Privacy compliance:

An approach for multinational pharmaceutical companies

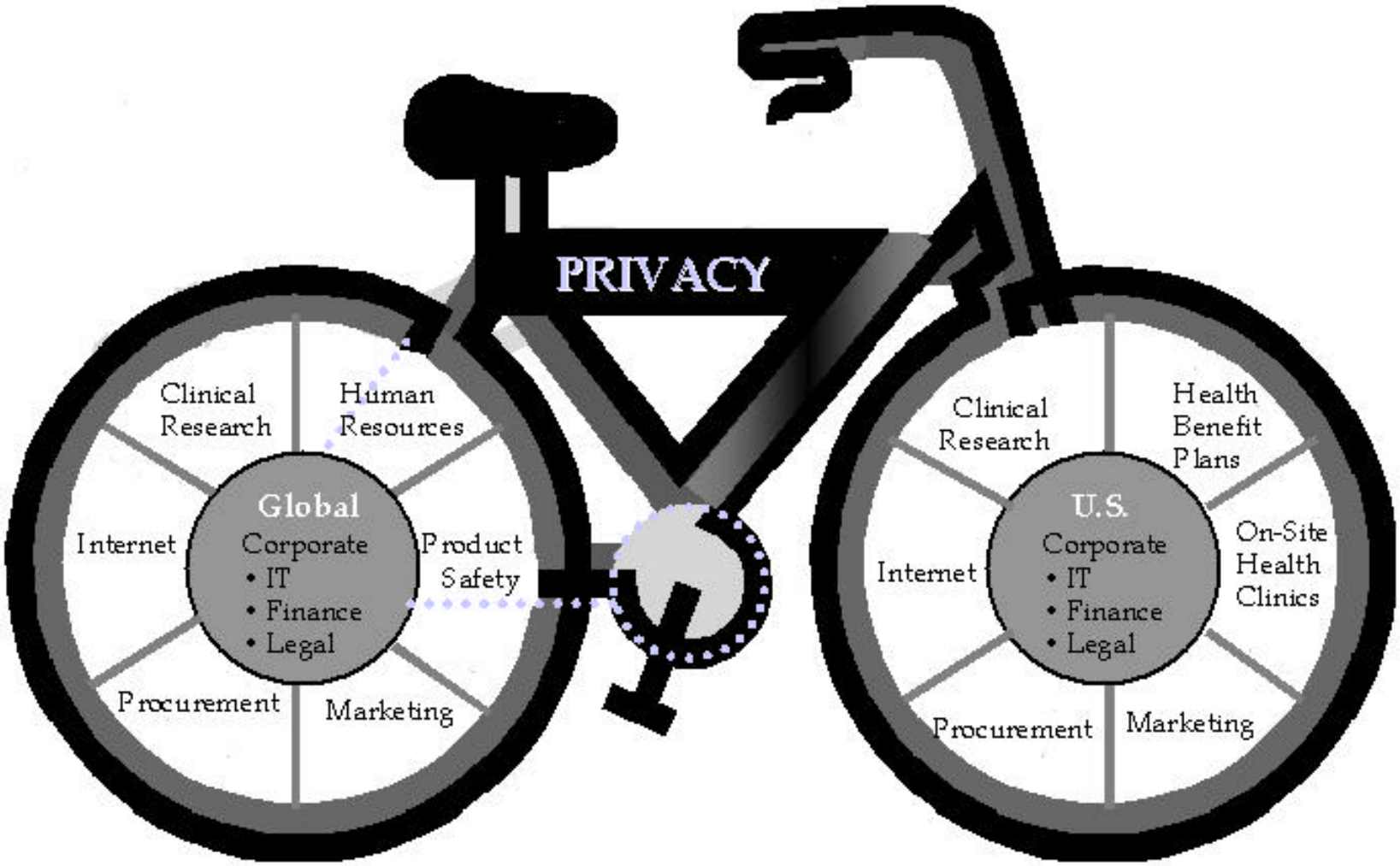
Presentation to the 5th Annual National Congress on Health Care Compliance

Preconference I, February 6, 2002

Hilary B. Schock

Assistant Privacy Officer, Merck Privacy Office

Business scope of privacy impact within a multinational pharmaceutical company



Merck Privacy Office (MPO): Business Model

- Centralized Coordination, Local Ownership
  - Flexibility necessary to support Merck's different businesses, cultures and legal regimes
  - Business units must own and plan for privacy
  - MPO a partner and resource to business units
- Small Staff with Strong Expertise Regarding
  - Merck's businesses
  - Global privacy and data protection issues and their impacts on Merck
  - Identification and coordination of pragmatic business solutions

Global Legal Framework

- HIPAA
- EU Data Protection Directive
- Worldwide national privacy and data protection laws in 40+ countries
- FTC Enforcement of online privacy policies

Legal Framework: HIPAA

- HIPAA
  - Privacy Standards [Deadline: April 14, 2003]
    - "Hybrid Entity" designation
    - Covered entities
      - On-site Health Clinics and "Business Associates"
      - Health Benefits Plans and "Business Associates"
    - Clinical investigators will have to obtain authorizations or IRB waiver to share the protected health information of clinic subjects with pharmaceutical sponsors
    - Marketing information may only be obtained from covered entities pursuant to an authorization or through deindentification.

