BUILDING YOUR PRIVACY PROGRAM:

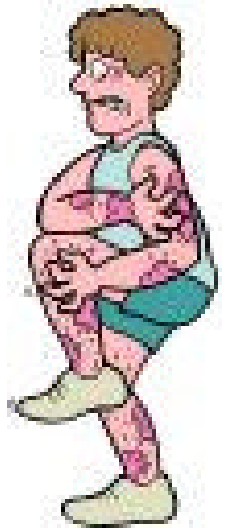
A Primer for Pharmaceutical and Device Companies

Stephen W. Bernstein, Esq.
McDermott, Will & Emery
28 State Street
Boston, MA 02109
(617) 535-4062
sbernstein@mwe.com

What's Out There Regulating You?

What can bite you in terms of improper disclosure of data?

- State Laws
- European Union
- Federal Laws
  - Federal Privacy Act
  - FTC Standards for Internet
  - Children's Online Privacy Protection Act
  - Gramm-Leach-Bliley Act
  - HIPAA



European Union Directive/U.S. Department of Commerce

- EU Directive on Data Protection - October 25, 1998

  Transfer of personal data may occur to non-EU countries that provide "adequate" level of privacy protection
- Safe Harbor Privacy Principles
  - Notice
  - Choice (Opt Out)
  - Onward Transfer
  - Security
  - Data Integrity
  - Access
  - Enforcement

European Union Directive/U.S. Department of Commerce

- Specific Application to Pharmaceutical and Medical Products
- Frequently Asked Questions - 14

  (see www.export.gov/safeharbor/FAQ14PharmaFinal.htm)
  - Collection of personal data in Europe, transferred to U.S.
  - Re-use of data
  - Use of data from subjects who have withdrawn from study
  - Data from European trials and disclosure to U.S. regulators
  - “Blinded” studies and access to data by research subjects
  - Application of Safe Harbor Principles to product safety/efficacy monitoring
  - Transfers of “key-coded” data from EU to U.S.

HIPAA: Remember Who You Are

How could I be covered by HIPAA?

- Provider
- Hybrid Entity
- Business Associate

Why Do I Care About Privacy?

- In re Pharmatrack Communications Litigation

  United States District Court, Southern District NY (January 23, 2001)
- Quintiles Transnational Corp. v. WebMD Corporation

  United States District Court, Eastern District NC

  (March 20, 2001)
- Anonymous v. CVS Corporation

  New York Supreme Court (Reported New York Law Journal (April 4, 2001))
- Weld, et al. v. Glaxo Wellcome, Inc.

  Massachusetts Supreme Judicial Court (May 1, 2001)
- Civil and Criminal Penalties

  Up to $250,000, 10 years imprisonment or both

Finding Yourself and Who You Are

- Are you a Covered Entity? If so, may not use or disclose protected health information, except as permitted by HIPAA
- Covered Entity: A Provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA
- Provider: Includes any other person or organization who furnishes, bills, or is paid for health care in the normal course of business
- Health Care: Includes sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription

Are You Hybrid Entity or a Business Associate?

- Hybrid Entity: A covered entity whose covered functions are not its primary functions.

- In Pharma Context: If company is paid for care management services, drugs or supplies pursuant to a prescription -- likely to be Covered Entity

You are likely to be a Business Associate

- On behalf of such covered entity. . . performs, or assists in the performance of:
  - a function or activity involving the use or disclosure of individually identifiable health information including. . . data analysis. . .benefit management; or
  - provides. . .data aggregation, management, administrative. . .services to or for such covered entity

Agreements with Business Associates

- Agreements between a Covered Entity and a business associate must provide that the business associate shall:
  - Only use or disclose PHI as permitted (i) under the agreement and (ii) by Covered Entities under the Final Rule
  - Use "appropriate safeguards" to prevent use or disclosure of PHI except as permitted by the agreement
  - Report any known misuse of PHI to the Covered Entity

Agreements with Business Associates (cont'd)

- A business associate must also agree to:
  - Impose the same requirements on its subcontractors and agents
  - Make PHI and an accounting of disclosures available to individuals as required by the Final Rule
  - Make its internal practices, books and records relating to use and disclosure of PHI available to DHHS

Agreements with Business Associates (cont'd)

- Agreements with business associates must also provide that:
  - The Covered Entity may terminate the agreement if the Covered Entity determines that the business associate has breached a material term of the agreement
  - Upon termination of the relationship, the business associate will return or destroy all PHI, if feasible (or extend the protections)

The "Brother's Keeper" Rule

- A material breach by the business associate of its contractual requirements will be considered noncompliance by the Covered Entity if the Covered Entity:
  - Knew of such breach and
  - Failed to take reasonable steps to cure the breach or terminate the agreement (or report to DHHS if termination is not feasible)

The "Brother's Keeper" Rule (cont'd)

- Practical Strategies
  - Start to review multi-year contracts for compliance and include provisions in new contracts
  - A contract addendum may be the easiest way to achieve compliance
  - Have two versions of contract language for use as a Covered Entity or a business partner
  - Limitations of liability may need exceptions for HIPAA violations
  - Review insurance coverage exceptions

Lines of Business -- and why you really care about Privacy

- Reimbursement Counseling and Patient Assistance Programs
- Disease Management
- Website Marketing
- Sponsored Research

Reimbursement Counseling

- Issue: Pharmaceutical companies often assist covered entities in assisting patients to obtain coverage for expensive drugs and devices
- Result: Covered entities need to disclose protected health information to company, thereby making Company a business associate of the covered entity
- Practical Problem: Often occurs in urgent situations, providers don't fully understand the availability of this assistance, and entering into a written contract may be difficult in the time frame available
- Solution: Unless regulations are modified, Pharma companies might consider developing their own form of business associate agreement and offer it to Covered Entities

Disease Management

- Issue: Where do disease management companies and their activities fit within HIPAA? Are disease management companies providers?
- Response: Disease management activities fall within "health care operations" or with respect to an individual the activities fall within "treatment."

