HIPAA Privacy:
Fundamentals and Key Challenges

Kirk J. Nahra
Wiley Rein & Fielding LLP
Washington, D.C.
202.719.7335
KNahra@WRF.com

February 5, 2003

Key Issues

- HIPAA 101
- For covered entities, employers and business associates
- Key remaining issues
- Advice/issues to watch out for

State of the HIPAA Rules

- Privacy
  - Final Final – August 14, 2002
  - Compliance date – April 14, 2003
  - No extension
- Standard Transactions
  - Compliance date – October 16, 2002
  - One-year extension possible
  - Filing necessary
- Security – projected to be published on December 27, 2002
  - Draft is four years old
  - Don't ignore security component of privacy

Health Care Privacy: How We Got Here

HIPAA Statute/1996

Administrative simplification and privacy (intersection of business developments and law)

- Congress missed August 21, 1999 deadline

Final Rule - published December 28, 2000

Final Final Rule -- August 14, 2002

Compliance date -- April 14, 2003

Final Rule Issues

- Consent/notice
- Marketing
- Business associates
- Modest fixes
- Politics, politics, politics

State of the Play

- Compliance is all over the map
- Major health insurers are generally in reasonable shape – “the leader of the behinds”
- Physicians are way behind
- Hospitals in reasonably good shape
- Groups/employers are way behind
- Many vendors/business associates are way behind

NCVHS Letter/Comments

NCVHS/ (National Committee on Vital and Health Statistics) is an advisory body for HHS on HIPAA. Their recent comments:

- "Surprised and disturbed" at the generally low level of implementation activities and the high levels of confusion and frustration
- Many providers have never heard of HIPAA and do not think it applies to them
- Likelihood of "widespread disruption" of the health care system as we approach April 14, 2003

NCVHS Letter/Comments

- Large employers with self-funded employee benefit plans have received no guidance on when their benefits-related activities are subject to the Privacy Rule
- “Nobody” seems to know whether HIPAA or state law applies in the numerous instances in which the laws conflict
- HHS HIPAA implementation assistance efforts need to be increased by several orders of magnitude – and quickly

Who Must Comply with HIPAA?

- Health plans (health insurers)
- Health care providers
- Health care clearinghouses
- Employers? Not directly – big issue
- Other insurance entities (e.g., life, auto, disability)? No
- Business associates (indirectly)

Key Concepts

- TPO
- PHI
- Business Associate
- Minimum necessary
- Covered entity

What Information is Covered?

- Protected health information ("PHI") – individually identifiable health information
- Transmitted or maintained in any form (electronic, paper, oral)
- Very broad coverage – names, address, virtually anything about health plan members

Rules of Disclosure

- PHI may not be used or disclosed by covered entities except as authorized by the individual who is the subject of the information or as explicitly provided by the rules.
- Exchange of protected health information should be relatively easy for health care purposes and more difficult for purposes other than health care.

Core Health Care Purposes

TPO-

Treatment – the provision, coordination or management of healthcare – performed only by health care providers

Payment – activities undertaken by health plan to obtain premiums or to determine or fulfill responsibility for coverage and provision of benefits under the health plan (e.g., eligibility, billing, claims management, medical necessity, utilization review) or by a plan or provider to obtain or provide reimbursement for health care.

Core Health Care Purposes

Health care **O**perations – administrative activities, including quality assessment and improvement activities, credentialing, underwriting, medical review, audits, fraud and abuse, business planning and development, business management of the health plan.

Additional Rules of Disclosure

- Consent now optional for everyone
- Notice of Privacy Practices must be given to patients by providers instead of consent
- Also disclosures without consent in identified "national priority areas" (e.g., public health emergencies, fraud investigations, required by law disclosures)

Compliance Obligations

- Develop a notice of information practices for distribution to customers
- Develop procedures for "minimum necessary disclosure" where disclosure is authorized
- Designate a company privacy official
- Train employees on privacy requirements
- Develop physical, administrative and technical safeguards for the protection of information
- Patient access/restrictions

Compliance Obligations

- Develop a means of tracking certain disclosures of protected health information
- Develop an internal complaint process
- Develop sanctions for wrongful acts
- Develop information sharing policies and procedures
- Draft contracts for arrangements with business associates to share protected information

Minimum Necessary: Standard

- When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make all reasonable efforts to limit PHI to the minimum necessary to accomplish the intended use or disclosure.

Notice: Standard

- Generally, individual has right to adequate notice of:
- the uses and disclosures of PHI that may be made by the covered entity
- the individual's rights and
- the covered entity's legal duties with respect to PHI

What Makes A Business Associate?

- Generally, someone who
  - on behalf of a CE, performs or assist in specified functions (claims processing, data analysis, UR) involving PHI
  - provides services for a covered entity involving PHI (legal, accounting, actuarial)

Individual Rights

- Access
- Complaints
- Accounting
- Amendment
- Notice

Member Rights

- Complicated
- Mainly for people with complaints
- Compliance and risk management
- Confidential communications

Spouses

- Normal course of business
- Low percentage of problems
- High risk where problems occur

Enforcement Issues -- Privacy Rules

- Complicated
- Extensive
- Ambiguous?
- Consistent?
- Relevant to real world?

