



Sixth National HIPAA A Summit

- ◆ Practical HIPAA Compliance Strategies for Medical Groups, IPAs and Clinicians
- ◆ *Privacy & Security Issues*
- ◆ Steven M. Fleisher, JD
- ◆ Fleisher & Associates
- ◆ Alamo, California



Perspective

- ◆ Focus today on outlook and needs of smaller providers in solo and small groups (whether IPAs or Medical Groups)
- ◆ Smaller practices: vast majority and fewest resources
- ◆ Assume basic HIPAA knowledge
- ◆ Questions at the end




The Setting

◆ A Distressed Cottage Industry

- Most physicians work in small or solo practices
 - PCPs: 34% Solo; 24% 2-10 [58%]
 - Specialists: 46% solo; 26% 2-10 [72%]
- Income is static or declining even in larger groups
 - No increases in reimbursement
 - Likely further decreases in budget/war crunch
- Costs continue to escalate

◆ Doctors unhappy with practice realities



Fear & Loathing on the HIPAA Trail

◆ Resistance to HIPAA

- Another un-reimbursed government mandate
- Concern about cost and change
- Unscrupulous pandering and 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



Provider Compliance

- ◆ Government (OCR) enforcement
 - Enforcement complaint driven
 - Very limited resources (30 staffers)
 - No jail 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
- ◆ LOTS of smaller CEs will be late and even later



So far.....

- ◆ 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 can they be helped?



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, afford specific rights 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/Czarina
 - 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



State Law (Preemption) Issues

- ◆ Be sure your forms, policies and procedures are state law compliant as well as HIPAA
- ◆ Preemption analysis and application to procedures and forms is a complex task
- ◆ Beg, buy or borrow someone else's
 - State/national medical and specialty societies
 - Bar Associations
 - Hospital associations
 - State agencies
 - Georgetown Privacy Project
 - Goldberg's ABA Project



Preemption (2)

- ◆ Evaluate Analyses
 - Scope of work-
 - does it cover small provider issues?
 - What sources were reviewed?
 - Inventory of state laws v. laws which HIPAA impacts
 - Assumptions
 - Updates
- ◆ Key areas: highly confidential PHI, access rights, minors, psychotherapy notes, authorizations



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
- ◆ Watch for any state law issues



Security Rule

- ◆ New Rule important to understand HHS' approach: principles *not* details
- ◆ Focus on “mini-security rule in §164.530(c) (“reasonably safeguard”)
- ◆ Risk assessment is *critical* and the place security compliance must start
 - Not rocket science
 - Use common sense



Physical Security

- ◆ Industrial security is a new concept in healthcare
- ◆ Access Restrictions
 - Office locks & keys
 - Physical access to computers
 - Chart racks
 - Visitor and patient supervision (vigilance)
- ◆ Waste disposal (*shred! shred! shred!*)



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
- ◆ Backups and disaster preparation



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 toolkit

- ◆ 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
- ◆ HIPAA compliance for most will be a low-tech affair for these physicians
- ◆ The TRA rules could be a significant benefit especially to smaller practices-
move them closer to the 21st Century



Contact Information

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