HIPAA and Employer Group Health Plans: *Nothing is Simple*

Beth L. Rubin
March 26, 2003

HIPAA Applicability

- Health Plans -- including employer group health plans
- Health Care Providers -- that transmit any health information in electronic form
- Health Care Clearinghouses

Health Plan Definition

- "Health plan" is broadly defined:
  - An "individual or group plan that provides, or pays the cost of, medical care"
    - Includes most ERISA employer welfare benefit plans, insured and self-funded, plus some non-ERISA plans

Privacy Rule Chronology

- Proposed Rule: November 1999
- Final Rule: December 2000
- Comment period: March 2001
- Proposed Changes: March 2002
- Final Final Rule: August 2002
- Guidance released: December 2002
- Compliance Date: April 14, 2003 (large plans)
- Compliance Date: April 14, 2004 (small plans)

Health Plans

- **Health plans must comply with all the Privacy Standards that apply to Providers, *plus* certain Standards applicable only to health plans**

Health Plans

Health Plans must comply with:

- Restrictions on Uses and Disclosures of PHI
- Plan Member Rights Requirements
- Administrative Requirements
- Firewall Requirements – Separation between the plan and plan sponsor

Restrictions on Uses and Disclosures

- Covered entities may not use or disclose PHI, except as permitted or required under the Standards
- Treatment, payment, and health care operations (TPO)

Restrictions on Uses and Disclosures

- Authorizations
  - For uses and disclosures not otherwise permitted by the rule
  - Authorizations are necessary for some, but not all, purposes other than TPO
  - Authorization content -- core elements

Restrictions on Uses and Disclosures

- "Minimum Necessary" Standard
- Business Associate Requirements, including re-contracting
- De-identification requirements
  - limited data set

Uses and Disclosures without Authorization or Opportunity to Agree

- Certain public health authorities
- Government authorities authorized to receive reports on child abuse or neglect
- FDA reporting, tracking and surveillance

Uses and Disclosures without Authorization or Opportunity to Agree

- Health oversight activities
- Judicial or administrative proceedings
- Law enforcement

Business Associate Definition

- A person who, on behalf of a covered entity, performs a function involving the use or disclosure of IHI

  (includes claims processing, data analysis, utilization review, quality assurance, billing, benefit management, and repricing)

OR

Business Associate Definition

- A person who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, where this service involves disclosure of IHI

Liability

- A health plan may be found liable if:
  - the plan "knew" of a pattern of activity of a business associate that violates the business associate's obligation under its contract with the plan, unless the plan took reasonable steps to end the violation

Liability

- If such steps were unsuccessful, the plan
  - Terminated the contract, if feasible, or
  - If termination was not feasible, reported the problem to the Secretary of DHHS

Business Associate Contracts

- **"Satisfactory assurance" requirement**
  - **Plans must have contracts with business associates that include many specified terms**

    (includes plan administrators)
  - **Transition period**

Member Rights

- Right to Notice of Privacy Practices
  - Strict content requirements
  - Self-funded plans must provide notice to members by the compliance date
    - After compliance date, to new members at the time of enrollment

Member Rights

- **Notice**
  - **Insured plans that do not create or receive PHI -- notice is provided by insurer/HMO**
  - **Insured Plans that create or receive PHI must maintain a notice and provide it upon request**

Member Rights

- Right to request restrictions on uses and disclosures
  - Plans are not required to agree to requested restrictions
  - More confidential mode of communication

Member Rights

- **Right to access PHI**
  - **Members have the right to access, inspect, and copy their health information**
  - **Strict deadlines and procedures**

Member Rights

- Right to amend PHI
  - Plans may deny requests for amendment if the PHI:
    - Was not created by the plan;
    - Is accurate and complete

Member Rights

- Right to an accounting of *certain* disclosures of PHI made by plan during the previous 6 years
  - Exceptions

Administrative Requirements

- Appoint a privacy officer
- Designate a contact person or office responsible for receiving privacy-related complaints

Administrative Requirements

- Plan workforce training
  - Policies and procedures
  - Retraining -- if the policies and procedures change materially
  - Documentation
  - Combine with Security training