Enforcement - Basics

- Civil penalties

  $100 per violation

  $25,000 in a calendar year for violation of identical prohibition or requirement

Enforcement - Criminal

- Knowingly violates
- Progressive penalties, starting with
  - $50,000 imprisonment of not more than one year; and
  - $250,000 imprisonment of not more than 10 years
- How likely?

Enforcement – Next Levels

- No civil penalty for criminal violators
- No penalty if entity did not know of violation and by exercising reasonable diligence would not have known of violation
- No penalty if violation due to reasonable cause and not to willful neglect and problem is corrected

Who Enforces?

- HHS Office of Civil Rights
  - Enforcement approach
    - Negotiation
    - Education
    - Cooperation
  - No enforcement rule
    - Staffing?
    - Resources?

Privacy Enforcement

- Less government?
  - Civil
  - Criminal/a real risk?
- Patients/individuals
- Class Actions

Enforcement

- Understanding where challenges will be
- Making smart decisions
- Keeping a good perspective
- Compliance vs. business vs. risk management

Litigation Basics

- No HIPAA private right of action
- What could happen?
- Gramm-Leach-Bliley?
- Insurance practices/deceptive trade practices?
- Common law?
- State privacy laws

Litigation – Next Steps

- Standard in the industry
- State deceptive trade practices
- Common law invasion of privacy
- Creativity

Key Issues

- What is the claim?
- Who is it by?
- What are the damages?

Smith v. Chase Manhattan Bank

- Financial institution gave list to third party, received payments on sales
- Said it didn't do these things in privacy notice
- No damages alleged/no cause of action
- Only unwanted telemarketing

Key Risk Areas

- Employment
- Marketing
- Spouses
- Individual rights
- Broadly applicable issues (code word – class action)

Conclusions

- Government has fewer and weaker tools in privacy
- Government will be creative in pushing the envelope
- Private litigation will be substantial and creative

Conclusions

- Private litigation probably more important
- Monetary implications are very unclear
- Pressure and adverse publicity are very important
- Some rule for whistleblowers/complaints

Relations with Employers

- Very complicated
- At least confusing/perhaps inconsistent
- Major client relations issues
- Opportunities and challenges
  - Shift to fully insured?
  - Will customers abandon group health care?
  - New client opportunities?
  - Keep an eye on this

Employer/Group Issues

- Rules make little sense
- Mass confusion
- Likelihood of mistakes
- Customer relations
- Will require significant changes

What Is The Issue?

Avoid having PHI used by employers for employment-related purposes

- HHS' fix:
  - HHS does not directly regulate employers or other plan sponsors
  - Instead, HHS places restrictions on the flow of information from covered entities to non-covered entities, including plan sponsors

The Role of the Employer

Plan Sponsor

- Is the employer a plan sponsor of a group health plan (GHP)?
- Rule restricts flow of PHI between GHP and plan sponsor
- Minimal impact of rule on plan sponsor that receives summary health information for premium bid purposes or enrollment information

Plan Sponsor (cont'd)

- Substantial impact of rule on plan sponsor that receives PHI
- Sponsor must amend and certify plan documents before receiving PHI – otherwise violation of HIPAA
- Amendments must spell out permitted uses and disclosures of PHI by sponsor

Compliance Obligations For Health Plans

- If fully insured and receive only Summary Health Information (SHI) or enrollment information, very limited effects
- If (1) self-insured or (2) fully insured and get PHI, substantial obligations – full covered entity

Contract Types

- Business associate (privacy)
- Chain of trust (security)
- Trading partner (standard transactions)

Focus on understanding/analyzing overlaps

Business Associates

- Who are they?
- When?
- What will you require of them? (requirements + options)
- Links to standard transactions

Additional Issues

- Enforcement rules on business associates
- Potential responsibility beyond enforcement rule
- Customer/public relations aspects?
- Risks on timing (wolf in sheep's clothing)

Preemption

- More stringent state law
- Other federal law
- No one understands this
- Strategy
- Multi-state issues
- How many states are you worried about?

Misconceptions – Minimum Necessary

- Misunderstood
- Hard
- Extensive
- Mainly a documentation project
- Will it require changes?

Misconceptions

Consent and authorizations

- Who must sign
- Underwriting
- Convenience
- Customer issues

Getting Started on HIPAA

- Audit of information use/practices
- Work HIPAA into contract negotiations/ renegotiations
- Educate employees
- Educate business associates
- Educate providers

Conclusions

- Still lots to do
- Very difficult balancing act
- Keep an eye on the lawsuits
- Be conscious of where people can complain – and where they may not
- Expect confusion
- An ongoing issue that will not be going away

Top HIPAA Reminders

- HIPAA requires significant change by all segments of the health care industry – and all at once.
- HIPAA changes all aspects of the way covered entities do business
- The general public will scrutinize the health care industry more stringently because of HIPAA
- Need to educate customers on requirements/non-requirements