



Monitoring Compliance with HIPAA Privacy

HIPAA Summit VII
Session 1.05
9/15/03

*Patricia Johnston, CHP, FHIMSS
Texas Health Resources
PatriciaJohnston@TexasHealth.Org*

Session Objectives

- Define the purpose of Compliance Monitoring in a Privacy Program
- Identify monitoring targets, metrics and methods
- Present a model for compliance monitoring
- Provide examples of monitoring tools and reports

Basic Assumption for this session: Privacy Program, including policies, procedures and training, is already in place.



Agenda

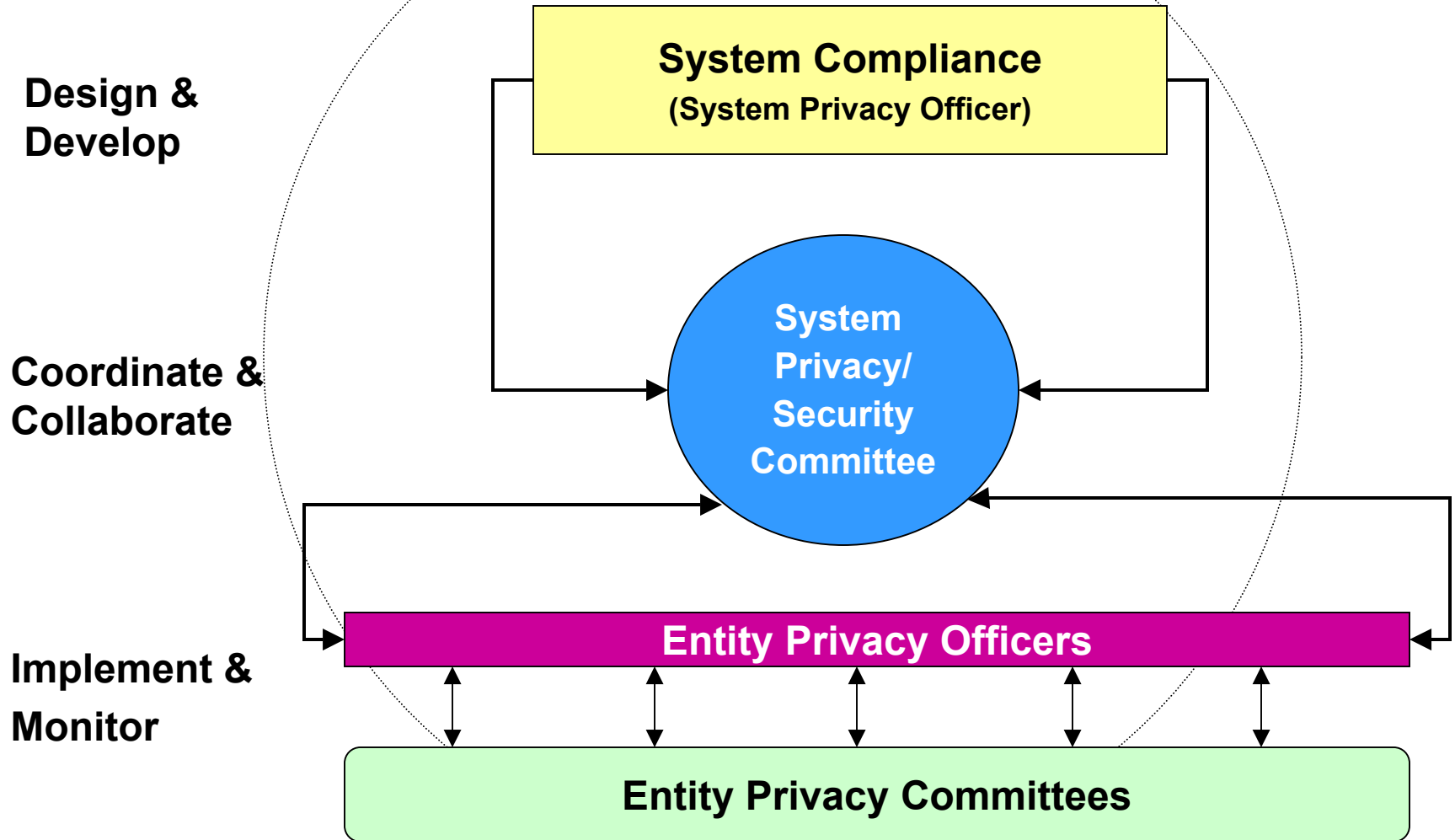
- Why Privacy Compliance Monitoring?
- The Monitoring Process
- A Monitoring Model
- Examples
- Q&A



Texas Health Resources Profile

- one of the largest faith-based, nonprofit health care delivery systems in the United States.
- serves more than 5.4 million people living in 29 counties in north central Texas.
- 13 acute-care hospitals with 2,405 licensed hospital beds, 1 million annual admissions.
- more than 17,000 employees, more than 3,200 physicians with active staff privileges.

