HIPAA SUMMIT II - EMPLOYER ISSUES

The Second National HIPAA Summit

Washington, DC
March 1-2, 2001

The Final HIPAA Privacy Rule: Issues for Employers

Alan C. Brown, Duane Morris
Robert L. Roth, Crowell & Moring LLP

Overview

Statutory Authority: HIPAA Administrative Simplification Requirements

- **H**ealth
- **I**nsurance
- **P**ortability and
- **A**ccountability
- **A**ct of 1996

Overview

Section 264 of HIPAA:

- **Recommendations to Congress**
- **Promulgation of Regulations**
- **Preemption**

Scope of HIPAA Privacy Regulations:

- What is covered?
  - Individually Identifiable Health Information
    - De-identified data
    - Summary data
- Who is covered?
  - Covered Entities
  - Hybrid Entities
  - Indirectly -
    - Business Associates
    - Health Plan Sponsors

What are “Covered Entities”

- HIPAA provides that the administrative simplification standards (including the privacy and security standards) apply to:
  - healthcare providers who transmit health information in electronic form in connection with certain enumerated transactions
  - all healthcare clearinghouses
  - most health plans

What is a HIPAA "Health Plan"?

- "Health Plan" includes, among other things:
  - a "group health plan"
  - a multi-employer plan

What Is A Group Health Plan?

- An employee welfare benefit plan, as defined in ERISA
- Including insured and self-insured plans
- That provide medical care to employees or their dependants
- Directly or through insurance, reimbursement, or otherwise

Multi-Employer Plans

- "Health Plan" also includes:

  "An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers."

Group Health Plans

- In short, HIPAA “covered entity” includes:
  - single or multi-employer group health plans
  - insured or self-insured
  - that pay for diagnosis, treatment or prevention of disease
  - of employees or their dependants
  - directly, by reimbursement, or through insurance

"Catch-all" Definition

- Rules also define "health plan" as including:
  - "Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care"
- Seemingly inconsistent with small plan exemption

Examples of Employer-Sponsored "Health Plans"

- Employer-sponsored:
  - Clinics
  - Health insurance
  - HMO membership
  - Vision care
  - Dental care
  - Prescription drug coverage (but not prescription discount programs)
  - Medical flexible spending accounts
  - Cafeteria plans that include medical care options

What Health Plans Are Not Covered

- Small, self-administered health plans are exempt
- A group health plan is NOT a “covered entity” if it
  - has less than 50 employees, AND
  - is self-administered (by the employer who established and maintains the plan)

These Are NOT Covered Entities

- Employers (but other laws such as ADA may protect employee health information)*
- 3rd party administrators
  - may be “business associates”
- Property, casualty, disability, and auto insurance plans, even when they pay for health care
- Workers compensation programs
- HMOs and insurers are covered entities, but do not become business associates by providing coverage to a group plan
- Stop-loss and reinsurers

Scope of HIPAA Privacy Regulations:

- "Hybrid entity means a single legal entity that is a covered entity and whose covered functions are not its primary functions."
- Use of firewalls

Preemption Under HIPAA

- Effect on ERISA Preemption

- HIPAA Preemption - 45 C.F.R. § 160.201 et seq.

Preemption Under HIPAA

- Effect on local laws
  - "State law means a constitution, statute, regulation, rule, common law, or other state action having the force and effect of law."

65 Fed. Reg. 82901 (Dec. 28, 2000)

  - "We agree that, to the extent a state treats local law as substituting for state law it could be considered to be 'state law' for purposes of this definition."

65 Fed. Reg. 82581 (Dec. 28, 2000)

Enforcement Under HIPAA

- Section 164.522(e)(1)(ii) of the proposed rule states: "If the Secretary determines that the matter cannot be resolved by informal means, the Secretary may issue written findings documenting the non-compliance to the covered entity and, where the matter arose from a complaint, to the complainant. The Secretary may use such findings as a basis for initiating action under section 1176 of the Act or initiating a criminal referral under section 1177."
- 64 Fed. Reg. 60063 (Nov. 3, 1999)

Enforcement Under HIPAA

- [S]ection 1176 grants the Secretary the authority to impose civil monetary penalties against those covered entities which fail to comply with the requirements established under part C . . . .
- Under section 1177(a), the offense of "wrongful disclosure" is a disclosure that violates the standards or requirements established under part C. These would include any disclosures not otherwise permitted under the privacy standards or the parallel security standards.

64 Fed. Reg. 60003 (Nov. 3, 1999)

Enforcement Under HIPAA

- Under Section 1176(a)(1): "Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000."
- Under Section 1177(a): A person who knowingly and in violation of this part -- (3) discloses individually identifiable health information to another person.

Enforcement Under HIPAA

- Enforcement - The Secretary has decided to delegate her responsibility under this regulation to the Department's Office for Civil Rights (OCR). OCR will be responsible for enforcement of this regulation. Enforcement activities will include . . . Seeking civil monetary penalties and making referrals for criminal prosecution.

65 Fed. Reg. 82472 (Dec. 28, 2000)

Enforcement Under HIPAA

- If the matter could not be resolved informally, the Secretary would be able to issue written findings, be required to inform the covered entity and the complainant, and be able to pursue civil enforcement action or make a criminal referral.
- Ninth, §160.312(a)(2) deletes the reference in the proposed rule to using violation findings as a basis for initiating action to secure penalties. This deletion is not a substantive change. This language was removed because penalties will be addressed in the enforcement regulation.

