The HIPAA Colloquium
Harvard University
August 22, 2002

HIPAA Compliance Strategies for the Pharmaceutical Industry

John T. Bentivoglio
202.942.5508
john_bentivoglio@aporter.com

Overview

- Obtaining Management Support -- Stressing Legal and Business Drivers
- Initial Assessment of Information Practices and Procedures
- Development of Business Plan
- Specific Compliance Tips

Securing Management Support

- Focus on the legal ***and*** business drivers -- too many privacy professionals focus solely on legal/regulatory mandates

- Business drivers:
  - Key customers and partners are covered under new Federal health privacy law (HIPAA)
  - Many customers and business partners are pushing to impose privacy safeguards via contract
  - Other customers may simply refuse to share information used in important activities, particularly in sales/marketing area

Business Drivers (cont'd)

- Sales and marketing (examples):
  - Current activities (*e.g.,* preceptorships, chart pulls) may need to be restructured to address privacy rules, some changes may be impractical
  - Sales reps may get resistance from physicians (*e.g.,* prohibiting them from coming into the "back office" where personal health information could be seen or overheard)
  - Disease management programs with healthcare providers (*e.g.,* hospitals, health systems) may need to be modified to comply with authorization requirements
  - Some customers (*e.g.,* hospitals) are requiring pharmaceutical manufacturers to sign contracts obligating them to establish privacy safeguards, indemnify the customer for violations
- Practical implications (particularly authorizations)

Business Drivers (cont'd)

- Clinical research (examples)
  - To share information with sponsors, investigators will be required to provide notice, obtain authorization from patients enrolled in clinical trials
  - Current informed consent forms may need to be modified
  - Current procedures regarding de-identification of data (*e.g.,* assigning codes in lieu of patient names) will need to be modified
  - Notice/authorization may make patient recruitment more difficult
  - Procedures under which data is obtained from clinical trials in Europe may need to be modified under EU Privacy Directive

Business Drivers (cont'd)

Other impacts

- Certain functions (*e.g.,* on-site health clinics, ERISA health plan) may be covered under HIPAA -- requiring designation of privacy officer and establishment of privacy safeguards

Reputational harm

- Example: As a result of an email mistake (involving 600 individuals using prozac.com website) Eli Lilly & Co. is now the "poster child" for misuse of sensitive personal information by the private sector (in addition to onerous FTC settlement)

Legal Drivers

- HIPAA (including criminal provisions)
- Other Federal Laws
- State Laws, Attorneys General
- Private litigation

Initial Assessment

- Scope and purpose
  - Domestic vs. international
  - Potential areas: sales/marketing, clinical research, regulatory affairs, human resources, e-business activities
  - The assessment can be a means to (1) collect information, (2) increase awareness, (3) identify potential privacy advocates/supporters
  - Support development of business plan for privacy program

- Methodology
  - Steering Committee or Task Force (sales/marketing, clinical research, regulatory affairs, human resources, e-business activities, public affairs, finance, contracting)
  - Written surveys (benefits, limits)
  - Collection, analysis of existing policies/procedures
  - Leverage current efforts (particularly Part 11 initiatives)

Initial Assessment (cont'd)

- Use of outside professional services
  - Benefits:
    - can provide needed expertise;
    - may be necessary where internal resources/people are not available
    - outside "experts" may be influential in convincing management to devote resources (management time, financial, etc.) to privacy program
  - Limits:
    - Beware of firms trying to sell you their last privacy assessment
    - Excessive reliance on outside advisers can result in missed opportunities for CPO to promote privacy, identify potential internal allies

Business Plan for Privacy Program

- Benefits of a "business plan"
  - Can foster management support
  - Establishes expectations, responsibilities
  - Identifies the key needs that can make or break a privacy program (e.g., resources)

- Key elements (examples)
  - Roles/responsibilities of CPO, Privacy Task Force
  - Overall goals and objectives
  - Specific goals and objectives in key areas (sales/marketing, clinical research, etc.)
  - Policies and procedures
  - Training
  - Resources
  - Timetable and milestones

Special Compliance Tips -- Business Associates

- Under HIPAA, “business associates” are entities performing activities “on behalf of” covered entities
- Disclosures of PHI to pharmaceutical companies pursuant to business associates agreements may not be permissible under HIPAA
- Some customers (*e.g.,* hospitals, health systems) are requiring business associate agreements even where no PHI is disclosed
- Consider developing “templates” for addressing privacy issues with your customers -- and raise these issues in advance, rather than in the late stages of contract negotiations

Special Compliance Tips -- Sales and Marketing

- Some activities -- *e.g.,* preceptorships -- may need to be discontinued
- Analyze whether sharing is necessary for treatment, payment, or operations -- may be permissible in some consulting contexts, particularly for medical device manufacturers
- Develop authorization language for covered entities that would allow sharing in appropriate circumstances
- Consider working with local or state medical societies that are drafting model authorizations for their members

Resources

- Government resources:
  - HHS Office for Civil Rights (responsible for enforcement of HIPAA rule)-- www.hhs.gov/ocr/hipaa
- Professional/trade associations
  - American Health Information Management Association (AHIMA) -- www.ahima.org
  - Health Care Compliance Association (HCCA) --www.hcca-info.org
  - International Association of Privacy Officers (IAPO) -- www.privacyassociation.org (which was established a Pharmaceutical Working Group)