The First National HIPAA Summit

HIPAA Privacy for Employers

It's Not Just For the Healthcare Industry!

Alan C. Brown

McKenna & Cuneo, L.L.P.

October 15-17, 2000 ♦ Washington, DC

Will The Final Privacy Rules Differ From the Proposed Rules?

- HIPAA required that final health information privacy rules be issued by February 21, 2000
- Proposed rules were directed primarily at providers and insurers
- Left numerous unanswered questions regarding application to employers
- HHS has hired outside employee benefit expert to assist on final rules
- Employer provisions are likely to change significantly in final rules

Are Employers "Covered Entities" Under The HIPAA Privacy and Security Rules?

- Employers outside the healthcare industry are not generally "covered entities"
- BUT components of employers can be covered entities:
  - Employee health plans
  - Clinics
  - Nurses Offices

What are “Covered Entities”

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

What is a HIPAA "Health Plan"?

- HIPAA defines "health plan" to include, among other things:
  - most "group health plans"
  - multi-employer plans
  - long-term care policies

Group Health Plan

- HIPAA incorporates definition from Public Health Service Act:
  - “The term "group health plan" means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income Security Act of 1974 (29 U.S.C. 1002(1))) to the extent that the plan provides medical care (as defined in paragraph (2)) and including items and services paid for as medical care) to employees or their dependents (as defined under the terms of the plan) directly or through insurance, reimbursement, or otherwise”

“Medical Care”

- Public Health Service Act provides that “Medical Care” means “amounts paid for”:

  (A) the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any structure or function of the body,

  (B) amounts paid for transportation primarily for and essential to medical care referred to in subparagraph (A), and

  (C) amounts paid for insurance

Group Health Plan

- In short, a HIPAA group health plan is:
  - an ERISA plan
  - that pays for diagnosis, treatment or prevention of disease
  - for employees or dependants
  - directly, by reimbursement, or through insurance

Which Group Health Plans are Covered Entities?

- Small plans are exempt if they
  - have less than 50 employees, AND
  - are self-administered (by the employer who established and maintains the plan)
- All other group health plans are covered entities

Multi-employer plans

- Covered Entity includes
  - “An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers”
  - Proposed rules specify that Multiple Employer Welfare Arrangements are included
  - Multi-employer trusts also included

“Catch-all” Definition

- Proposed rules also define “health plan” as including:
  - “Any other individual plan or group health plan, or combination thereof, that provides or pays for the cost of medical care”
- Inconsistent with small plan exemption

What Is Not a Covered Entity?

- Workers compensation programs
- Property, casualty, and auto insurance, even when they pay for health care

Other Employer Components

- Components of non-covered employers can be “covered entities”
  - clinics provided as part of health services
  - on-site nurses offices
- Are treated as separate entities from the employer for purpose of privacy rules

Dual Personalities

- Proposed rules treat a health plan or clinic as a separate entity
- Transfers of protected information from the plan or clinic to the employer is considered a “disclosure”
- Transfers for employment purposes are prohibited in the absence of individual consent

What Disclosures Are Allowed?

- No consent required for disclosures for treatment, payment and healthcare operations purposes
- Broad exceptions that will permit most disclosures necessary for basic operation of plan
- Protection does not follow information
  - Protected information that is properly disclosed to a non-covered employer is no longer protected under HIPAA
- “Minimum Necessary Disclosure” rule

"Payment" and "Health Care Operations" Disclosures

- Comments to proposed rules identify several permitted disclosures to employer
  - disclosure to employer for negotiation of experience rate
  - eligibility, fitness for duty, and coordination of benefits with workers comp
  - utilization management
  - auditing of plans and administrators
  - quality of care studies

Major Question

- Is the contemplated “firewall” between plan and employer realistic?
  - HR office may supply staffing for health plan
  - How can information be divided?
  - Is an employer that provides administrative support a “business partner”?
- Will require further explanation in final rules

Other Question Areas

- Disease management and risk assessment programs
- Coordinated health, disability, and workers comp programs
- Industrial health and safety studies (injury, absenteeism, etc.)

Administrative Requirements

- Designation of privacy official
- Training/Certification
- Security
- Internal complaint process
- Sanctions
- Written policies and procedures

Individual Rights

- Right of Access
- Right to Accounting of Disclosures
- Notice of Information Practices
- Right to Request Amendment and Correction

Business Partner Agreements

- "Business Partners" defined as entities that carry out, assist with, or perform on behalf of, a function or activity for the covered entity
- Key feature is that "the business partner is performing an activity for or on behalf of the covered entity" 64 Fed Reg 59947
- Includes plan administrators, actuaries, etc.
- Is an insurer or HMO a "business partner" of a health plan that provides benefits through a health insurance or managed care contract?

