HIPAA Compliance Strategies for Employers, METs, MEWAs and Taft Hartley Union Trust Funds

The HIPAA Colloquium at Harvard University

Presented by: Melissa Davis Hartranft, Esq.
Senior Legal Counsel
Fidelity Investments
August 22, 2002

Agenda

- Privacy Rule
- Fidelity's HIPAA Compliance Strategy
- Q&A

Privacy Rule

- Standards for Privacy of Individually Identifiable Health Information
- Final Privacy Rule
  - Effective: April 14, 2001
  - Compliance required: April 14, 2003
- NPRM: March 27, 2002
- Amendments to Final Privacy Rule
  - Published: August 14, 2002
  - Effective: October 15, 2002

General Rule

"Covered Entities" must not use or disclose "Protected Health Information"

- Without the express permission of the individual to whom it pertains; or
- Except as otherwise explicitly permitted or required by the Privacy Rule.

Protected Health Information (PHI)

- Individually identifiable health information
  - Created/received by a covered entity or an employer
  - Relates to the past, present, or future
    - Physical or mental health consideration
    - Provision of health care
    - Payment for health care
  - Identifies the individual or there is a reasonable basis upon which to believe the information can be used to identify the individual
  - Transmitted or maintained in any form or medium
- Includes demographic information collected from an individual (e.g., city, county, precinct, zip code)
- Specifically excludes individually identifiable health information in
  - Education Records
  - Employment Records held by a covered entity in its role as employer

Covered Entities

- Health plan – an individual or group plan that provides, or pays for the cost of, medical care
  - Group health plans (employee welfare benefit plans under ERISA that provide medical care to employees and their dependents, directly or through insurance, reimbursement or otherwise, that has 50 or more participants or is administered by an entity other than the employer who established the plan)
  - health insurance issuer
  - HMO
  - issuer of long-term care policy
  - employee welfare benefit plan or arrangement established or maintained to offer or provide health benefits to employees of two or more employers

Covered Entities (cont.)

- Health care provider – provider of health services who transmits health information in electronic form
- Health care clearinghouse – entity that receives health information and processes it from non-standard to standard format (or vice versa)
  - billing service
  - community health management information system
- Employers/Plan Sponsors/Employee Organizations are NOT covered entities

Permitted Uses and Disclosures of Protected Health Information

- Some examples of how a covered entity may use or disclose protected health information, as expressly provided under the Privacy Rule, include the use or disclosure:
  - to the individual
  - for:
    - treatment (includes, but is not limited to, provision of health care, consultation between providers and referrals),
    - payment (includes, but is not limited to, activities undertaken to obtain premiums, reimbursements, coordination of benefits and cost sharing amounts), or
    - health care operations (includes, but is not limited to, activities involving quality assessment and improvement and M&A due diligence)

Permitted Uses and Disclosures of Protected Health Information (cont.)

- pursuant to an authorization (use or disclosure must be consistent with authorization)
- as required by law (includes, but is not limited to, law enforcement proceedings, domestic violence and judicial or administrative proceedings)

Minimum Necessary Requirements

- Covered entities must make reasonable efforts to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose
- Exceptions to minimum necessary requirements for uses and disclosures
  - To the individual
  - Pursuant to an authorization initiated by the individual
  - To a provider for treatment purposes
  - To the Secretary of HHS for enforcement
  - Required for compliance or required by law
- A covered entity may reasonably rely upon another covered entity's request (or the request of a business associate on behalf of a covered entity) for PHI as the minimum necessary for the intended disclosure

General Obligations

- Covered Entities must:
  - Limit use and disclosure of Protected Health Information (PHI)
  - Permit individuals to access and modify their PHI, and to obtain an accounting of disclosures (accounting does not include disclosures for treatment, payment or health care operations; pursuant to an authorization; made to the individual; or pursuant to any other authorized use or disclosure)
  - Contract with Business Associates
  - Develop policies, training, sanctions, and complaint processes
  - Draft notices, consents and authorizations
  - Designate a Privacy Officer

Business Associates

- A person who performs services for or on behalf of a covered entity involving the use disclosure of PHI (including, but not limited to, claims processing, data analysis, utilization review, quality assurance, billing)
  - Lawyers
  - Accountants
  - Auditors
  - Actuaries
  - Consultants
  - Administrators
  - Other
- Contract required to assure PHI is safeguarded and used only as permitted
- Sample contract language in NPRM and minor modifications contained in amendments to Final Privacy Rule

Employers/Employee Organizations as Plan Sponsors

- No clear compliance framework
  - Employers/Employee organizations are not covered entities
  - Group health plans/Employee welfare benefit plans maintained for two or more employers are covered entities
  - Self administered plans do not operate themselves

Group Health Plan's Disclosure of Protected Health Information

General rule: Group health plan cannot disclose PHI to the plan sponsor (or to provide for or permit the disclosure of PHI by a health insurance issuer or HMO with respect to the group health plan), unless the plan document restricts the uses and disclosures of such PHI by the plan sponsor

Exceptions:

- Group health plan may disclose *summary health information* to the plan sponsor if the plan sponsor requests the information to:
  - obtain premium bids from health plans for providing health insurance coverage under the group health plan, or
  - modify, amend or terminate the group health plan
- Group health plan may disclose to the plan sponsor an individual's participation *or enrollment/disenrollment* status
- Group health plan may disclose PHI to a plan sponsor pursuant to an authorization

Fidelity's HIPAA Compliance Strategy

- Fidelity, as an employer and plan sponsor, is not subject to HIPAA because it is not a covered entity. Therefore, the first step in the compliance strategy is to identify the covered entities that are subject to HIPAA:
  - Medical plans (including prescription drug)
    - Fully insured HMOs
    - Self-insured PPO
  - Flexible Spending Accounts
  - Employee Assistance Program
  - Dental plan
  - Long-Term Care plan
  - Retiree Medical plan
- Other practices/programs to consider

Fidelity's HIPAA Compliance Strategy (cont.)

- After identifying the covered entities, the next step in the compliance strategy is to document the current flow of PHI:
  - how/where PHI currently is used and disclosed by each covered entity
  - how/where PHI currently is used and disclosed by Fidelity
  - how/where PHI is used and disclosed by outside vendors

Fidelity's HIPAA Compliance Strategy (cont.)

- While documenting the current flow of PHI, the following factors also are taken into account and analyzed:
  - Evaluate security (both internal and external)
  - Assess personnel needs for PHI (department(s) within the company, employee hierarchy)
  - Determine whether certain practices currently are in place to address State law requirements

Fidelity's HIPAA Compliance Strategy (cont.)

- The next step in the compliance strategy involves taking an inventory of existing contracts with outside vendors to determine which ones will need to be amended to include business associate language and the timing of such amendments
- In addition to existing contracts, it also is necessary to determine whether there are existing relationships that will need to be memorialized into business associate agreements in light of HIPAA

Fidelity's HIPAA Compliance Strategy (cont.)

- Other steps that will need to be taken include:
  - Amending plan documents and drafting certifications
  - Establishing/fortifying firewalls
  - Building systems for tracking and accounting for uses and disclosures of PHI
  - Drafting authorizations (no consents)
  - Amending contracts to include business associate sample language

Fidelity's HIPAA Compliance Strategy (cont.)

- Drafting policies and procedures
  - Use, transfer, retention of PHI
  - Complaints, sanctions
  - Privacy notice
- Training associates (ongoing)
- Sending privacy notices