Compliance Monitoring of the HIPAA Privacy Rule

National Medicaid Conference

_experience the commitment

CGI

Art Leyland
Senior Manager
CGI Information Systems and Management Consultants, Inc.
February 11, 2003

Session Objectives

- To define Privacy Rule compliance monitoring
- To discuss roles and responsibilities
- To outline how to conduct the monitoring
- To provide compliance monitoring examples in some key areas

Assumptions For Session

- Focus on one agency: A hypothetical state Medicaid Agency
- Policies and procedures are in place
- Approach can be used both pre/post April 14, 2003
- A formal internal audit function exists for the agency

Key Steps

- Determine scope of monitoring
- Set frequency of monitoring
- Assign monitoring responsibility
- Design monitoring tools
- Conduct monitoring
- Prepare monitoring report
- Perform root cause analysis on problems
- Take corrective action
- Monitor again for compliance

Determine Scope of Monitoring

- Conducting periodic review of the agency's compliance with its HIPAA policies and procedures
- Not a review of whether policies and procedures are compliant (Should be a separate process, if needed.)

Frequency of Monitoring

- Compliance with all policies and procedures should be monitored periodically (e.g., annually)
- Some areas could be monitored more frequently
  - High risk areas
  - Past problem areas
  - New policies and procedures
  - Ease of monitoring

Assign Monitoring Responsibilities

- Agency Internal Audit Department
- Agency HIPAA Privacy Official
- Agency Department supervisors
- Ideal: shared responsibilities

If Responsibilities Are Shared

- Training of auditors will be required
- Clear lines of responsibility should be drawn to avoid duplication
- Internal audit should review work of other monitors

Shared Responsibilities Example

Monitoring of employee conversations with beneficiaries/others

- Verifying identity?
- Only permissible disclosures?
- Providing only minimum necessary PHI?

Shared Responsibilities Example

- Supervisors monitor phones for compliance with policies and procedures
- Supervisors prepare individual reports on results
- Privacy Official compiles reports and looks for trends and root causes of any problems
- Internal audit ensures that supervisors and Privacy Officer are doing monitoring

Design Monitoring Tools

Types of tools needed

- Audit process and procedures
- Forms

Conduct Monitoring

- Some monitoring should be ongoing (e.g., monitoring of phone conversations)
- Some monitoring should be done quarterly (e.g., high risk areas)
- Some monitoring should be done annually (e.g, infrequent occurrences)
- Some monitoring should be informal (e.g., shredding monitoring)
- Some monitoring should be formal (e.g., business associate contracts)

If Internal Audit Is Responsible

More likely to be formal process

- Audit announcement
- Entrance conference
- Preliminary investigation
- Fieldwork
- Audit work review
- Draft audit report
- Final audit report issued
- Follow-up audits

Prepare Monitoring Report

- Purposes of report
  - Document compliance
  - Identify non-compliant areas
  - Highlight areas for root cause analysis
  - Document areas for special attention in future monitoring
- Agency audiences for report: Supervisors, HIPAA Privacy Official, Internal Audit, Agency Senior Management

Perform Root Cause Analysis

Some things that can cause problems:

- Unclear policies and procedures
- Uneven enforcement of policies/procedures
- Ineffective training
- Employee motivation

Take Corrective Action

Corrective actions could include:

- Revising policies/procedures
- Requiring tighter supervision
- Retraining employees
- Remotivating employees

Remonitor For Compliance

- Within reasonable time after corrective action taken (e.g., 2-4 weeks)
- Special monitoring schedule for some period (e.g, next six months)
- Flagged for future monitoring reviews

Some Examples of Monitoring

- Business Associates
- Accounting for Disclosures
- Training
- Safeguarding of PHI

Business Associate - Definition

- Performs or assists with a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, UR, QA, billing, benefit management, practice management, and repricing, or any function or activity regulated by the Privacy Rule
- Performs legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation and financial services involving the disclosure of PHI

Business Associate Examples

- Law Firms
- IT Companies
- Medical Record Coders
- Private Financial Auditors
- Document Imaging Firms
- Transcription Firms
- Shredding Firms
- Medicaid Assistance Firms

Business Associate Monitoring

Review Handout – Example 1

Business Associate Monitoring

Have policies and procedures been followed:

- Has agency identified all “business associates”?
- Do all of the agency’s business associate’s contracts contain proper language?