  Unclear whether disease management companies are indeed providers. Specific activities need to be examined, and a determination made as to whether "standard transactions" are made electronically by the company
- Action Step: Need to evaluate specific activities. Determine whether you or another entity has obtained consents to disclose information to you. Determine if you are conducting standard transactions.

Marketing and Websites

- Issue: If you are a covered entity or a business associate of a covered entity, and you obtain protected health information, there will be limitations on how information is used for marketing
- Rules:
  - Not marketing if covered entity:
    - –describes plans coverage, or
    - –communication is tailored to circumstances involving
      - treatment of individual
      - purpose of recommending to individual treatment alternatives, therapies, health care providers, etc.
    - –oral communication
    - –written communication, but covered entity does not receive direct or indirect remuneration from third party for making the communication

Marketing Rules (continued)

- Covered entity may not disclose protected health information for marketing without an authorization, except:
  - –If communication occurs face-to-face;
  - –Concerns products or services of nominal value; or
  - –Concerns health related products and services of the covered entity or of third party, and
    - communication identifies covered entity
    - prominently states it will receive remuneration for making the communication, and
    - describes how patient can opt out of receiving future communications

Targeted Marketing

- If protected health information is used to target individuals based on health status:
  - Covered entity must determined in advance that product is beneficial to targeted class or individual
  - Communication must explain why individual has been targeted
  - Covered entity must make reasonable efforts to ensure that individuals who elect not to receive future communications in fact don't receive them

Marketing Filtered through Websites

- In addition to HIPAA - be mindful of other website regulatory hurdles:
  - Fair Information Practices
  - Child's Online Privacy Protection Act
  - Gramm-Leach-Bliley
- Hi Ethics Principles
  - Privacy Policy; Fair Information Practices
  - Enhanced protection for health related personal information
  - Safeguard info with third parties
  - Disclosure of ownership and financial sponsorship
  - Identification of Advertising
- Government "Surf" Days

Marketing Action Steps

- Remember who you are
  - A covered entity or a business associate
- Watch what information you collect and how you use it
- What consents have you obtained? Paper or electronic? Mandatory click-through Agreement?
- Do your pharmacy compliance and refill reminder programs qualify for certain marketing exceptions? If not, have you obtained a written authorization?

Special Issues for Research

- The privacy standards for PHI will affect Covered Entities' research, and indirectly, affect pharmaceutical companies and medical device companies who sponsor research
- Three pathways for Covered Entities' disclosure of PHI to sponsors of research:
  - Pursuant to an Authorization (§ 164.508(f))
  - Pursuant to a Waiver of Authorization from an IRB or new Privacy Board (§ 164.512(i))
  - De-identification (§ 164.514(a))
    - Removal of 18 identifiers (safe harbor)
    - statistical conclusion "very small" chance of identifying subject

Authorization

- An authorization for use and disclosure of PHI must be obtained for research that includes treatment of individual subjects, including a description of the extent to which PHI will be used
  - Existing consents are grandfathered
- This pathway would apply to most prospective clinical research studies
- Authorization may be included with:
  - Consent to participate in research
  - Consent to use or disclose PHI for treatment, payment or health care operations
  - Notice of privacy practices

Exception for FDA Reports

- There is an exception to the authorization requirement for disclosure to pharmaceutical companies and medical device companies (as persons subject to the jurisdiction of the FDA) to:
  - report adverse events
  - enable product recalls
  - track products (as FDA-required)
  - conduct post-marketing surveillance (as FDA-required)

Research: Authorization Not Required When . . .

- Under certain circumstances, disclosure of PHI for research is permitted without an authorization:
  - pursuant to a waiver from IRB or new Privacy Board
  - for review of PHI necessary to prepare a research protocol
  - the disclosure is sought solely for research on decedents
- The waiver pathway likely would be used for retrospective studies involving medical record reviews

Waiver of Authorization

- To grant a waiver, the IRB or Privacy Board must find that:
  - disclosure involves no more than minimal risk to the individual who is the subject of PHI
  - research could not practicably be conducted without PHI or waiver
  - privacy risks are reasonable in relation to anticipated benefits to the individuals and the importance of the knowledge that may reasonably be expected to result from the research
- To grant a waiver, the IRB or Privacy Board must find that:
  - there is an adequate plan to protect PHI from improper use and disclosure and to destroy identifiers at the earliest opportunity consistent with the conduct of the research
  - PHI will not be reused or disclosed to any other person (except as required by law or for authorized oversight of the research project)

Privacy Rules Will Impact How Research Is Conducted

Action Steps:

- Informed consents for clinical studies will need to conform to requirements for authorizations for research; IRBs will need to review/approve
- IRBs will need to review/approve waivers of authorization
- May be difficult to meet de-identification "safe-harbor" for database research; waivers may required

Getting Your Arms Around Privacy

- Consumer demand for privacy protections is here -- you need to deal with them
- Research subjects expect protection
- Consumers, if they haven't already, will come to expect protection
- Assess Your Own Business
  - Remember who you are
  - Analyze what is required one business line at a time
  - Be sensitive to how you use data
  - Get consents and authorizations that are specific but user friendly