Privacy Program Organization

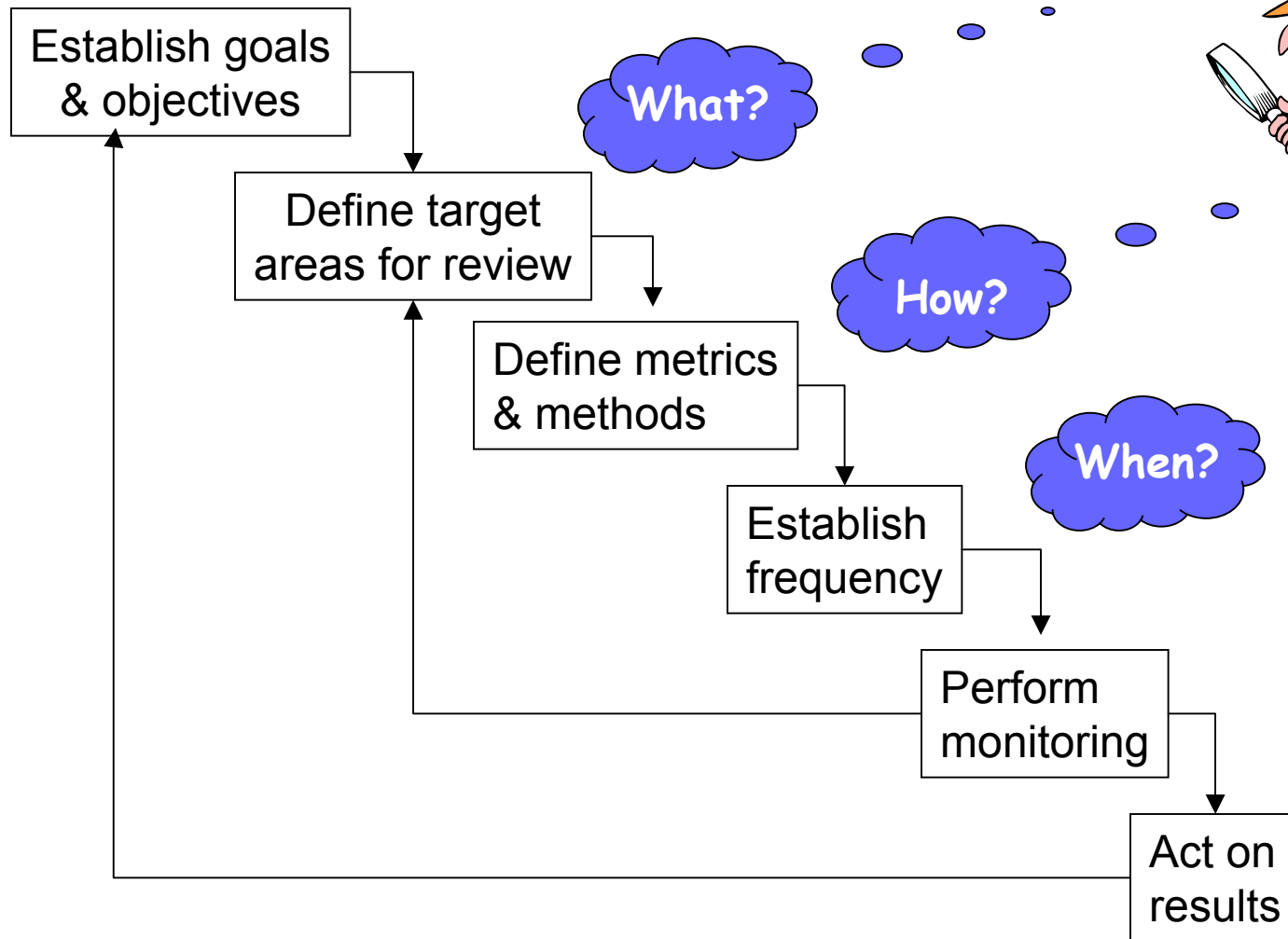




Why Privacy Compliance Monitoring?

- To ensure program goals for confidential protection of health information are achieved.
- To determine if policies, procedures and programs are being followed (protect our investment).
- To minimize consequences of privacy failures through early detection and remediation.
- To provide feedback necessary for privacy program improvement.
- To demonstrate to the workforce and the community at large, organizational commitment to health information privacy.