Identified Business Associates?

Monitoring process you might use:

- Sampling of invoices
- Statistically valid
- Stratified random sample
- Contract cover sheet completed?
- Review of non-business associate contracts
- Interview with agency contact for vendor

Proper Business Associate Contract?

Monitoring process you might use:

- Review list of identified business associates
- Review contracts for proper language

Accounting for Disclosures Compliance

- Beneficiaries have a right to an “accounting for disclosures” agency has made to outside individuals/organizations
- Accounting does not have to address all disclosures made

Accounting for Disclosures Compliance

Types of disclosures that don't need an accounting

- To carry out TPO
- To individuals of PHI about themselves
- Incidental to an otherwise permitted or required disclosure
- Pursuant to an authorization
- For a facility directory or to persons involved in the individual's care or other notification purposes
- For national security or intelligence purposes
- To correctional institutions or law enforcement officials in certain situations
- As part of a limited data set
- That occurred prior to the compliance date

Accounting for Disclosures Compliance

Examples of disclosures that do need an accounting:

- To attorneys under subpoenas/discovery requests
- Under court orders
- To most law enforcement officials
- To public health authorities
- For research (without authorization)

Accounting for Disclosures Compliance

Review Handout – Example 2

Accounting for Disclosures Compliance

Areas you would want to monitor:

- **Have workforce members been informed of what types of disclosures need to be accounted for?**
- **Are all disclosures that need an accounting being made by the Compliance Director?**
- **Is the Compliance Director maintaining the log?**
- **Are requests by beneficiaries for an accounting being properly handled?**

Accounting for Disclosures Compliance

Monitoring process you might use:

- Review training materials on accounting for disclosures
- Review beneficiary files for disclosures that require an accounting
- Ensure that any disclosures found are being made by Compliance Director
- Review Accounting for Disclosures Log

Training Compliance

- All current “workforce members” must be trained by 4/14/03 (Privacy Implementation Date)
- Workforce includes employees (including temporary employees), students, and others under direct control of agency
- There are ongoing training requirements
  - New workforce members
  - Material changes in the Privacy Rule

Training Compliance

Review Handout – Example 3

Training Compliance

Areas for compliance monitoring

- **Is training done on agency's policies and procedures?**
- **Has training been documented?**
- **Did all "workforce members" receive policy and procedure training prior to 4/14/03?**
- **Did workforce members hired after initial training was done receive policy/procedure training?**
- **Did workforce members receive the right training?**
- **Have there been changes to the Privacy Rule? Was new training needed? Was it done?**

Compliance Monitoring of Safeguards

Privacy Rule requires that the Medicaid agency:

- **must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the Privacy Rule.**
- **must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.**

Compliance Monitoring of Safeguards

- In the Privacy Rule, “Safeguards” is stated as appropriate administrative, technical, and physical safeguards
- Will overlap with the HIPAA Security Rule
- We have been doing combination Privacy and Security Assessments for these reasons

Compliance Monitoring of Safeguards

Review Handout - Example Number 4

Compliance Monitoring of Safeguards

Shredding Areas of Monitoring:

- Does agency have shredding contract?
- Does agency provide process?
- How is material stored until shredded?
- Are workforce members putting PHI in shredding containers? (Wastebasket Diving)

Compliance Monitoring of the HIPAA Privacy Rule

National Medicaid Conference

_experience the commitment

CGI

QUESTIONS AND DISCUSSION