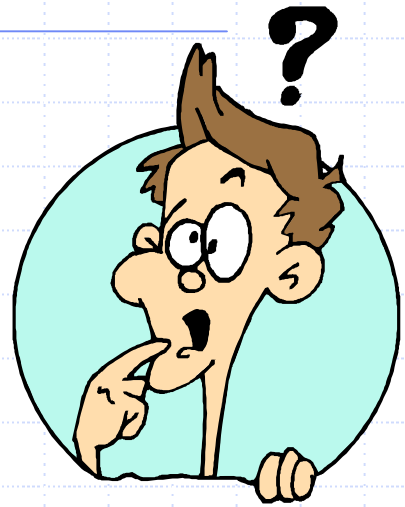
HIPAA



Now What???

Bill MacBain, CDPHP

HIPAA administrative simplification

- Privacy Rule
- Transaction and Code Standards
- Security Rule

compliance deadlines

- Privacy Rule

  -- *April 14, 2003*

- Transaction and Code Standards

  -- *Oct 16, 2003*

- Security Rule

  -- *April 21, 2005/2006*

PRIVACY RULE

- Shift: implementation to compliance
  - Documentation
  - Person responsible
  - training
  - compliant process
  - Response process
  - Audits
  - Investigation and remediation

--DHHS OIG Guidance 63 FR No. 35 2/23/98 Notices pp 8987-8998

Compliance

- Documentation
  - Policies
  - Procedures
  - Standards of conduct
  - Maintenance
    - Changes in internal conditions
    - changes in public policy
      - by Rule
      - by Interpretation

Compliance

- Person Responsible
  - Privacy Official
  - Cooperate with Fraud and Abuse Compliance officer, security officer
  - Access to top of organization
  - support
    - Administrative (space, time, secretarial)
    - technical (training, peer groups)

compliance

- Training
  - Regular
    - classes
    - reminders
  - Test for effectiveness
  - hands on
  - New employees / new responsibilities

compliance

- complaint process
  - multiple avenues
    - Supervisor
    - compliance or privacy officer
    - the boss
  - anonymous option (hot line)

compliance

- response process
  - investigate
  - if indicated…
    - MITIGATE
    - EDUCATE
    - DISCLPLINE
    - PREVENT RECURRENCE
    - RESPOND TO COMPLAINANT

COMPLIANCE

- AUDIT
  - MONITOR COMPLIANCE
  - IDENTIFY SPOT AND SYSTEMIC ISSUES
  - REPORT AT HIGH LEVEL
  - SYSTEMATIC APPROACH
    - AUDIT TOOL CROSS-REFERENCED TO REQUIREMENTS
    - INTEGRATE REGULATION, POLICIES
    - CYCLICAL SCHEDULE

COMPLIANCE

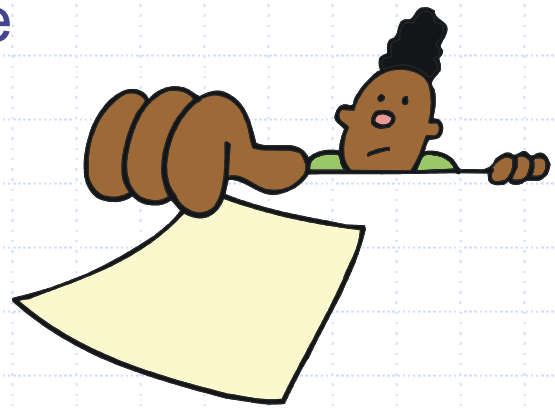
- INVESTIGATION AND REMEDIATION
  - FORMAL RESPONSE TO AUDIT FINDINGS
    - REPORTED TO HIGH LEVEL
  - PREVENT RECURRENCE
    - procedure change
    - technical modifications
    - training
    - sanctions
    - Bar access or employment

transaction & code standards

- Proceed with the end in mind
- hands-free transactions
  - example: pharmacies
- reduce denials to minimum
  - eliminate duplicates
  - determine eligibility real time
- concurrent payment

transaction & code standards

- Work with trading partners to test
- Consider all relevant transactions, not just claims
  - Eligibility
  - Inquiry
  - Referral / authorization
  - payment / remittance advice
- prioritize
- pleeeeeeese
  - don’t go back to paper



security rule

- administrative safeguards
- physical safeguards
- technical safeguards
- overlaps with privacy rule
  - adequate safeguards are required now

security rule

- Electronic P.H.I.
- required standards
- addressable standards
  - Do it
  - do something equivalent
  - don’t do it
  - document rationale

security rule

- administrative safeguards

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)

security rule

- physical safeguards

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

security rule

- technical safeguards

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

HIPAA – Now what??

discussion