The Monitoring Process



The Monitoring Process

- Many options for target areas and populations, metrics and methods of measurement.
- Monitoring must be designed to demonstrate the implementation and achievement of the privacy program goals.
- Cost/benefit balance must be achieved.



Degree of Risk

Cost to Monitor



The monitoring process

■ Establish goals and objectives

- Identify monitoring goals based on privacy program objectives, risk assessment, feedback from incident reporting system, and cost/benefit analysis.
- Determine the baseline (risk assessment).
- Identify the desired outcomes (where do we want to be?).

The monitoring process

■ Establish goals and objectives

□ Broad goals

- PHI is secured using appropriate physical and technical security techniques.
- Privacy program will be a differentiator with our customers.

□ Specific goals

- 100% of PC placement is in compliance with workstation guidelines.
- No more than 3 privacy complaints filed per quarter.

The monitoring process

- Define target areas to review (what?)
 - Identify high risk areas
 - If not properly performed, pose a high probability of a breach and/or consequences are of high magnitude (e.g., release of information areas, high profile patients).
 - Identify high volume areas
 - Law of averages says there is potential for problems here (e.g., emergency departments)
 - Identify problem-prone areas
 - Complex functions that are difficult to achieve (e.g., accounting of disclosures).

The monitoring process

- Define target areas to review (what?)
 - Define minimum standards for routine monitoring in order to reinforce compliance (e.g., each department reviewed annually).
 - Determine the ability to readily collect the needed data (may not be feasible or cost-effective to measure).
 - If results for a target area are always good, measure something else.
 - Incident reporting should identify key targets.

The monitoring process

■ Define metrics and methods (how?)

Target	Metric	Method
■ Compliance with Notice Policy	■ Signed Acknowledgment of receipt of Notice	■ Chart audits or computer system documentation
■ Required workforce training	■ % of workforce trained	■ Learning management system reports or class rosters.
■ Providing patients with access to their PHI	■ Number of access requests fulfilled within timeframes	■ Document all requests processed in ROI system; or file request forms and perform periodic sampling.

The monitoring process

- Define metrics and methods (how?)
 - Chart audits (required documentation)
 - Computer system audit reports (access controls)
 - Walkthroughs (observations of compliance)
 - Surveys and interviews (workforce awareness, patient satisfaction)
 - Drills (hypothetical issues presented to staff)
 - “Mystery Shoppers” (try to “break the system”)

The monitoring process

- Establish frequency (when?)
 - Ongoing (high risk areas)
 - Quarterly (past problem areas, new policies and procedures)
 - Annually (departmental reviews)
 - Informally (e.g., workstation placement)
 - Formally (e.g., business associate contracts)
- Perform Monitoring



The Monitoring Process

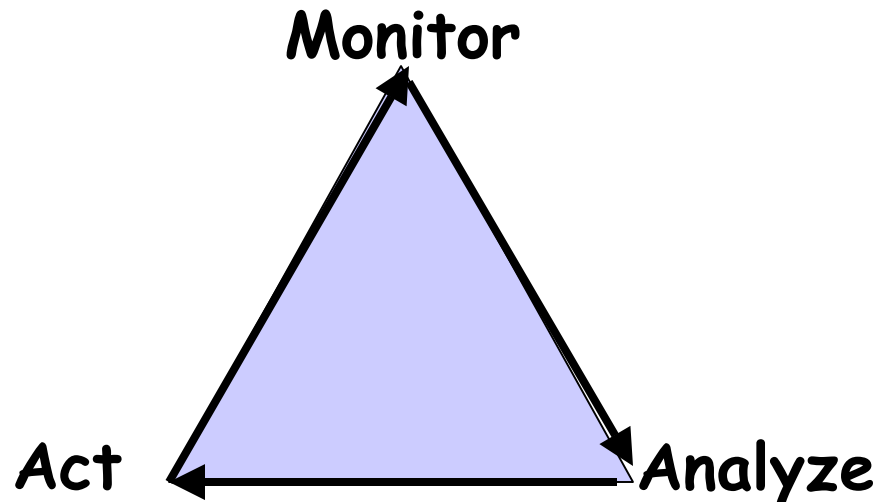
■ Reporting

- Document results
- Compare results to objectives
- Identify non-compliant areas
- Highlight areas for root cause analysis
- Document areas for special attention in future monitoring
- Identify trends



The monitoring process

- Act on results (so what?)
 - If no analysis and action, monitoring is a waste of time
 - If results consistently meet expectations, monitor something else



The monitoring process



- Act on results
- Things that can cause problems include:
 - Unclear policies and procedures
 - Inconsistent (or non-existent) enforcement of policies and procedures
 - Ineffective training
 - Lack of employee motivation



The monitoring process

- Act on results
- Take corrective action
 - Revise policies and procedures
 - Refine or focus training
 - Redesign processes
 - Tighten supervision
 - Modify monitoring program
- Re-monitor for compliance within 2 to 4 weeks after corrective action is taken.
- Continue quarterly monitoring for some period, or flag for future monitoring reviews.