Administrative Requirements

- **Privacy safeguards**
  - **Install appropriate administrative, technical, and physical safeguards**
  - **Scalability**
  - **Intersection with Security Rule**

Administrative Requirements

- Complaints
  - Process
  - Documentation

Administrative Requirements

- **Sanctions**
  - **Establish and apply appropriate sanctions against plan workforce members who violate the plan's privacy policies and procedures or the Privacy Standards**

Administrative Requirements

- **Mitigation**
  - **Mitigate, if practicable, any harmful effect resulting from a violation of the plan's policies and procedures or the Standards**

Administrative Requirements

- **Privacy policies and procedures**

Firewall Requirements

- HIPAA applies to health plans, not plan sponsors
- For this reason, the Standards focus on plans, and force plans to impose certain requirements on plan sponsors

FIREWALL REQUIREMENTS

- Right brain vs. Left Brain
  - Brain firewall
- Right hand vs. Left Hand
- Wearing different hats while performing different functions
- Is training important?

Firewall Requirements

- **Plan sponsors may access identifiable health information only for plan administration purposes**

Firewall Requirements

- **Plan sponsors may NOT access PHI for employment-related actions without written permission from the plan member**

Firewall Requirements

- **Recent Clarification:**
  - **Employment records are not considered Protected Health Information**

Firewall Requirements

- **Plan Documents**
  - **If Plan Sponsors receive PHI other than summary and enrollment/disenrollment information, they must amend their plan documents to include specified terms**

Firewall Requirements

- **Exceptions: Group health plans may give plan sponsors:**
  - **Summary health information**
  - **Enrollment/Disenrollment information**

Firewall Requirements

- **Summary Information (mostly de-identified) may be disclosed to a plan sponsor for the purpose of**
  - **Obtaining bids**
  - **Modifying, amending, or terminating the plan**

Plan Documents

- **GHP may disclose PHI to the PS only upon receipt of a certification that the plan documents have been amended to include the following:**
  - **Permitted and required uses and disclosures of such information by PS**

Plan Documents

- **PS agrees not to use or further disclose the information other than as permitted or required by the plan documents or as required by law**

Plan Documents

- PS agrees to ensure that any agents, including subcontractors, to whom it gives PHI agree to the same restrictions

Plan Documents

- **PS agrees not to use or disclose PHI for employment-related actions or in connection with any other benefit or employee benefit plan**
- **PS agrees to report to GHP any use or disclosure inconsistent with these requirements**

Plan Documents

- **PS agrees to make available PHI for employee access, amendment, and accounting rights**
- **PS agrees to make its internal practices and records relating to the PHI available to DHHS for determining Plan's compliance with the Standards**

Plan Documents

- **When no longer needed, PS agrees to return or destroy all information received from GHP**
  - **If not feasible to return or destroy the information, PS agrees to limit any further uses and disclosures of the information**

Plan Documents

- **Plan documents also must establish "adequate separation" between the GHP and PS by**
  - **Describing those employee positions (or other persons under control of PS) who may access the information**
    - **Individuals who use identifiable information relating to payment or health care operations of GHP**

Plan Documents

- **Restrict access to and use by such employees and other persons to the plan administration functions that the PS performs for the GHP**

Plan Document

- Plan documents also must provide an effective mechanism for resolving issues of noncompliance by those designated persons

Firewall Requirements

Reminder:

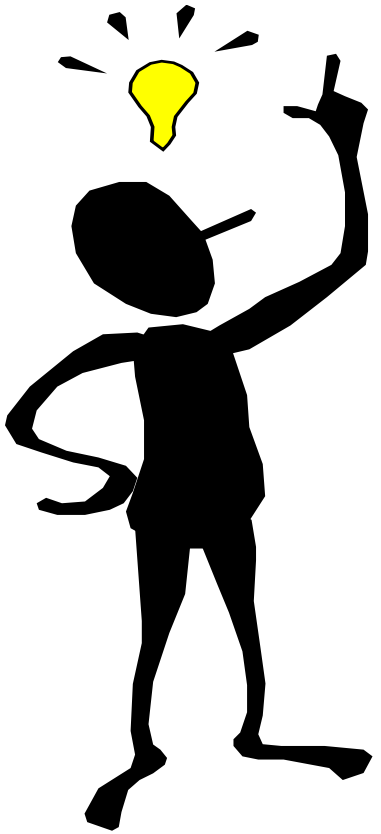
- **Written authorization from the member is required for disclosure of PHI to a plan sponsor for**
  - **Employment-related actions**
  - **Actions relating to any other benefit or plan maintained by the plan sponsor**

