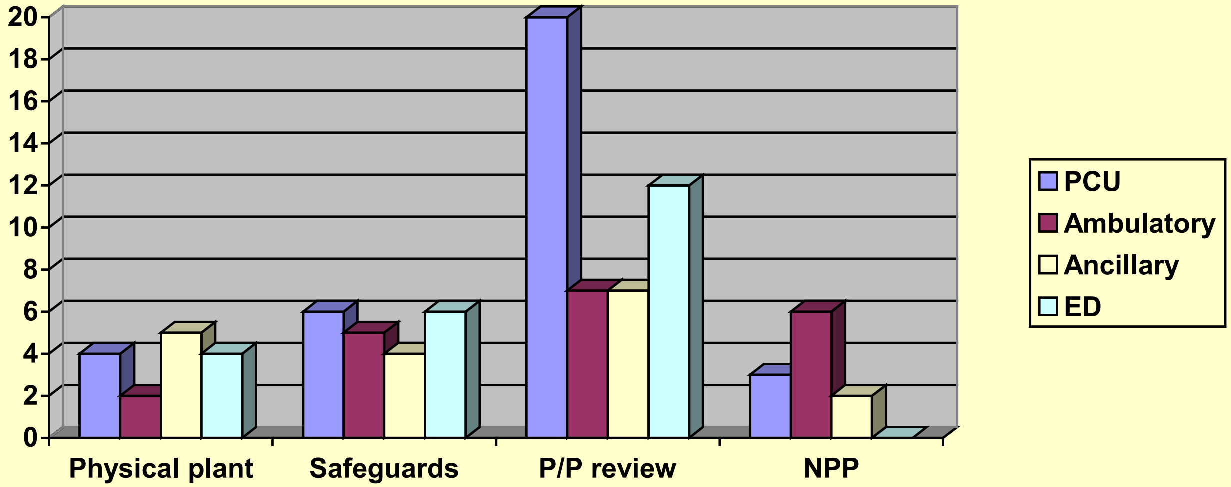
Check: Assess the results

Privacy Rounds

Issues identified included:

- Re-enforcing Privacy Polices/Procedures with staff;
- Recommendations were made for modifications to specific reception areas to increase privacy;
- Patient Safety vs. Privacy concerns were being addressed with Patient Safety taking priority.

Privacy Rounds- Summary of issues 3rd & 4th Qtr 2003



Check: Assess the results

HIPAA - compliant authorization

Issues identified during Privacy Rounds/discussions with staff;

- When did departments need to use the new authorization form?
- Departments were using variations of SIUH authorization for release of PHI form.

Check: Assess the results

Accounting of Disclosures P/P

Request sent out to staff to respond to an “Accounting of Disclosure request in 4th quarter 2003:

- 18% compliance rate initially
- Staff educated on process
- 57% compliance
- Staff were unclear as to their responsibility concerning;
  - timeframes,
  - how to access the database for data entry,
  - purpose of the request,
  - double data entry.

Check: Assess the results

Security/Disposal of PHI P/P

- Monitored during rounds by Privacy Officer, Administrator On Duty Program, Safety Team, JCAHO Team, and Security staff;

- Complaints

Check: Assess the results

Opting Out of Directory P/P

- Electronically done through HBOC System;
- High profile patients- Alias Policy
- Issues identified through employee concerns:
  - Clergy staff;
  - “Work around” process;
  - One department given ability to reverse patient’s decision in HBOC system;
  - Script for staff.

Check: Assess the results

Business Associates Agreement

- Monthly meetings with Legal to review status of BAA;
- BAA includes reference to EPHI (PHI that is either transmitted or maintained in electronic format) if the following is true:
  - Is PHI maintained in electronic form?
  - Is PHI transmitted electronically?

Act: Corrective Actions

What is a Corrective Action Plan?

A corrective plan describes how the issue/problem will be resolved, including the actions to be taken, the time frame, and who will be responsible. A corrective action plan must not be merely a promise to correct, but define a plan to achieve improvement.

Act: Corrective Actions

Education and Training

- Completion of HIPAA training - component of re-credentialing and HIPAA "Read and Sign" made available to delinquent departments;
- Revised current "cumbersome" training database and placed on SIUH intranet;
- As of December 98% compliance. Issues remain with per diem staff/physicians;
- HIPAA update included in mandatory Corporate Compliance Training for 2004;
- Privacy Officer visible, attends staff meetings to clarify concerns of staff.

Act: Corrective Actions

Complaint Process

- Specific education was provided to areas with high complaint/concern rate- Emergency Department in the 3rd quarter and 4th quarter 2003 and Ambulatory services in the 1st quarter 2004;
- Hotline number advertised on posters throughout the hospital and ambulatory sites;
- Ongoing monitoring – results discussed with department managers and quarterly reports were submitted to HIPAA Task Force and Board of Trustees.