A Monitoring Model



Policies

Training

Safeguards

What
Monitoring goals
& targets

How
Metrics &
Methods

When
Frequency

What
Compliance
With P&P

How
Chart audits
Observation
Surveys

When
Variable

What
All workforce
trained

How
Training
Reports

When
Monthly

What
Implemented
Safeguards

How
Walkthrough

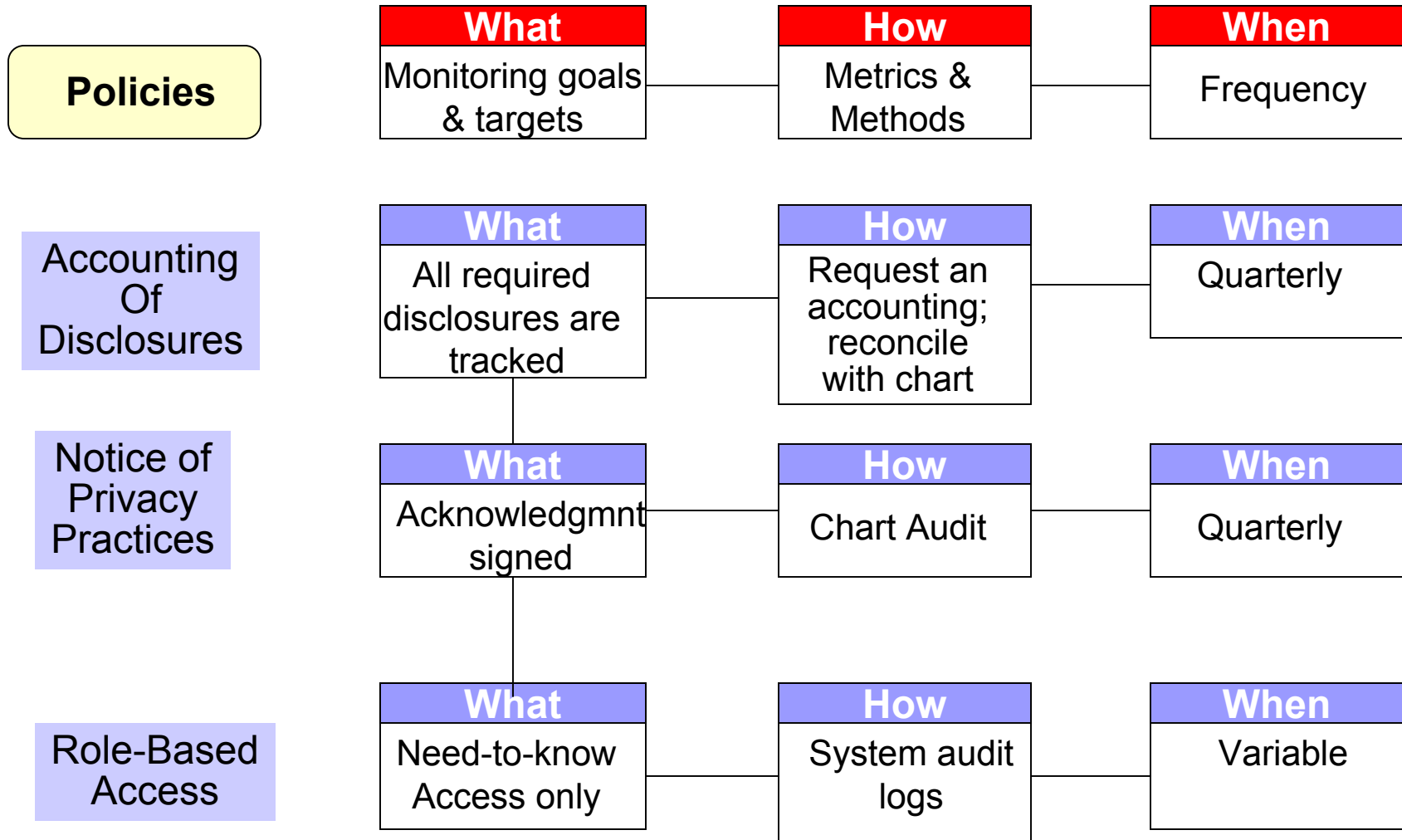
When
Quarterly
Annually



A Monitoring Model

- Compliance with Policies
 - Monitoring the organization's compliance with its own policies, not whether or not the policies are compliant with the Privacy Rule.

