PRIVACY AND SECURITY PROGRAM AUDIT AND MONITORING

HEALTH CARE COMPLIANCE ASSOCIATION
COMPLIANCE INSTITUTE
Kenneth Hopkins, Director, Internal Audit & Privacy Officer
April 24, 2007

✓ Compare Auditing vs. Monitoring
✓ Overview of key privacy and security program provisions
✓ How to audit the privacy and security programs for compliance and improvement
✓ How operating departments can monitor the program
✓ Practical tips to implement an effective audit and monitoring program
**Auditing**

A systematic and structured approach

- Formal review (performed by an individual(s) independent of the department);
- Includes planning, risk identification, assessing internal controls, sampling of data, testing of processes, validating information; and
- Formal communication of recommendations and corrective action to management and the Board.

---

**Monitoring**

A process involving ongoing “checking” and “measuring” to ensure quality control

- The process is less structured than auditing; and
- typically is performed by departmental staff
  - Operational managers or the privacy officer
- Daily, weekly, or other periodic spot checks to verify that essential functions are being adequately performed and that processes are working effectively.
- May identify the need for a more detailed audit
PRIVACY PROGRAM
PRIVACY OFFICIAL
NOTICE OF PRIVACY PRACTICES
POLICY AND PROCEDURES
PATIENT PRIVACY RIGHTS
TRAINING
COMPLAINTS

ACCESS
CHANGE
ACCOUNTING
CONFIDENTIAL COMMUNICATION
RESTRICT
Auditing – audit more visible areas and higher risk; high volume or problem prone
- Notice and acknowledgment
- Faxing of PHI
- Training
- Disposal of PHI
- Complaints

Auditig Process
- Plan & understand the process
- Risk assessment
- Internal controls
- Audit steps - test and documentation
- Audit report and recommendations
- Corrective actions
Most visible HIPAA requirement!

Planning
- Provide notice at time of service
- Tracking notice in the computer
- Signed acknowledgment – chart
- Notice Posters – service locations
- Notice posted on web-site

Risk Assessment
- Complaints - Office of Civil Rights (OCR)
- Potential fines and penalties - $100 per violation up to $25,000 per standard annually
- Potential OCR investigation
- Potential damage to hospital reputation
Internal Controls
• Notice tracking process
• Acknowledgement signed by patient
• Policy and Procedures
• Training staff

Audit steps -
• Review notice tracking reports by service
• Review sample of patient charts
• Determine compliance percentage
• Walkthrough – for posters
• Review web-site for posted notice
• Document exceptions
Audit report
Prepare audit report with findings and conclusions (what needs improvement?)
- recommendations
- corrective actions
- follow-up

Requirements
- Cover sheet (important warning)
- Procedures
  - cover sheets at all fax machines?
  - double check fax numbers?
  - complaints related to faxing?
  - misdirected faxes?
  - walk-through
Findings
- PHI left on fax machines
- Patient complaints
Corrective actions
- HIPAA e-mail
- Training focus
- Discipline employee

Key to effectiveness!
List of all new workforce members (1 year)
- Understand the processes and content
  - orientation and web based course
- Sample – higher risk areas
- 100% audit of training
- HealthStream reports
- Physician credentialing
Results
- Identify delinquent staff
- 2\textsuperscript{nd} chance to complete
- Manager accountability
- Alternate training methods
- Corrective action

List of all confidentiality bins
- Understanding the process
- Check copy machines for PHI
- Check waste baskets for PHI
- Audit vendor facilities
- Identify problem areas
- Mitigate
- Corrective action
List of all complaints during the past year (identify that procedures are effective)

• Review the complaint log and issues
• Review the investigations
• How was each resolved? timely?
• Summarize by types of issues
• Mitigate – improve processes
• Corrective action taken

Review OCR national data base statistics on complaints (Top 5: 11,280 complaints)

• Impermissible disclosures (gossiping)
• Lack of adequate safeguards (leave files out)
• Failure to provide access to records
• Disclosure of more than minimum necessary
• Failure to include valid language in authorizations
Results -
• 24% - Impermissible disclosures
• 52% - Lack of adequate safeguards or following established procedures
• Recommendations/trends
  - consistent discipline, follow procedures
  - training, training, training
  - HIPAA h-mail (reminders)

Monitoring
• Notice and acknowledgement - registration
• Disposal of PHI - department
• Faxing of PHI - department
• Accounting of disclosures - department
MONITORING PROCESS

• Determine what to monitor
• Buy-in from department managers
• Periodic spot checking
• Identify problem areas or compliance
• Communicate Issues
• Corrective actions
• Follow-up

MONITORING NOTICE

• Registration manager reviews notice report daily for compliance
• Review a few charts for patient sign-off
• Observe registration process periodically
• How are exceptions being handled?
• Reinforce importance with staff
• Communicate issues - staff & Privacy Officer
MONITORING DISPOSAL OF PHI

