Building Compliance into Your HIPAA Program

Christine Jensen - Denver Health

HIPAA Summit West II

March 15, 2002

Agenda

- Why Monitor the HIPAA Compliance Program
- Compliance Program Structure
- Start at the Beginning
- Transactions
- Security
- Privacy
- Acting on Findings

Denver Health

- Public Health System for Denver
- Acute Care Hospital with Level 1 Trauma
- 10 Off Campus Primary Care Clinics
- 14 School Based Clinics
- Public Health Department
- Behavioral Health and Substance Treatment
- Paramedics
- Rocky Mountain Poison and Drug Center
- Teaching and Research
- Correctional Care and Telemedicine

Why Monitor Compliance?

- To ensure you are protecting the privacy of PHI
- To verify you are meeting goals for your use of transactions and EDI
- To ensure you are providing a secure environment for PHI
- To identify opportunities to improve the program

HIPAA Compliance Program Organization

- Integrate the program and reporting with existing organization monitoring activities
  - Quality Improvement Program
  - Internal Audit Program
  - Risk Management
  - Customer Satisfaction

HIPAA Compliance Program Framework

- Structure
  - Foundations of the program: HIPAA rules, State and Federal Laws, JCAHO/NCAQ, patient care programs in your organization
- Process:
  - How do you do_____?
- Outcomes:
  - Were goals achieved?

HIPAA Compliance Program What to Monitor

- High Risk
  - Functions that if not properly performed pose a high probability that the privacy/security of PHI is in jeopardy
    - Revoked Consents
- High Volume
  - Functions performed frequently
    - Claims Submitted, Consents Obtained
- Problem Prone
  - Functions that, due to complexity, are generally problematic
    - Accounting of Disclosure, Revoked Consents

HIPAA Compliance Program
Start at the Beginning

- Integrate compliance monitoring into program development
- Determine current status so you can measure improvement
  - TCS - # of claims denied, no authorization
  - TCS - # of days to submit secondary claim
  - Security - # of days to get an employee of the systems
  - Privacy - # of privacy complaints

HIPAA Compliance Program
Start at the Beginning

- Proactive Monitoring/Testing
  - Test processes during implementation
  - Grant's Captain
  - "Walk Through" - Are all the pieces in place
  - Incorporate HIPAA requirements in:
    - > New patient care programs
    - > New/renovated buildings
    - > System implementation/upgrades
- Monitoring and Testing finds problems before 4/13/03

Monitoring - Transactions

- TCS is where the HIPAA rules are supposed to save healthcare $money$
- But how do you know if you are saving $$ if you don't know your current status, set goals and monitor outcomes?
- Setting Goals
  - Increased % EDI claims, EDI payment/RA
  - Increased # of clean claims
  - Decreased FTEs involved in posting claims
  - Decreased # of claims denied: no authorization, not eligible, etc.

Monitoring - Security

- The Security NPRM is the only HIPAA rule that specifically addresses “audit”
- “ Technical security services must include all of the following . . Audit controls (mechanisms employed to record and examine system activity). §142.308(c)(1)(ii)
- But what about non-system activity since the security rule is largely non-technical?

Monitoring - Security

- Broad strategic goals:

  PHI is secured using appropriate physical and technical security techniques and systems

- Specific goals:
  - No incidents of unauthorized access to PHI
  - 100% of PC placement in compliance with work station location guidelines
  - New workforce members receive security training within *1 week* of start date

Monitoring - Security

- Goal
  1. New workforce members trained within *xxx weeks*
  2. 100 % of access to Data Center authorized and logged
  3. No sharing passwords or smart card
- Monitoring
  1. Compare hiring, volunteer, medical staff records to participation in training.
  2. “Hacker” attempts to access data center without authorization
  3. Observations, “hacker” asks for passwords, failed sign-on attempts

Monitoring - Privacy

- The Privacy rule does not require monitoring
- However, the rule anticipates changes in the Privacy Program, the Notice must be revised when the program changes - changes may be driven by monitoring
- The Privacy Official is responsible for the development and implementation of the P&Ps of the entity. How can you implement P&Ps without monitoring to find out if they are followed and work.

Monitoring - Privacy

- Broad strategic goal

  The entity's privacy program will be a deciding factor in patient's selecting us as their health care provider.

- Specific goals
  - Consents are obtained from 99% of individuals seeking care
  - No more than 3 privacy complaints per quarter
  - Timeframes for processing requests and responding to the individual are met 100% of the time.

Monitoring - Privacy

- Goals
  - 99% Consents Obtained
  - 100% of clinical staff trained
  - 80% of staff can describe how/who to refer a patient to if they request access to their record
- Monitoring
  - # of opportunities vs. signed consents
  - Compare staff roster to training attendance
  - Staff interview, privacy drill, “privacy hacker”

Monitoring - Privacy
Be Proactive

- Don’t wait until you have a problem to begin monitoring
- Test the system
  - Privacy Drills
  - Privacy “Hackers”
  - “Walk Abouts”
  - Patient Satisfaction Surveys

Monitoring - Privacy

- Privacy Drills
  - Model after disaster drills
  - Present a issue to staff and have them follow through on the process
  - “I’m a patient who wants to see my record.”
  - Do all the stakeholders know the process, forms, timeframes, who to refer the individual to?

Monitoring - Privacy

- Privacy Hackers
- Can a “privacy hacker” break the the privacy program “firewall”?
  - Access to a record
  - Media Call
  - Requesting PHI
  - “Hacker” in a white coat

Monitoring - Privacy

- Walk About
- Look and Listen and Snoop
  - Is PHI posted in public areas - “whiteboards”?
  - Are patient’s charts or reports containing PHI in open/public areas?
  - Are staff discussing patients in public areas?
  - Are computers logged-off?
  - Are passwords posted on PCs, smart cards left in readers?

Monitoring - Privacy

- Patient Satisfaction Surveys
- How can you know if your program is protecting the privacy of individual's PHI if you don't ask the primary stakeholders?
  - Did you sign a consent, was it explained?
  - Did you receive a copy of the Notice of Privacy Practices, was it explained?
  - Do you feel like you have more control over the use of your health information?

Monitoring - Security & Privacy

- Incident Reviews - Incident may not have led to an actual breach of privacy
  - Process for formal review
    - What
    - Where
    - When
    - Why
    - Who
  - Track commonalties to determine if there are deficiencies in the program

Monitoring - Security & Privacy

- Sentinel Event Review - Actual breach of privacy
  - Root causes
    - Why did it happen,
    - Why was it done,
    - Why didn't staff know how to do….
  - Analysis of event and needed system/process changes

Acting on the Results

- Monitoring without analysis and action is a waste of resources
- If results meet your expectations and outcomes, monitor something else
- If the results don’t meet expectations
  - What
  - Where
  - When
  - Why
  - Who
- Plan of Action ➲ Monitor

Your Program

- You can't monitor everything!
- Like the program's P&Ps, monitoring should "be reasonably designed, taking into account the size of and the type of activities that relate to PHI undertaken by the CE".
  - What are the goals of your HIPAA program?
  - What are the risks in your environment?
  - What are your resources?