A Monitoring Model



Monitoring Model

- Role-based access

- Utilize information system audit capabilities.

- Determine criteria for audit:

- Random

- By patient

- By staff role

- Sensitivity of data

- High-profile patients

- All new employees during first 60 days



Monitoring Model



■ Role-based access

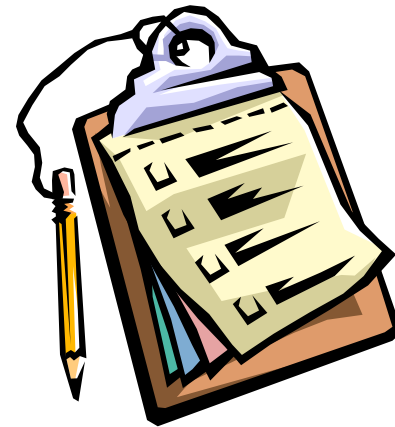
- Requires maximization of system auditing capabilities.
- Consider the vulnerabilities of the system when deciding how stringent controls should be.
- Must determine audit log retention needs.
- Assignment of responsibility is key.

Monitoring Model - Training

- Documentation of training of workforce as of April 14, 2003
- Training of new employees
 - Within pre-defined timeframe
- Training of students, volunteers, medical staff
- Training of contractors
- Average training scores
- Refresher training
 - In response to privacy incidents
 - In response to results of monitoring
 - In response to new policies or procedures
- Document, track and report

Monitoring Model - Safeguards

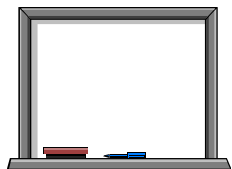
- Monitor by “walking around”
- Develop checklists
- Formal, informal
- Track number of observances of non-compliance
- Reward good practices



Monitoring Model - Safeguards

■ Areas to review

- PHI in trash or unsecured recycle bins
- Workstations not logged off or securely positioned
- Discussion of confidential information among staff in public areas
- PHI in open view in hallways, on desks
- PHI left on faxes, printers
- PHI on whiteboards
- Doors propped open
- Sharing passwords
- Dictation conducted in public areas
- Business visitors not badged or signed in





Monitoring Model – Business Associates


- Monitor compliance from two aspects
 - Have you identified all of your business associates?
 - Do you have required contract terms with your business associates?
- Ongoing challenge for most organizations
 - Periodic sampling of invoices
 - Reports from contract management systems
 - Periodic departmental surveys
 - Random sampling of contracts

Monitoring Model - Documentation

- Ensure that required documentation is in place:
 - Authorizations, court orders, subpoenas, satisfactory assurances
 - Requests and responses for access, amendment and restrictions
 - Documentation of disclosures available for accounting
 - Accounting requests and responses

Monitoring Model - Documentation

- Ensure that required documentation is in place:
 - Complaints and resolutions
 - Privacy incident investigations
 - Marketing and fundraising opt-out requests
 - Minimum necessary protocols
 - Current and past Notice of Privacy Practices
 - Training records
 - Policies and procedures



Monitoring Model - Documentation

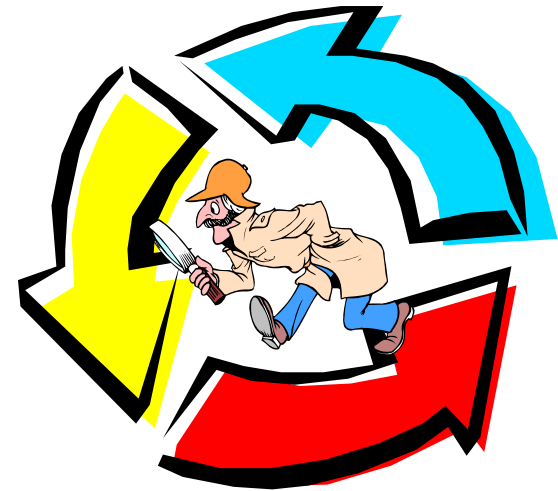
- Ensure that required documentation is in place:
 - Patient acknowledgement of receipt of Notice
 - Designation of affiliated covered entity
 - Business Associate contracts
 - Data Use agreements
 - Research waiver requests and approvals
 - Definition of designated record sets

