Health Care Information Technology 2003

- Session 2.3
- Practical Initiatives in Complying with HIPAA & California's Health Care Privacy and Security Laws and Regulations

- ***The Physician Perspective***

- **Steven M. Fleisher, JD**
- **Fleisher & Associates**
- **Alamo, California**

The Setting

- A Distressed Cottage Industry
  - Most physicians work in small or solo practices of five or less (42% of CMA members are in groups of 1-4)
  - Income is static or declining even in larger groups
    - No increases in reimbursement
    - Likely further decreases in budget/war crunch
  - Costs continue to escalate
- Focus today on physician's own activities, not hospital or community based planning
- Assume basic HIPAA understanding

Fear & Loathing on the HIPAA Trail

- Resistance to HIPAA
  - Another un-reimbursed government mandate
  - Concern about cost and change
  - Unscrupulous rumor mongering by vendors and others
    - Penalties and enforcement
    - Absurd "HIPAA requirements"
- Little appreciation of the potential upside with the TRA regulations

Physicians as Covered Entities

- Some use electronic means to engage in covered transactions and so are Covered Entities
  - Sleeper: the swipe cards for eligibility determinations
- Medicare will **require** all larger providers (>10 FTEs) to file electronically after 10/16/03
- The health plans will not be far behind
- Most doctors who bill will be covered by HIPAA in the next several years

Motivation for Physician Compliance

- Government (OCR) enforcement
  - Enforcement complaint driven
  - Very limited resources
  - Not unless you are *really bad*
- Civil Liability
  - Plaintiffs lawyers know all about HIPAA
  - HIPAA privacy and security regulations likely to become national standard of care for healthcare records

So far…….

- Doctors (especially small and solo practitioners) feel broke and besieged
- They are afraid of HIPAA
- Most will be covered despite the "opt out of HIPAA" campaigns
- How will they make compliance work?
- Will technology help?

Transaction & Code Set Rule

- This is the upside for providers
  - Significant reductions in costs per transaction
  - Reduced staff time per claim
  - Reduced number of "lost" claims
  - One study → $7,200 savings per physician per year (51% back office, 37% bad debt, 12% pre-authorization and eligibility/benefit verification)

Practical Vendor Issues

- Providers essentially dependent upon vendors for the technology for the transaction sets
  - Clearinghouse or billing service/software vendor
  - Testing and compliance issues unclear for providers
    - "Don't worry doctor, we are HIPAA compliant"
    - Why to worry……..

Vendor Issues

- When will you start testing (before 4/16/03)?
- What will you test (which of the eight transactions)?
- Will you get certified? By whom?
- What security solutions will you use for:
  - Identification and authentication
  - Encryption
  - Disaster recovery

Electronic Medical Records

- Cost
- Techie propensities desirable
- No uniform standards
- Time required to customize and train (6 months)
- Financial stability of vendors
- Interesting, useful for HIPAA compliance but no panacea

Privacy Rule Overview

- Two key concepts with regard to PHI
  - Enhance patient's control and understanding
  - Enhance provider's duty to protect it
- Confidentiality is a concept providers understand
- Mainly a need to enhance existing awareness and increase staff training

Privacy: practical approaches

- In response to fear, lack of funds and general resistance, our focus is on the simple and practical
- Approach: remove the fear, compliance is just *work*
- Technology, especially the expensive or complex types, while helpful, cannot be at the center of compliance strategies for most physician practices

Practical Privacy Tips

- Put one person in charge (Privacy Official)
  - The HIPAA Czar
  - Give him/her training and authority and time
- Inventory types, uses and disclosures of PHI
  - Critical for success
- Telephone, office and hallway conversations
- Remove PHI from easy patient access
  - Chart racks, chart holders
  - reception areas, exam rooms, hallways
  - physician's desk

Practical Privacy Tips (2)

- Employees
  - clearance procedures
  - training procedures
  - proper uses and disclosures
    - On-going obligations
    - Role-based access
  - sanction procedures
  - termination procedures
- In-coming (faxes & other PHI)
- Out-going (faxes, commercial couriers, and spike haired kids)
- Patient email: have a written agreement!

Patient's Rights

- Document all activities
  - Request, response, tracking of actions
  - File separately, especially complaints
  - Only one request in place at a time (limits on use of PHI or alternative channel of communication)
- Do the Notice of Privacy Practices last to assure consistency and conform for specific practice:
  - Pediatricians re joint custody issues
  - Oncologists re treatment areas and support groups
  - All re leaving messages and sending postcards
- Be sure your forms, policies and procedures are state law compliant as well as HIPAA

Business Associate Agreements

- Examples: billing service, transcription service, collection agency, software vendor, outside practice manger
- Prepare a list of BAs
- Usually will be an amendment to existing agreement
- Watch termination dates so they coincide
- Respond if any reason to believe BA has breached contract
- Further disclosures regulated under California law

Physical Security

- Industrial security is a new concept in healthcare
- Office locks (*quality*)
- Office keys (*quantity*)
- Visitor and patient supervision (vigilance)
- Waste disposal (*shred! shred! shred!*)
  - California law also requires safe destruction of PHI
- Check ability to view computer screens

Physical Security (2)

- Limit access to computer to authorized staff
- Storage of backups and removable media
- Home use and storage
- PDAs & laptops-theft is foreseeable!
- Lab and treatment devices which store/contain PHI
- Locked chart racks?
- Burglar alarms and motion detectors

Technical Security Tips

- Passwords
  - *Good* passwords (H*X23#ym)
  - No sharing
  - "Post-Its" with passwords
  - Changing and terminating passwords
- Access rights according to function, audit, authorization
- Screen savers
- Anti-virus software;
- OS and applications regularly updated for security fixes
- Firewalls (software and hardware routers)
- Encrypt PHI before sending on internet

Practical Solutions

- Extremely difficult for physicians in smaller practices to organize compliance on their own
- Larger practices can hire a consultant
- Many medical societies and private vendors seeking to respond
- Problems
  - Training/education
  - Implementation planning
  - Policies, procedures and forms which integrate state preemption analysis

CMA's Approach: a CD tookit

- Complete physician-focused compliance tool
  - Policies, procedures & forms customized for California law by CMA attorneys
  - Training for physicians & staff
  - Implementation planning
  - Regular updates
- CD technology readily accessible
- Designed to use without a consultant

Conclusions

- Most front line doctors love high tech in the hospital, not in their offices
- The TRA rules could be a significant benefit especially to smaller practices- move them closer to the 21st Century
- HIPAA compliance for most will be a low-tech affair for these physicians

Contact Information

- Steven M. Fleisher
- Fleisher & Associates
- 35 Corwin Drive
- Alamo, CA 94507
- 415.882.5159
- fleisherassociates@att.net