Basics of Building an Effective Privacy Program

Privacy Officers Association
Privacy and HIPAA Compliance Training

Robert R. Belair
Grand Hyatt Hotel
Washington, DC
October 24, 2001
Prospects for Privacy After 9/11/01

- Privacy legislation will not move this year
  - Online privacy
  - Social security number privacy
  - Genetic privacy
Prospects for Privacy After 9/11/01

Factors driving privacy have not changed
- Public concern
- Media coverage
- Identification theft
- The “urge to merge”
- Extraordinary state interest
Prospects for Privacy After 9/11/01

*Fundamental factors driving privacy have not changed*

- It’s the technology
  - The Internet, the Internet, the Internet
  - Location tracking
  - Biometric technologies
  - Emerging technologies
Prospects for Privacy After 9/11/01

- Emerging public debate about public safety vs. privacy
  - Background checking
  - Passenger screening
  - National ID card
Prospects for Privacy After 9/11/01

One possible “hinge”

- About 80 percent of Americans distrust government
- About 76 percent of Americans distrust big business
- Privacy thrives in an environment of distrust
- Recent polls show Americans’ trust in federal government is surging
Effective Corporate Privacy Program

“An effective privacy program genuinely promotes the protection of personal privacy in a manner that is relevant and appropriate for the corporation or organization.”
How to Genuinely Promote Privacy

- Notice
- Choice
- Access/ correction
- Data integrity
- Security
- Confidentiality
- Remedies
How to Disingenuously Promote Privacy

- The 10,000 foot privacy policy
- The privacy policy that is all policy and no implementation
- The “as permitted by law” privacy policy
- The “as required by law” privacy policy
- The limited scope privacy policy
A Relevant Privacy Program

- Privacy policy should address the kinds of personal information that the company collects and uses.
- Privacy policy should almost always address HR information.
- Privacy policy should address information flows that actually impact the company.
- Privacy policy should avoid preserving “maximum flexibility.”
An Appropriate Privacy Program

- Privacy program is sensitive to overall corporate goals
- Privacy program views personal information as a corporate asset
  - Research
  - Marketing
  - Consumer trust
  - Employee management
An Appropriate Privacy Program

- Privacy program has an exit strategy for customer/patient information
- Privacy program minimizes its expense
- Privacy program outsources appropriately
An Appropriate Privacy Program

- A comprehensive, effective privacy policy
- Readable, accurate, comprehensive privacy notices
- A privacy audit and review capability
- A privacy task force or other privacy outreach
An Appropriate Privacy Program

- Effective relationships with IT, HR, Government Relations, Public Relations, Legal, CIO, Marketing
- A privacy lawyer
- A privacy sponsor at a senior corporate officer level
An Appropriate Privacy Program

- A media program
- A plan for handling privacy firestorms
- A plan for importing personal information from the EU, Canada, Australia, etc.
- A plan for reviewing new products and services
- A plan for reviewing new or changed policies
- A plan for managing, “controlling” your CEO
An Appropriate Privacy Program

- A plan for HIPAA compliance
- A privacy training program
- A state legislative monitoring program
- A plan for handling sensitive health information - AIDS, genetic, mental health, etc.