Insured Plans

- **Insured plans that do NOT receive PHI (other than summary and enrollment/disenrollment) are exempt from many requirements, including:**

Insured Plans

- **Exempt from:**
  - Privacy officer
  - Workforce training
  - Privacy safeguards
  - Complaints
  - Workforce sanctions
  - Mitigation



Insured Plans

- **Exempt from:**
  - **Policies and procedures**
  - **Notice of privacy practices**
  - **Patient rights of access, amendment and accounting**

  Why? Individuals enrolled in these plans have these rights through the insurer/HMO

Insured Plans

- Do you create or receive PHI?
  - From the Administrator/Insurer?
  - From Plan members?
    - E.g., Assistance with claims
    - Keep plan sponsor employees outside the Plan firewall

GHP Action Plan

- Develop a HIPAA Group Health Plan privacy [and security] action plan
  - Phases may include assessment, strategic analysis, and implementation

GHP Action Plan

- Outline discrete tasks for each phase, including re-negotiating business associate contracts
- Set timelines

Initial Documents

- Inventory/Assessment Questionnaires?
- Plan document amendments
- Policies and Procedures
- Notice of Privacy Practices
- Forms/Logs

Policies and Procedures

- What types of Plan policies and procedures are needed?
  - Overall privacy policy addressing handling of PHI and "adequate separation"
    - Must be consistent with plan documents
    - May address "minimum necessary" standard

Policies and Procedures

- Plan member rights (detailed)
- Plan Member Privacy Complaints
- Plan Workforce Training
- Privacy-related Workforce Sanctions

Policies and Procedures

- Policy on Safeguards for Protecting PHI -- detailed
- Policy on Plan Documentation and Retention of Certain Records
- Policy on Authorizations (including Authorization form)

Do's and Don'ts of Policy Drafting

- Avoid overly broad, absolute pronouncements about security and privacy
  - Avoid extraneous detail
  - Avoid overstating protections and safeguards
    - Never "ensure"

Do's and Don'ts of Policy Drafting

- Allow flexibility for practice variation and innovation if permitted under the Privacy Standards
- Do not adopt a policy or procedure that will not be, or is not capable of being, implemented

Selected Issues

- Telephone inquiries from spouses/others regarding a member's benefits/claims
  - Systems issue
  - Customer service problem
  - Employee/union issues
  - Creative solutions

Selected Issues

- What is the Plan workforce? Which employees are Plan workforce members?
  - Consequences/potential liability related to wearing two hats
  - Training and workable sanctions
  - Clear policies and procedures

Selected Issues

- Notice of Privacy Practices
  - Self-funded plans must send this notice soon
  - Will the TPA also be sending a notice?
    - Will plan members get two different notices with different privacy complaint contacts?

Selected Issues

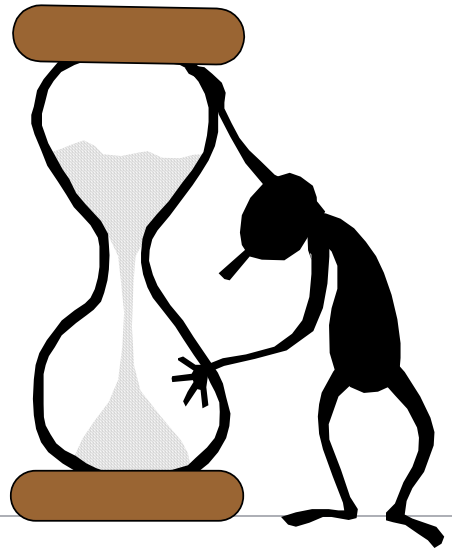
- Re-negotiation of third party administrator agreements
  - Add required business associate terms
  - Consider adding/modifying other related terms
  - Transition period

Selected Issues

- Can a self-funded Plan use a TPA for all required tasks and not have policies and procedures, privacy officer, etc?
  - No -- You can delegate tasks, but can't delegate all HIPAA responsibilities