Act: Corrective Actions

Notice of Privacy Practices

- Ongoing monitoring of receipt of NPP through Compliance staff audits and Privacy Rounds;
- Posting of NPP- Easel-type display distributed to all points of entry and on patient care units;
- Computer "glitch" repaired;
- Ongoing monitoring – during Privacy Rounds.

Act: Corrective Actions

Privacy Rounds

- Self monitoring implemented in 4th quarter by Managers for inpatient and ambulatory;
- Rounds by Administrator On Duty;
- Use of a standardized tool for reviews;
- Ongoing monitoring by Privacy Officer - continue unannounced rounds. (benefits include accessibility to staff)

STATEN ISLAND
UNIVERSITY
HOSPITAL

HIPAA Privacy Rounds

Unit / Site: **Date:**

Issue	**Y**	**N**	**N/A**	**Comments**
1. Staff is not discussing confidential patient information among themselves in public areas. (Cafeteria, Elevators, Lobby, etc.)				
2. Computer monitors are positioned away from the view of the general public and/or have screen savers in use.				
3. Documents with confidential patient information are face down or concealed, avoiding observation by patients or visitors.				
4. PHI is maintained in (Hot Boxes) outside the patient rooms/exam rooms and stored or filed in Binders provided.				
5. Confidential patient information is not left unattended in a printer, photocopier or fax machine, unless these devices are in a secure area.				
6. Patients lists, including scheduled procedures, with information beyond room assignments are not readily visible by patients or visitors.				
7. Patient Room/Exam Room doors are closed during treatment/consultation with patients.				
8. Staff has knowledge of Privacy Hotline Number. (888-586-2950)				
9. NOP is posted where appropriate- clinics, PAST, CAS, Radiology, etc.				
10. There is documentation in the medical record the patient has received the Notice of Privacy Practice. (Sample 10 current charts.)				

3/2/2004

Act: Corrective Actions

HIPAA - compliant authorization

- Checklist developed as a guide for staff;
- Distributed to departments and posted on the HIPAA intranet site;
- Examples of all authorizations were given to Legal Affairs for review;
- Ongoing monitoring- periodic reviews by HIM staff, Privacy Officer, department managers .

Checklist to validate HIPAA Compliant Authorizations

What must a HIPAA compliant Authorization contain?

- □ The identity of the person or entity to whom the information is to be released;
- □ The scope of the information to be released, i.e.: “laboratory results from June 2003, results of MRI preformed May 22, 2003;
- □ The purpose for which the information is being released (if the release is not requested by the patient);
- □ The signature/date of the patient or his/her legal representative. If the patient or legal representative is not present to show their ID, then the signature must be notarized. If the legal representative is requesting disclosure, proof of legal representation is required;
- □ The expiration date or expiration of the event (none or “end of research study” is sufficient for research related use, research databases or research repositories).
- □ A statement with information regarding the individual’s right to revoke authorization and the limitations on that right i.e.: does not apply to any use or disclosure of PHI prior to the request to revoke authorization. If the authorization is to permit disclosure of PHI to an insurance company, the individual may not have the right to revoke the authorization. Please call the Privacy Officer for guidance. The procedure to revoke authorization; (revocation will become effective on the date that it is received by SIUH).
- □ A statement that the patient does not have to sign the authorization as a condition of receiving treatment at SIUH, except:
  - o If the treatment is research related –provision of treatment may be conditioned on receipt of an authorization to use/disclose PHI related to his treatment as necessary for research; or
  - o If the purpose of the treatment services is to create PHI for disclosure to a third party, provision of the services may be conditioned on receipt of the authorization to disclose PHI to the third party.
- □ A statement of the potential that the information released may be disclosed to unauthorized persons by the recipient and may no longer be protected by the federal privacy rules regarding protected health information.
- □ (A marketing authorization must be used if the purpose of the disclosure is for marketing purposes.)

HIV Information – SIUH will follow New York State guidelines for the release of confidential HIV related information. The SIUH Authorization form has been approved by NYS Department of Health for release of HIV related information. AIDS and HIV related information would only be released upon receipt of an approved NYS Department of Health consent form, which is signed by the patient, legal guardian or by "court order upon application with notice to all parties". You may always fax an SIUH form to the requesting party if there is any question about the validity of the requesting party’s authorization form.

