Managing the Privacy Function at a Large Company

Kimberly S. Gray, Esq., CIPP
Chief Privacy Officer
Highmark Inc.

Privacy Program

- Organizational structure
- Staffing
- Policy and procedure development and implementation
- Interdepartmental collaboration
- External collaboration
- Subsidiaries/affiliates
- Privacy breach investigations and incident response
- Culture

Organizational Structure

- Centralized Model
  - Accountability and oversight known to all
  - Management hierarchy allows issues to be resolved quickly
  - Better able to match strategic direction with corporate mission and value statement
- Decentralized Model
  - Everyone accountable for his/her own actions
  - Compliance more embedded in minds of individuals and more part of overall corporate culture

Staffing

- Chief Privacy Officer
  - Management level (executive, senior management recommended)
  - Visible
  - Attorney?
  - Information security accountability?
- Subject matter experts
  - Legal compliance
  - Information security
  - Customer service
  - Sales, marketing?
  - Other?
- Operational staffing
  - Ability to communicate well with others
  - Ability to lead projects
  - Some subject matter expertise

Policy & Procedure Development and Implementation

- Legislative review and comment
- Identification of regulatory obligations and risk management posture
- Consumer attitude survey review
- Provide analysis and requirements to affected business units
- Oversight of business unit compliance or direct project oversight
- Executive steering committee?
- Training and communication of new policy/procedure/process (multi-channel) to all or to management (train the trainer)
- Compliance monitoring, assessment, enforcement

Interdepartmental Collaboration

- Legal
- Other compliance departments
- Internal audit
- Customer-focused business units
- Physical security and safety
- Information security
- Sales and marketing
- Public relations, media relations
- Informatics and reporting
- Information systems
- Government/regulatory affairs
- eCommerce
- Human resources/employee relations
- Risk management

External collaboration

- Federal and state government and regulatory bodies
- Customers
- Media
- Vendors
- Outside counsel
- Business partners
- Data protection authorities (global)
- Law enforcement
- Professional organizations

Subsidiaries and Affiliates

- Reporting relationships
- Oversight and accountability
- Ownership and status designation
- Committees
- Differing business needs
- Differing regulatory requirements
- Global versus domestic

Privacy Breach Investigations and Incident Response

- Fact gathering, interviews, forensics
- Corrective action plan
- Mitigation of damages
- Employee discipline
- Security incident per state or federal law?
- Notifications
- Post-incident reporting to management (Compliance Committee)
- Privacy incident response team
  - Privacy Officer
  - Information Security Officer
  - Safety and Security Officer
  - Legal
  - Corporate communications, media relations
  - Affected party
  - Affected business unit

Culture

- Legal compliance requirements
- Risk management posture
- Consumer attitude considerations
- Ethics (“doing the right thing”)
- Treating the confidential information as if it were your own