Areas with significant PHI access
- Confidential shredding bins (locked)
- Shredder (if available)
- Paper, computer medium such as CDs, plastic, etc.
- Walkthrough:
  - Check copy machines for PHI
  - Waste baskets for PHI

MONITORING FAXING OF PHI

Areas – high volume faxing
Sending faxes that contain PHI
- Use of approved cover sheet
- 5 point fax checklist
- Reasonable steps
- Misdirected faxes
- PHI left on fax machines
### Accounting of Disclosures Must Contain

- Date, Name and, if known, address:
- Description of the PHI disclosed; and
- Purpose of disclosure
- 6 year period
- Centralized software such as – Disclosure Trac

---

- Print Disclosure Trac report for the period
- By disclosure reason (user)
- Print out a sample of detail (25 patients)
- Review any requests for AOD
Definition:
Formal information security program with administrative, physical facility and technical safeguards; policies and procedures; and processes to manage security.

Covers – all electronic patient health information
<table>
<thead>
<tr>
<th><strong>SAFEGUARDS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Administrative</td>
</tr>
<tr>
<td>• Physical facilities</td>
</tr>
<tr>
<td>• Technical</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SECURITY PROGRAM AUDITING</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security management</td>
</tr>
<tr>
<td>• Security Walkthrough - new facilities</td>
</tr>
<tr>
<td>• Training and reminders</td>
</tr>
<tr>
<td>• Incidents</td>
</tr>
<tr>
<td>• Evaluation</td>
</tr>
<tr>
<td>• Security rounds</td>
</tr>
</tbody>
</table>
## Auditing Security Management

- Select all new hires for review
- Obtain security access authorizations
- Review for appropriate access for job
- Termination of access (timely)
- High risk areas
  - data center employees
  - disgruntled employees (high risk)

### New facilities:

- Perform a physical security walk-through
- Document controls and safeguards
- Card key access
- Data center
- Exits not closing
- Workstation locations
- Laptops
• Combined privacy & security training
  Same audit as privacy
Differences:
• Awareness of risks – training content
  - passwords and malicious software
• Periodic reminders – (HIPAA e-mail)

• Security log maintained – all incidents
• Identify top 5 issues/trends
• Documentation
• Inappropriate access to computer PHI
• Audit trail (permanent record on CD)
  - What patients has a user accessed?
• Sanctions – suspension, termination
Changes and new facilities

- Ongoing evaluation and audit
- New computer applications
- New physical facilities
- New technical safeguards
- New risks (Wireless, camera phone, PDA)
- Document actions to reduce risk

Use the work of security staff

- Open doors
- Theft of computers
- Surveillance cameras – proactive
- Card key access reports
- ID Badges
- Opening doors for staff
- Termination of facility access
Computer access
Laptop security
Physical security
Security officer walk-through
Workstations
Card key access reports
Password management

Discourage unauthorized viewing of PHI
- Computer access based upon job
- Use of audit trail (CD permanent storage)
- High Profile patients (VIP, celebrities)
- New hires within 60 days
- High risk departments
- Random selection of users
Obtain inventory of laptops and locations
- Walkthrough locations
- Locking cables in use
- Check for PHI stored on the hard drive
- CDs or diskettes with PHI secured
- Are laptops taken home?

Walkthrough areas where PHI is stored after regular hours and week ends
- Are doors secured by loading docks?
- Data center access – card key access reports
- Sensitive areas (i.e. PHI or computers)
### MONITORING – WALK-THROUGH

- Observe do employees wear ID badges?
- Workstations logged on unattended
- Doors locked appropriately
- Workstation with password labeled
- Wireless personal computer carts
- Compare employee behavior to policies
- Weekends and off hours

### MONITORING WORKSTATIONS

- Screens pointed away from public
- Screen savers in use
- Check for anyone logged on and not present
- Any passwords attached to keyboard
### MONITORING CARD KEY ACCESS

Obtain list of those with access to sensitive areas and card key access reports:

- Data Center
- Medical Records/coding
- Operating Room
- Billing
- MIS

### MONITORING PASSWORD MANAGEMENT

Review password do’s and don’ts:

- Policy on passwords
- Expiration period
- Request report of passwords used
- Review logs of failed log–on attempts
- Help desk – resetting passwords
Disclaimer

The information contained herein has been obtained from sources believed to be reliable. The author and Jefferson Regional Medical Center disclaims all warranties as to the accuracy, completeness or adequacy of such information and and shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations hereof. The reader assumes the sole responsibility for the selection of these materials to achieve the intended result. The opinions expressed herein and by the presenter are subject to change without notice and are not necessarily the opinions of Jefferson Regional Medical Center.

PRIVACY AND SECURITY
PROGRAM AUDIT AND MONITORING

Questions and Answers

Kenneth Hopkins, Director, Internal Audit & Privacy Officer, CPA, CIA, CISA, CHC
Kenneth.hopkins@jeffersonregional.com