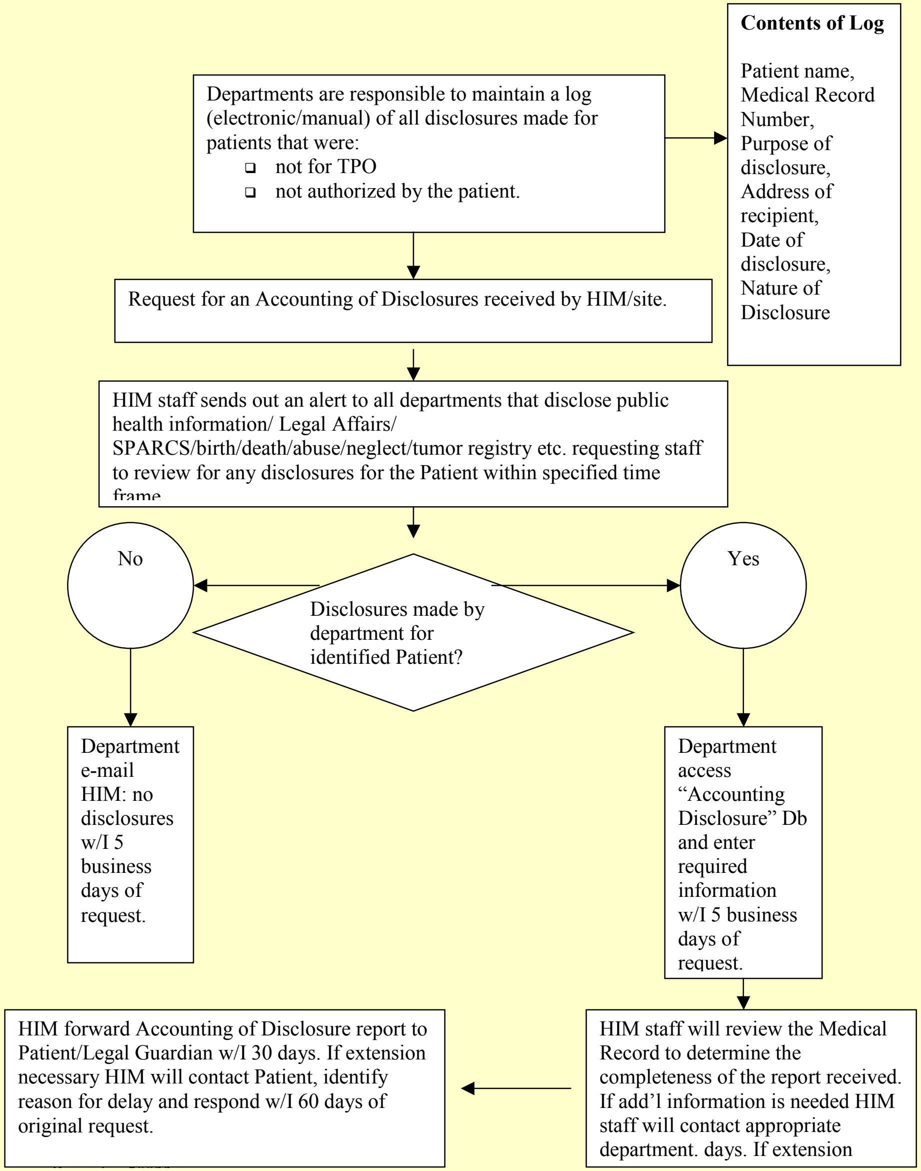
.

Psychiatric/Alcohol/Drugs –requires execution of the NYS mandated authorization form for release of this information.

Act: Corrective Actions

Accounting of Disclosures

- Revision to process;
- Policy with revised flow sheet distributed;
- Re-trained staff on the Accounting of Disclosure requirement, policy revision and their role/responsibility;
- Meetings were held with Accounting of Disclosure Team to review issues/concerns;
- Ongoing monitoring- requests will continue to be sent from Director of Health Information Management- Gatekeeper of the process.



Departments are responsible to maintain a log (electronic/manual) of all disclosures made for patients that were:

- not for TPO
- not authorized by the patient.

Contents of Log

Patient name, Medical Record Number, Purpose of disclosure, Address of recipient, Date of disclosure, Nature of Disclosure

Request for an Accounting of Disclosures received by HIM/site.

HIM staff sends out an alert to all departments that disclose public health information/ Legal Affairs/ SPARCS/birth/death/abuse/neglect/tumor registry etc. requesting staff to review for any disclosures for the Patient within specified time frame

Disclosures made by department for identified Patient?

No

Department e-mail HIM: no disclosures w/I 5 business days of request.

Yes

Department access "Accounting Disclosure" Db and enter required information w/I 5 business days of request.

HIM staff will review the Medical Record to determine the completeness of the report received. If add'l information is needed HIM staff will contact appropriate department. days. If extension

HIM forward Accounting of Disclosure report to Patient/Legal Guardian w/I 30 days. If extension necessary HIM will contact Patient, identify reason for delay and respond w/I 60 days of original request.

Act: Corrective Actions

Opting Out of Directory P/P

- Education provided to registrars, security staff, information desk staff in the 1st quarter 2004;
- Script provided to staff;
- Ongoing monitored through complaints, employee concerns, Privacy Rounds.

Conclusion

- Implement an ongoing process to monitor effectiveness of Privacy Program;
- Utilize standardized tools for monitoring and reporting activities;
- Monitor the effectiveness and workability of your policies and procedures;
- **COMMUNICATION!!!!!!!!!!!!!!**
  - Remain visible and available to staff;
  - Keep staff current on the results of monitoring activities to identify areas for improvement (HIPAA Task Force).
- **What gets Measured gets Managed!**

Questions?