Legal Framework: HIPAA

- HIPAA (cont'd)
  - Transaction Standards [Deadline: October 16, 2002 to comply or to file a plan with DHHS]
    - Health benefit plans are required to have the capacity to conduct transactions in the standard electronic format
    - On-site clinics may continue to conduct transactions on paper, but to the extent that transactions are conducted electronically, they are require to be implemented in the standard formats
    - Options: internal compliance, trading partner agreements
  - Security Standards [proposed rule]
    - requires administrative procedures and physical and technical safeguards [authentication, authorization, audit trails]

Legal Framework: EU Directive

- EU Data Protection Directive
  - Notice and consent to process personal data (Articles 7 and 10)
  - Explicit consent to process sensitive data (Article 8)
  - Limitations on transborder data flows (Articles 25 and 26)

    Tools: Safe Harbor, Consent, Model Contracts, Anonymization
  - Processor agreements(Article 17)

  Major Impacts:

  ⌫ Clinical studies conducted in European Economic Area

  ⌫ Collection and use of employee information

  ⌫ Collection and use of customer and investigator information

  ⌫ Websites and other e-business programs

  ⌫ Arrangements with third party entities that perform services on the company's behalf.

Legal Framework: Worldwide

- Worldwide national privacy and data protection laws in 40+ countries around the globe [enacted or pending]
  - EU national laws implementing the Directive
  - EEA national laws implementing the Directive (Iceland, Norway)
  - CSB national laws (Bulgaria, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Slovak Republic, Slovenia)
  - CIS national laws: (Ukraine, Russia)
  - Asia Pacific (Australia, Hong Kong, Japan, Malaysia, New Zealand, Thailand, Taiwan]
  - Americas (Argentina, Canada, Chile, Mexico, Paraguay, Peru, U.S.)
  - Switzerland, Israel,

Most of these laws are similar to the comprehensive European model

Legal Framework: FTC Enforcement

- FTC Enforcement of online privacy policies:
  - Children's Online Privacy Protection Act (COPPA) - requires parental consent to collect personal information online from children under the age of 13.
  - Enforcement power under Section 5 of the FTC Act for unfair and deceptive trade practices. This power is the basis for enforcement actions against web site operators who operate in violation of their own privacy policies and privacy notices.

Develop a Business Plan for Privacy

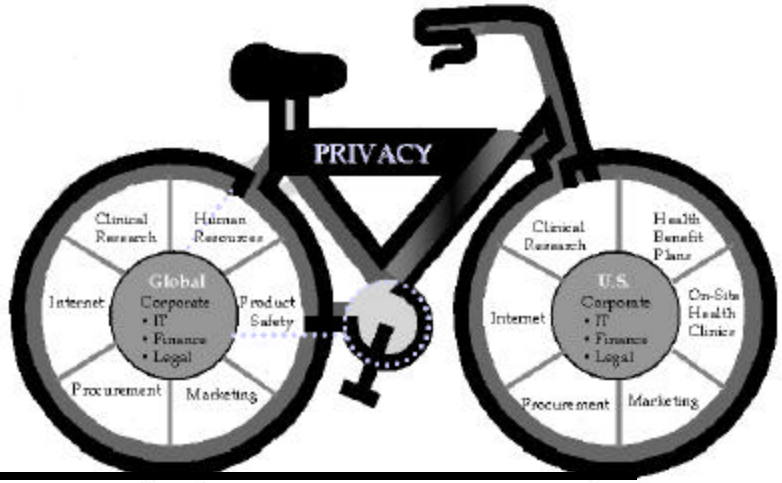
- Identify critical privacy issues
- Identify business stakeholders (local owners) for each issue
- Identify and allocate resources
- Set priorities and realistic timelines
- Collaborate with business stakeholders to assess the issue
- Analyze gaps between current and required policies, practices and procedures

IMPLEMENT

Implementing the Business Plan for Privacy

- Collaborate with business stakeholders to implement solutions that are compliant with applicable laws and regulations
  - Privacy polices and procedures (SOPs)
  - Privacy notices and appropriate consent forms
  - Implement privacy provisions in contracts with entities performing services that involve the handling of personal data on your behalf
  - Establish and ensure appropriate physical and technical safeguards and accompanying administrative processes.
  - Establish a coordinated access and complaint program
  - Conduct training
  - Establish measures to enforce privacy practices

. . . *THANKS*


PRIVACY
Clinical Research
Human Resources
Global Corporate • IT • Finance • Legal
Internet
Product Safety
Procurement
Marketing
Clinical Research
Health Benefit Plans
U.S. Corporate • IT • Finance • Legal
Internet
On-Site Health Clinics
Procurement
Marketing