Monitoring Model - Documentation

- Ensure that required documentation is in place:
 - Title/Office of:
 - person responding to access and amendment requests
 - person responding to complaints
 - privacy official

Key Steps - Summary

- Identify targets for monitoring, based on program objectives, risk assessment, feedback from incident reporting system, cost/benefit analysis
- Establish metrics and methods
- Create baseline and performance goals
- Design tools
- Conduct monitoring
- Report results
- Analyze results
- Take corrective action
- Monitor again



Examples

Monitoring Plan



Walkthrough Checklist



Survey



Documentation Audit

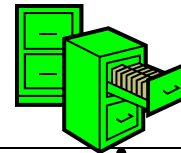


Chart Audit



Training and Incident Reports



Drills and Mystery Shoppers

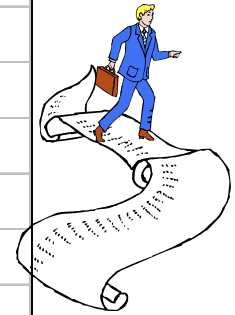


Compliance Monitoring Plan

#	Metric	How Measured	Frequency	Performance Goal	Comments
1	Number of substantiated breaches	Information Privacy Reports	Quarterly	look at trend to go down.	THR Compliance will provide quarterly reports to the entities, based on their incident reports.
2	Response to Patient Complaints: numbers of days between filing and response.	Information Privacy Reports	Quarterly	look for minimum response time	THR Compliance will provide quarterly reports to the entities, based on their incident reports.
3	Training Timeliness	% new hires trained within 30 days	Quarterly		Entity Privacy Officers will run reports to determine new employees needing to complete training.
4	Observed compliance with P&P's				
4a		Walkthroughs	Every two weeks to a month; all departments surveyed at least once a year		See worksheet; 12-month schedule developed by EPOs
4b		Chart Audits	Compliance will audit for presence of acknowledgement of Notice and filled out authorization for verbal release during their quarterly audits	Provide feedback to Admissions OPIC	Acknowledgement of receipt of Notice; filled out authorization for verbal release; flagged charts for restrictions or no information patients
4c			Privacy Officers will audit five No Information patient charts a month	Monthly	
5	Accounting of Disclosures	Select a patient for an accounting, and then compare report to chart for completeness	Quarterly		



#	Activity	Observed (Y/N)	# of occurrences	Comments
1	Confidential information is discussed by staff in public areas.			
2	Conversations with patient/family regarding confidential information are held in public areas.			
3	Overhead and intercom announcements include confidential information.			
4	Phone conversations and dictation are in areas where confidential information can be overheard.			
5	Computer monitors are positioned to be observed by visitors in public areas.			
6	Unattended computers are not logged out or protected with password-enabled screen savers.			
7	Computer passwords are shared or posted for unauthorized access.			
8	Documents, films and other media with confidential patient information are not concealed from public view.			
9	Whiteboards in public areas have more than the allowable information.			
10	Medical records are not stored or filed in such a way as to avoid observation by passersby.			
11	Confidential patient information is called out in the waiting room.			
12	Confidential information is left on an unattended fax machine in unsecured areas.			
13	Confidential information is left on an unattended printer in unsecured areas.			
14	Confidential information is left on an unattended copier in unsecured areas.			
15	Confidential information is found in trash, recycle bins, or unsecured pre-shredding receptacles.			
16	Patient lists, such as scheduled procedures, are readily visible by patients or visitors.			
17	Contractors, vendors and other non-patient visitor third parties not appropriately identified.			
18	Staff are not wearing name badges.			
19	Patient records not filed in locking storage cabinets or rooms that are locked when unattended.			
20	Security access mechanisms for buildings or departments are bypassed.			
21	When questioned, staff demonstrate lack of privacy awareness.			



Walkthrough Checklist

Surveys - Examples



Employee Awareness

- I know what a privacy breach is.
- I know how to report a privacy breach.
- I can locate our privacy policies.
- I understand how to protect health information on my computer.
- I understand when I need a patient authorization to release information.
- I know what patient information is allowable to use for fundraising.
- I understand patient's privacy rights.