Requirements of Business Partner Agreements

- Restrictions on use and disclosure are passed from party to party as data is transmitted
- Use and disclosure
  - only as provided in contract
  - in accordance with Privacy Standard
- Adequate safeguards to prevent use or disclosure
- Partner must make its privacy practices and records available to HHS for audit
- Partner must make information available in response to patient request
- Partner must incorporate corrections
- Destroy or return data at end of contract

Administrative Burden

- Business partner agreements are intended to pass all limitations and duties of covered entity to its partners
  - Partner can only use data to the extent entity could
  - Partner would be bound by terms of covered entity's notice of privacy practices
    - partners will have to track specific restrictions on data received from multiple sources
  - Partner would have to pass same restrictions to its subcontractors
- Covered entities must
  - make available to patient non-redundant protected information in possession of partners
  - pass corrections and explanations to partners

Responsibility for Business Partners

- Covered entity must take “reasonable steps” to ensure that partner complies with Privacy Standard in carrying out activities for entity
- If entity “knew or should have known” of violation by partner, entity must take corrective action or terminate agreement
  - Failure to take action subjects covered entity to sanctions
- Business partner contracts must state that patients are “intended third party beneficiaries”
  - Creates right in individual to sue for breach of contract

Scalability

- One set of rules for all types of covered entities
  - result is lack of specific guidance
- Small employer that purchases community rated insurance/managed care policy
- Large employer that purchases experience rated insurance/managed care contract
- Large self-insured employer, self or 3rd party administered
- Multi-employer plans

Simplest Plan

- Employer provides benefits through purchase of community rated insurance
  - does not handle claims, no administration
- Does not need or obtain protected information
- Nonetheless, requires written procedures, privacy official, right of access, other administrative requirements
- May be liable for privacy breaches by insurer as “business partner”

Americans with Disabilities Act

- *Cossette v. Minn. Power & Light (8th Cir. 1999)*
- Employee of MP&L applied to US Postal service for a job
- MP&L disclosed to Postal Service that employee had a back injury, resulting in rejection of applicant
- ADA prohibits employer from disclosing results of medical tests and other confidential medical information (42 U.S.C. 12112(d)
- Confidentiality provision applies to ALL employees -- “disability” is not required

International Requirements - European Data Protection Directive

- Comprehensive European personal information privacy regimen
- Prohibits transmission of data outside EU unless recipient country provides “adequate” level of privacy protection
- Important definitions:
  - "personal data" shall mean ***any*** information relating to an identified or identifiable natural person
  - "processing of personal data"shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
- Covers paper records and manual systems as well as computers

Safe harbor principles

- US and EU have agreed on a set of safe harbor principles
- US companies meeting the principles will be able to receive personal data from Europe
- US companies can be listed by Dept of Commerce by self-certifying compliance, or by joining an approved voluntary standards group

Elements of safe harbor

- **Notice** of purpose of collection, intended uses and disclosures and point of contact
- **Choice** - opportunity to opt-out of additional uses or disclosures; opt-in required for any disclosure or further use of “sensitive” data, including health data
- No **Onward Transfer** unless recipient subscribes to safe harbor, or by contract agrees to provide equivalent protections
- Reasonable **Security** to prevent loss, destruction, misuse, or unauthorized access
- **Data Integrity** - must take reasonable steps to ensure data is reliable, and is compatible to intended use
- Right of **Access** to review information, and to correct or delete inaccurate data
- **Enforcement** requires complaint and dispute process. Ultimate enforcement will be under § 5 of FTC Act

US and EU have provided "FAQ"s to address special issues

- FAQ 9 addresses "Human Resources" data
  - Employment data is covered by the Directive
  - Transfer is permitted if US recipient is a safe harbor participant
  - Laws of country in which data was collected must be honored
  - Notice and choice required for unrelated uses
  - Statistical reporting of aggregated data is not affected

Privacy Litigation - A Growing Risk

- So, you say that HIPAA does not provide a private right of action?
- Doe v. Community Health Plan - Kaiser Corp. (May 11, 2000)
  - Clerk disclosed confidential health information at a party
  - NY Appellate Division held:
    - state privacy statutes do not create private right of action
    - *but breach of statutory duty of confidentiality provides basis for tort action*

Three-step analysis

- **Duty -** "[T]he duty not to disclose confidential personal information springs from the implied covenant of trust and confidence that is inherent in the physician-patient relationship, the breach of which is actionable as a tort"
- **Standard -** "While a private cause of action may not be predicated on CPLR 4504, CPLR 4508 or Public Health Law § 4410(2), these statutes define and impose the scope of the actionable duty of confidentiality which arises between certain health care providers, such as CHP, and their patients."
- **Defenses -** "We observe that in the absence of **permission** from the patient, **waiver** or **legal justification**, there is no defense to a cause of action seeking to recover damages for wrongful dissemination of confidences by persons or entities upon whom such duty of protection is imposed."

Other courts have also inferred a duty

- Weld v. CVS (Massachusetts)
  - Class action filed against CVS pharmacy, four drug companies, and marketing firm for use of prescription information in a direct mail program
  - Asserted various statutory and common law claims
  - Court denied defendants' motions for summary judgment and certified Massachusetts class, stating:
    - "Although this court is not aware of any case which holds that pharmacists owe their customers a duty of confidentiality, it is reasonable to infer that a person who imparts private medical and prescription information to a pharmacist expects that such information will be maintained in confidence . . . .

HIPAA rules will provide a new standard of care

- HIPPA privacy and security rules will establish a national standard of care for protection of medical information
- Will provide a basis for state negligence and breach of fiduciary duty suits
- Will likely be applied even to entities that are not HIPAA “covered entities”
  - I.e., state law creates duty of confidentiality; HIPAA regs reflect “reasonable” nationwide standard of care
- Also, draft HIPAA rules contains a “backdoor” right of action in mandatory “3rd-party beneficiary” provision of business partner agreements

Alan C. Brown

McKenna & Cuneo, L.L.P.

Washington, DC

P: 202-496-7386

F: 202-496-7756

alan_brown@mckennacuneo.com