The Path to HIPAA Compliance

Pamela McNutt
VP & CIO
Methodist Hospitals of Dallas
PamMcNutt@MHD.com

Organizing for Compliance

- Corporate Compliance Committee is the ultimate watch dog
- HIPAA Compliance Committee
  - Senior level administrators
  - Chaired by the CIO
- Designated Privacy Officer
  - One for each entity, probably an Administrator in Corporate, Risk Management? Legal? CIO?
- Designated Security Coordinator in I/S

Transaction Data Set Standards:

Federal Register 8/17/2000, full compliance 10/16/2002

- Opportunity to get electronic eligibility, authorizations and claims status on all payers
- The dilemma - EDI batch transactions versus Internet portals (direct data entry)? Which vendors will survive?
- MHD Compliance Team:
  - Patient Accounting
  - Admitting/Registration
  - Reimbursement
  - I/S
  - Medical Records
  - Administration

Transaction Data Set Standards:

Preparing for the 837 Format

- Providers must comply with the code set requirements
- Providers may continue to submit by paper but paper forms will be modified substantially
- Track how and when your patient accounting and clearing house vendors will be prepared
- Analyze the 72 new data elements, many are “situational” or can be derived from existing data

Transaction Data Set Standards:

Preparing for the 837 Format

- Determine crosswalks between UB92 data and the required 837data
  - Appendix F, National Electronic Data Interchange Guide, Healthcare Claim:Institutional ASC X12N 837 (004010X096)
  - New elements do not have a spot on the UB92
- Impact of NDC codes replacing HCPCS J-Codes for pharmaceuticals on bills
  - HCFA announced 4/2002 for acceptance, 10/2002 for compliance
  - We will get NDC codes from our Pharmacy system

Privacy Standards:

Federal Register 12/28/2000, full compliance 4/28/2003

- MHD Privacy Standard Compliance Team
  - Medical Records
  - Admitting/Registration
  - Information System
  - Legal
  - MSO
  - Quality Improvement
  - Human Resources
  - Hospital Education
  - Risk Management
  - Patient Accounting
  - Administration

Privacy Standards: **Key Tasks**

- Determine “roles” for security and authentication for every system and sign-on
- Determine necessary PHI data for each role
- Appoint Patient Representatives as the first contact for complaints and inquiries
- Policies, procedures and training for all employees and business partners
  - Concept of “identifiable data” and “authorized disclosure” must become as well know as Universal Precautions
- Notice to patients of their rights and our data use practices at time of consent (HHS verbiage)

Privacy Standards: **Patient Rights**

- Leverage current Release of Information process to handle requests for:
  - Review and update of medical records
  - Tracking and listing of all disclosures
- Really tough issue - how to handle requests that data be suppressed from specific usage?
- Change intake consent forms to cover the use of PHI for treatment, payment or operations
- Determine situations where an authorization for PHI release is necessary

Privacy:
Disclosures to Business Associates

- Business associates do not include medical staff or employees
- “Chain of trust”or business associate agreements
  - Inventory, review and update all contracts involving data exchange, processing or storage
  - Office of CIO and Legal reviews and approves all contracts
  - Give third parties de-identified and only the minimum data needed
  - Develop standard confidentiality clauses

Privacy:

The Really Hard Part - Exceptions and Definitions

- Determine if your health plan and your affiliates are business associates, separate covered entities or a component entity needing “safeguards”
  - Self insured health plans
- Understand the exceptions, document how they apply in your operations
  - Clergy
  - Patient locators and information desks
  - Emergencies, deaths and minors (documentation required)
  - Consultations
  - Indirect treatment relationships
  - Psychiatric notes

Privacy:

The Really Hard Part - Exceptions and Definitions

- Where does disclosure for payment stop?
  - Collection agencies
  - Credit bureau (limited data)
  - Chart review by carriers
  - “For your payment only” does not include non-owned physicians
- Define what “operations” is to your facility
  - Look at all business functions, internal and contracted, for non-operational activity which needs authorization
  - QA and research
  - Contacts for patient satisfaction, follow-up and scheduling
  - Marketing and fundraising restrictions

Security:

Draft, final regulation expected Spring 2001

- Information access controls and security configuration management
  - Keep Y2K derived inventory of hardware and software current
  - Add password and ID security methodology to the database of systems
  - Enforcement of standards for computer systems and the procurement process
- Compliant network security requires state of the art data network with robust monitoring tools

Security:
Data Integrity and Physical Controls

- Contingency and disaster recovery
  - Redundant network and server architecture
  - Mainframe hot-site arrangement, tested off-site tape backup storage
- Physical controls for testing and revision
  - Change control methodologies applied to all systems and vendors
  - “Test” systems setup - no live system upgrades
  - Restricted/authenticated dial-in vendor access

Security:
Data Integrity and Physical Controls Integrity

- Authorization and authentication control
  - Automatic logoffs keep workstations from being tied up
  - “Single sign-on” solutions are convenient for users, is it the answer to user compliance as well?
- Secured workstations
  - “Public PCs” with locked setup including no disk drive access
  - Network ports alarm and disable if an unknown PC plugs in

Security:

Internet and Remote Access Issues

- HIPAA will help enforce unpopular issues
- Security concerns introduce new challenges
  - Tokens or biometrics for authentication
  - Encryption and network authentication without loading proprietary software on physician's PC
  - Web servers need to be secured from rest of network
  - Security concerns about DSL, cable modems and other "tunneling" connections

Vendor Software Issues:

Is now the time to buy new systems?

- Most commercial systems do not have:
  - Logs tracking access by patient by user ID
  - Finely delineated role based security functions
- Vendors are already hurting - consolidations and product “sunsets” will be rampant
- We are spending our resources to get up-to-date on the current releases of our software
- Put clauses in contracts that fixes and enhancements for HIPAA will be at no charge

State Privacy Law:
Reconciliation with HIPAA

- Big task to reconcile your current and pending state laws with HIPAA
  - Different definitions and terminology
- Many states have enacted or have pending bills that are highly redundant to HIPAA
- Recent publicity about HIPAA's "lax" marketing and fundraising stance with a call to action for states to address locally