Don't Agree

Completely Agree

1 (2) 3 4 5 →

1 2 (3) 4 5 →

1 2 (3) 4 5 →

1 2 3 (4) 5 →

1 (2) 3 4 5 →

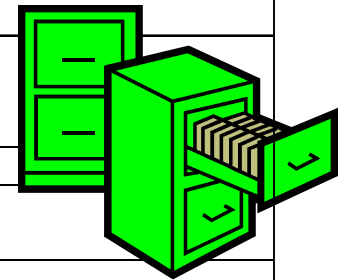
1 2 3 4 (5) →

1 2 (3) 4 5 →

Patient Satisfaction

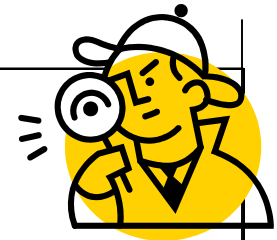
- I am confident my health information is treated confidentially by [hospital name].
- I am aware of how the hospital uses my health information.
- I understand my rights regarding my health information.
- I know how to register a complaint concerning confidential treatment of my health information.
- I am satisfied with the protection of my health information.

Requirement	Location	Compliant Y or N
Requests and responses for access	Correspondence section of chart	
Requests and responses for amendments	Medical record	
Accounting of Disclosures	Correspondence section of chart; disclosure tracking system.	
Complaints and resolutions	Privacy officer files	
Fundraising: authorizations, opt-out requests	Foundation department files	
Marketing: authorizations and opt-out requests	Marketing department system	
Minimum Necessary protocols	IntraNet	
Current and past versions of Privacy Notice	Privacy Officer files and hospital website on Internet	
Restriction requests and response	Medical Record	
Sanctions	Employee records	
Designation of SACE	System Privacy Officer files	
Business Associate contracts	Legal Department, Supply Chain Management	
Research Waiver requests and approvals	IRB files	
Designated Record Sets	Privacy officer files	
Titles and Offices	Privacy Officer files	
Training Records	Learning Management System; employee files	
Confidentiality agreements	Employee files; vendor and agency files	



Documentation Audit

Chart Audit



Entity/ cases audited	Privacy notice not initialed	ROI form incomplete	Notes
# 1/49	0	0	1 patient was unable to sign due to condition
# 2 /38	5	1	Admit document was not witnessed or dated, 1 case contained no forms to audit
# 3/24	1	2	
# 4/50*	4	5	29 cases were for < 4/14/03 date of service
# 5/27	11	12	1 patient left AMA, no paperwork to audit
# 6/24	1	11	1 case without admission paperwork completed
# 7/47	3	9	Admit document was not witnessed or dated. 10 cases where Admission acknowledgments were incomplete.
# 8/50	1	3	2 cases admit notes state patient is unable to sign admission documents, discharge condition described as awake and alert.
# 9/50	1	6	1 case, the patient refused to sign, 2 cases, signatures were incomplete.
# 10/46	1	0	
# 11/43	0	0	
# 12/50*	5	6	5 cases with admission paperwork incomplete. 4 cases were for < 4/14/03 date of service.
Total/498	33	55	

