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

System Compliance
(System Privacy Officer)

System Privacy/Security Committee

Entity Privacy Officers

Entity Privacy Committees
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

- Establish goals & objectives
- Define target areas for review
- Define metrics & methods
- Establish frequency
- Perform monitoring
- Act on results

What?
How?
When?
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.
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?)

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

**What**
- Monitoring goals & targets
- Compliance With P&P
- All workforce trained
- Implemented Safeguards

**How**
- Metrics & Methods
- Chart audits Observation Surveys
- Training Reports
- Walkthrough

**When**
- Frequency
- Variable
- Monthly
- 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

**Policies**

**What**
Monitoring goals & targets

**How**
Metrics & Methods

**When**
Frequency

**Accounting Of Disclosures**

**What**
All required disclosures are tracked

**How**
Request an accounting; reconcile with chart

**When**
Quarterly

**Notice of Privacy Practices**

**What**
Acknowledgment signed

**How**
Chart Audit

**When**
Quarterly

**Role-Based Access**

**What**
Need-to-know Access only

**How**
System audit logs

**When**
Variable
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

<table>
<thead>
<tr>
<th>Monitoring Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Walkthrough Checklist</td>
</tr>
<tr>
<td>Survey</td>
</tr>
<tr>
<td>Documentation Audit</td>
</tr>
<tr>
<td>Chart Audit</td>
</tr>
<tr>
<td>Training and Incident Reports</td>
</tr>
<tr>
<td>Drills and Mystery Shoppers</td>
</tr>
<tr>
<td>#</td>
</tr>
<tr>
<td>----</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>4b</td>
</tr>
<tr>
<td>4c</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>#</td>
</tr>
<tr>
<td>----</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>18</td>
</tr>
<tr>
<td>19</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td>21</td>
</tr>
</tbody>
</table>
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.

**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.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Location</th>
<th>Compliant Y or N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests and responses for access</td>
<td>Correspondence section of chart</td>
<td></td>
</tr>
<tr>
<td>Requests and responses for amendments</td>
<td>Medical record</td>
<td></td>
</tr>
<tr>
<td>Accounting of Disclosures</td>
<td>Correspondence section of chart; disclosure tracking system.</td>
<td></td>
</tr>
<tr>
<td>Complaints and resolutions</td>
<td>Privacy officer files</td>
<td></td>
</tr>
<tr>
<td>Fundraising: authorizations, opt-out requests</td>
<td>Foundation department files</td>
<td></td>
</tr>
<tr>
<td>Marketing: authorizations and opt-out requests</td>
<td>Marketing department system</td>
<td></td>
</tr>
<tr>
<td>Minimum Necessary protocols</td>
<td>IntraNet</td>
<td></td>
</tr>
<tr>
<td>Current and past versions of Privacy Notice</td>
<td>Privacy Officer files and hospital website on Internet</td>
<td></td>
</tr>
<tr>
<td>Restriction requests and response</td>
<td>Medical Record</td>
<td></td>
</tr>
<tr>
<td>Sanctions</td>
<td>Employee records</td>
<td></td>
</tr>
<tr>
<td>Designation of SACE</td>
<td>System Privacy Officer files</td>
<td></td>
</tr>
<tr>
<td>Business Associate contracts</td>
<td>Legal Department, Supply Chain Management</td>
<td></td>
</tr>
<tr>
<td>Research Waiver requests and approvals</td>
<td>IRB files</td>
<td></td>
</tr>
<tr>
<td>Designated Record Sets</td>
<td>Privacy officer files</td>
<td></td>
</tr>
<tr>
<td>Titles and Offices</td>
<td>Privacy Officer files</td>
<td></td>
</tr>
<tr>
<td>Training Records</td>
<td>Learning Management System; employee files</td>
<td></td>
</tr>
<tr>
<td>Confidentiality agreements</td>
<td>Employee files; vendor and agency files</td>
<td></td>
</tr>
<tr>
<td>Entity/cases audited</td>
<td>Privacy notice not initialed</td>
<td>ROI form incomplete</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td># 1/49</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td># 2/38</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td># 3/24</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td># 4/50*</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td># 5/27</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td># 6/24</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td># 7/47</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td># 8/50</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td># 9/50</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td># 10/46</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td># 11/43</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td># 12/50*</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Total/498</td>
<td>33</td>
<td>55</td>
</tr>
<tr>
<td>Cost Center Name</td>
<td>Total Employees</td>
<td>Total Completed</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>160100 - Nursing Admin.</td>
<td>70</td>
<td>68</td>
</tr>
<tr>
<td>160130 - Station 13-Pediatric</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>160140 - Med. Surg. Admin.</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>160230 - Station 23-LDRPN</td>
<td>69</td>
<td>68</td>
</tr>
<tr>
<td>160310 - Station 31-Telemetry</td>
<td>50</td>
<td>48</td>
</tr>
<tr>
<td>160320 - Station 32-Oncology</td>
<td>43</td>
<td>40</td>
</tr>
<tr>
<td>160330 - Station 33-Postpartm</td>
<td>49</td>
<td>48</td>
</tr>
<tr>
<td>160420 - Station 42-Medical</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>160430 - Womens Services</td>
<td>27</td>
<td>26</td>
</tr>
<tr>
<td>160520 - Station 52-Ortho/Neu</td>
<td>45</td>
<td>45</td>
</tr>
<tr>
<td>160910 - NICU</td>
<td>68</td>
<td>68</td>
</tr>
<tr>
<td>161210 - Intensive Care</td>
<td>51</td>
<td>51</td>
</tr>
<tr>
<td>161400 - Cardiac Care</td>
<td>5</td>
<td>50</td>
</tr>
<tr>
<td>162110 - Inpatient Surgery</td>
<td>115</td>
<td>110</td>
</tr>
<tr>
<td>162150 - Cardiac Cath. Lab</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>162180 - Post Anesthesia Care</td>
<td>52</td>
<td>50</td>
</tr>
<tr>
<td>162300 - Emergency Services</td>
<td>100</td>
<td>98</td>
</tr>
<tr>
<td>162500 - Central Supply</td>
<td>21</td>
<td>19</td>
</tr>
<tr>
<td>170100 - Laboratory</td>
<td>97</td>
<td>86</td>
</tr>
<tr>
<td>170400 - Radiology</td>
<td>66</td>
<td>63</td>
</tr>
<tr>
<td>170410 - Special Procedures</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>170420 - CT</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>170440 - Ultrasound</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>
Problem Type

Patient/family dissatisfaction
Unauthorized release
Physical security
Faxing
Accidental disclosure
Computer logons
Not properly discarded

Category
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.
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.