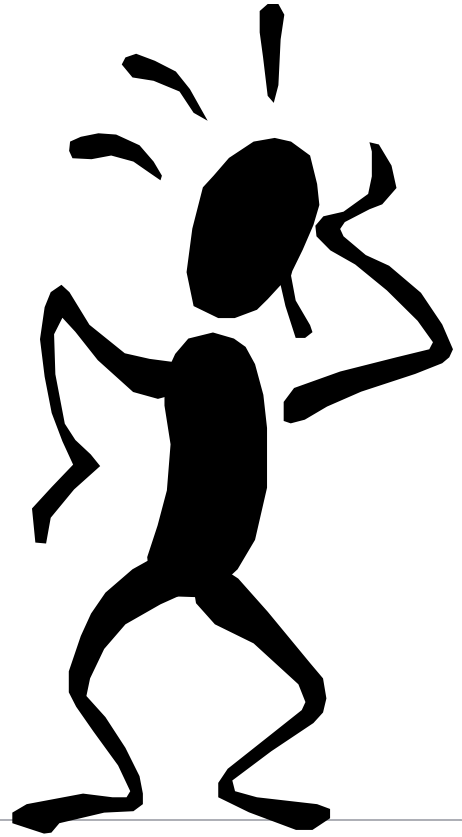
Compliance Dates

- **Small health plans (with annual receipts of $5 million or less)**
  - **April 14, 2004**
- **Other (not small health plans)**
  - **April 14, 2003**



Penalties

- **Violating the privacy rule can create both civil and criminal liability**
  - **“Nice HIPAA”**
  - **“HIPAA for crooks”**



Penalties

- **Civil penalties: $100 per violation**
  - **Capped at $25,000 per person, per year, per standard**

Penalties

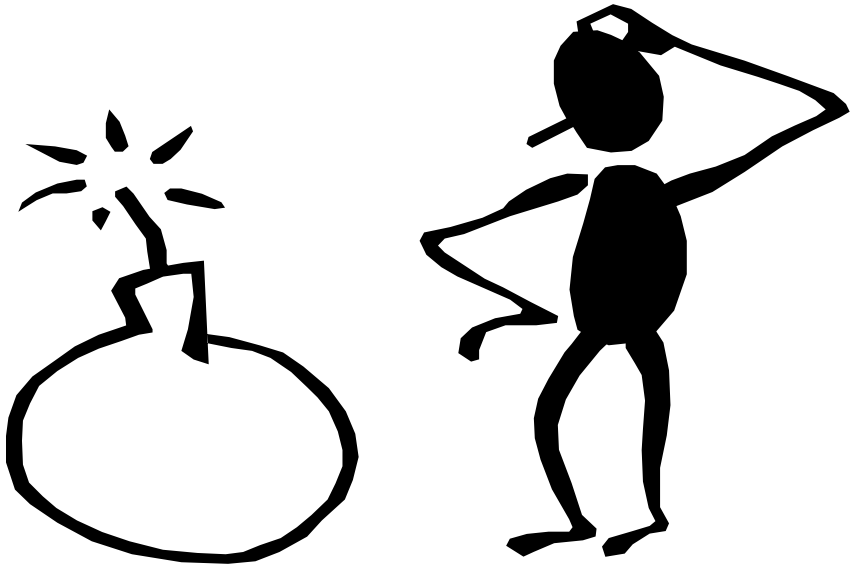
- **Criminal penalties: up to $250,000 and prison sentences of up to 10 years, if:**
  - **Offense is committed with an intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm**

Case Law

- In May 2001, a federal judge noted that although compliance is not required until April 2003, the HIPAA privacy regulations are "persuasive in that they demonstrate a strong federal policy of protection for patient medical records." *U.S. v. Sutherland*
- The judge applied the HIPAA regulations to that case
- Another judge recently did the same

Enforcement

- **A new "standard of care" for how health plans (employers) should handle identifiable health information?**



Beth L. Rubin
Dechert LLP
4000 Bell Atlantic Tower
1717 Arch Street
Philadelphia, PA 19103

beth.rubin@dechert.com
215.994.2535