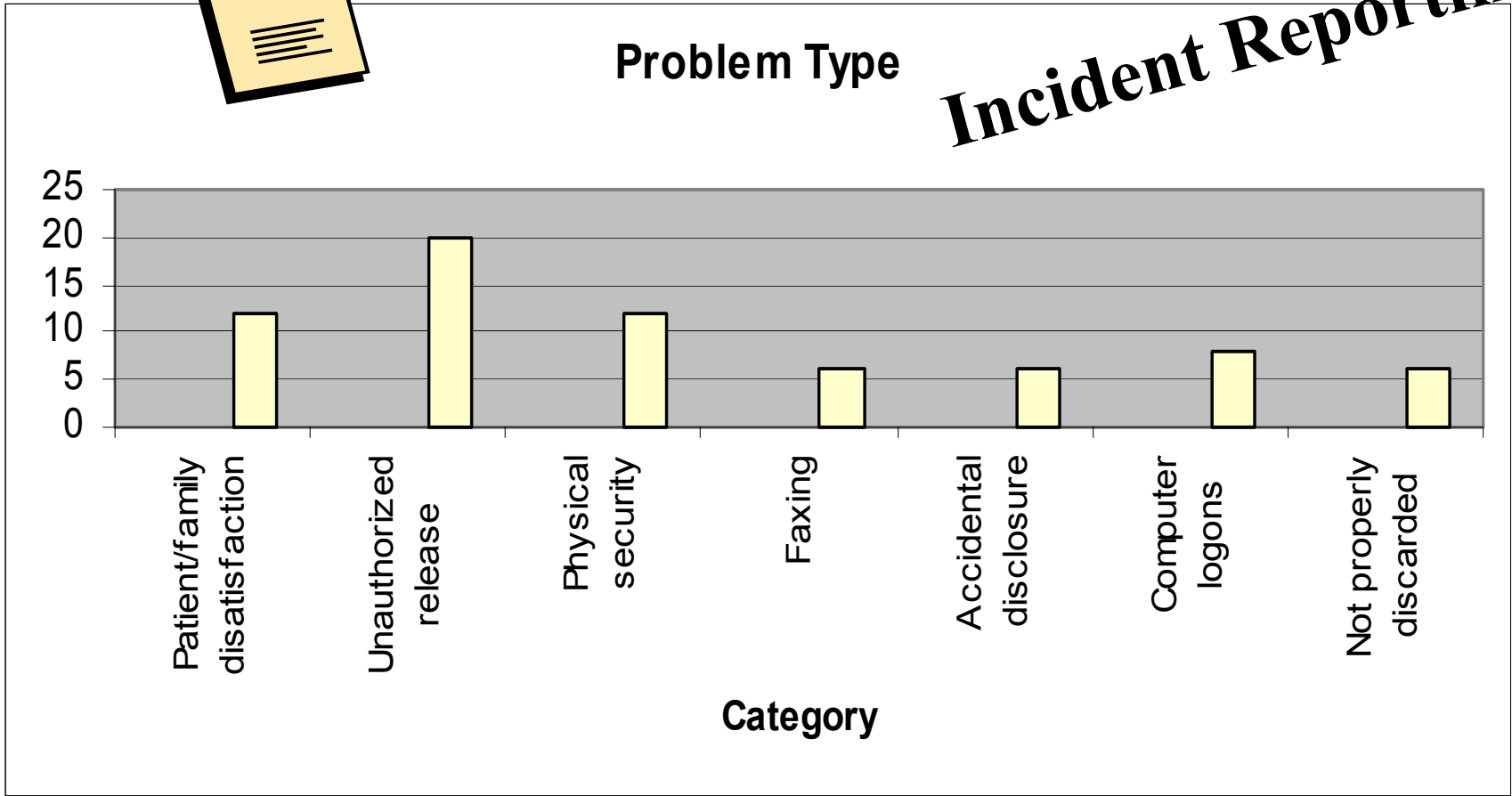
Cost Center Name	Total Employees	Total Completed	% Compliant
160100 - Nursing Admin.	70	68	97%
160130 - Station 13-Pediatric	22	22	100%
160140 - Med. Surg. Admin.	2	2	100%
160230 - Station 23-LDRPN	69	68	99%
160310 - Station 31-Telemetry	50	48	96%
160320 - Station 32-Oncology	43	40	93%
160330 - Station 33-Postpartm	49	48	98%
160420 - Station 42-Medical	42	42	100%
160430 - Womens Services	27	26	96%
160520 - Station 52-Ortho/Neu	45	45	100%
160910 - NICU	68	68	100%
161210 - Intensive Care	51	51	100%
161400 - Cardiac Care	51	50	98%
162110 - Inpatient Surgery	115	110	96%
162150 - Cardiac Cath. Lab	19	19	100%
162180 - Post Anesthesia Care	52	50	96%
162300 - Emergency Services	100	98	98%
162500 - Central Supply	21	19	91%
170100 - Laboratory	97	86	89%
170400 - Radiology	66	63	96%
170410 - Special Procedures	4	4	100%
170420 - CT	11	11	100%
170440 - Ultrasound	8	8	100%

Training Completion





Incident Reporting



Drills and Mystery Shoppers

Drills

- Ask staff how they respond to amendment requests.
- How does an incident get reported?
- What documentation is required with a subpoena?
- What identifiers need removal to de-identify PHI?

Mystery Shopper

- Request information over the phone.
- Start reviewing medical charts.
- Ask for a password.
- Pretend to be a family member with a privacy complaint.
- Access “secured” areas.



Questions & Answers

Patricia is Director of Health Information Privacy/Security for Texas Health Resources (THR) in Arlington, Texas. She is responsible for the development and management of THR's HIPAA Program Management Office, as well as serving as THR's System Privacy Officer. Her background and work experience is focused exclusively on health care, including a variety of management positions in Information Technology and clinical laboratory science. Patricia has published a variety of articles and conducted seminars related to healthcare computing as well as HIPAA compliance for the healthcare provider. She holds a certification in Healthcare Privacy. She is a fellow of the Healthcare Information and Management Systems Society, as well as a member of the American College of Healthcare Executives and the International Association of Privacy Officers. Patricia received her Masters Degree in Information Management from University of Texas at Dallas, and her Bachelor's Degree in Medical Technology from University of North Texas.