65 Fed. Reg. 82487 (Dec. 28, 2000)

Business Associates of Employer-Sponsored Health Plans

- Plan sponsors are not business associates, even if they provide administrative services
  - special rules for sponsors
- Employees of plan or sponsor are not business associates
- Outside actuaries, third party administrators, ERISA counsel, plan consultants can be business associates if they receive protected health information

Requirements for Business Associates

- Contracts required with business associates that impose most of the requirements of the rule, and provide for HHS audit rights
- Covered entity violates rule if it “knew” of a “pattern of activity or practice” in breach of the business associates obligations and failed to take reasonable steps to cure
  - oversight duty decreased in final rule
  - “third party beneficiary” requirement eliminated in final rule

Administrative Requirements For Health Plans

- Privacy official and contact person
- Training (certification requirement deleted)
- Security (administrative, technical and physical safeguards)
- Internal complaint process
- Whistleblower protections
- Sanctions
- Written policies and procedures

Simplified Requirements For Plans That Purchase Coverage

- Group health plans that
  - offer benefits solely through purchase of insurance or by contracting with an HMO, AND
  - do not create, receive or maintain PHI other than summary information and enrollment information
- Do not have to comply with the privacy officer, training, security, or complaint requirements, provide a privacy notice, or have written policies and procedures
- Must comply with new requirements relating to plan documents

Small Plans Get Extra Time

- "Small Health Plans" that are covered entities get an extra year to comply
  - "Small" means annual receipts of $5 million or less
  - For health plans, "annual receipts" means "pure premiums"

Plan and Sponsor As Distinct Entities

- Statute perpetuates fiction of separation between plan and employer
  - Plan is covered entity
  - Employer (plan sponsor) is not
- Typical that EMPLOYER, not plan, administers plan, in whole or in part
- Same individuals likely to have other functions within employer organization
- Final rule begins to confront this issue

Disclosures To Plan Sponsor

- Protected information may be disclosed to the plan sponsor (the employer) by the plan, or by an insurance issuer or HMO, for plan administration purposes
  - agreement required with sponsor
  - information may be used only for plan administration
  - uses must be specified in plan documents
- Administration means payment or healthcare operations purposes

Required Changes to Plan Documents

- To permit disclosure to sponsor, plan documents must be amended
- Plan sponsor must agree to the restrictions and obligations
- Sponsor must certify that plan documents have been amended before any disclosure may occur
- Requirements are similar to those of a business associate

Plan Document Requirements

- Description of permitted disclosures to, and uses and further disclosures by the sponsor
- Any agent or subcontractor must agree to the same restrictions that apply to the sponsor
- Information may not be used for any employment related purpose or in connection with any other benefit plan
- Sponsor must report to the plan any unauthorized use or disclosure
- Sponsor must agree to provide beneficiaries with access to personal information, opportunity to amend, and disclosure accounting

Plan Document Requirements (cont.)

- Sponsor must make its internal practices, books and records available to HHS for audit
- Return or destroy information when no longer needed
- Provide for “Adequate Separation”
- No patient consent required
- Disclosures to sponsor subject to “minimum necessary” standard

"Adequate Separation" Between Plan and Employer

- Plan documents must:
  - describe classes of sponsor's employees or persons who will receive protected information
  - restrict the access and use by those persons to plan administration functions that the sponsor performs for the plan
  - provide an "effective mechanism" for resolving any noncompliance by one of these persons
- HHS describes this as a "firewall"

Disclosure of Summary Information

- Employers may also receive “summary information” from the plan for purposes of soliciting bids from insurers, or for purposes of modifying or terminating the plan.
- “Summary” health information is data that summarizes the claims history and expenses from which identifiers have been removed
  - because of the size of the group, re-identification may still be possible
- Plan must provide notice that data may be disclosed to the employer

Domestic Violence Protection

- Beneficiaries may request confidential or alternative means of communications
  - e.g., a dependant may request that advice of payment forms not be sent to the named insured
  - might request information be sent to work
- Health plans must accommodate all reasonable requests if the individual states that disclosure could endanger the individual
- “Reasonable” relates only to burden
- May not require justification of risk

Some Effects On Employers

- Privacy requirements become a new element in decision whether to self-insure
- Can “experience ratings” and other contracts be negotiated using only summary data?
- More wrongful termination suits? (protected health information was improperly used by the HR Dept in decision to terminate)

Other Question Areas

- Disease management and EAPs
- Coordinated health, disability, and workers comp programs
- Industrial health and safety studies (injury, absenteeism, environmental hazards, etc.)
- Drug testing
- Return-to-work determinations
- Is the information provided by a covered entity?
  - e.g., physicians who do not engage in standard transactions are not covered entities
- Employee consent

HIPAA SUMMIT II - EMPLOYER ISSUES

ALAN C. BROWN

Duane Morris
Washington, DC
P: 202-776-7893
F: 202-776-7801
acbrown@duanemorris.com

ROBERT L . ROTH

Crowell & Moring LLP
Washington, DC
P: 202-624-2870
F: 202-628-5116
rroth@cromor.com