Implementing an Accountable Privacy Program

The IAPP Canada Privacy Symposium
Friday, May 9th, 2014

Samara Starkman
Director, Privacy & Access, CancerCare Ontario

Pamela Snively
Managing Director, AccessPrivacy by Osler
Changing Data Universe

- Changing public perception/sensitivity and expectations
- Increasingly active regulators
- Active privacy advocates and advocacy groups
- Social Media influence
- International regulators
- Explosion of Data – volume, speed
- Sharing of Data
- Analytics
- Big Data
Privacy Challenges Today

• Consent Model cannot always be supported – is strained in some circumstances
  • Informed Consent – do we even want to be informed?
  • Is understanding possible?
  • Uses cannot always be anticipated
• Anonymization – can it work?
  • De-identification
Tension  - Big Data and Privacy

HealthCare Industry sometimes views privacy as a barrier to innovation and to saving lives

Vs.

Privacy advocates and regulators see a failure to appreciate privacy as a fundamental right and greed as the driver
Thoughts from OECD Foresight Forum on Big Data

• You need to be accountable for your use of Big Data as well as for your failure to use it.

  • You need to consider the real risk/benefits of using data as well as the opportunity costs of not using it.
Governance & Accountability

• Beyond “just” consent – trying to resolve the tension
• Use Cases – context matters
• Privacy as a fundamental right can be respected through proper governance requirements – true accountability
• This doesn’t mean consent isn’t relevant anymore – this is still primarily a consent-based regime – but there are already recognized exceptions
Section 45

Approval

(3) A health information custodian may disclose personal health information to a prescribed entity under subsection (1) if,

(a) the entity has in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information; and

(b) the Commissioner has approved the practices and procedures, if the custodian makes the disclosure on or after the first anniversary of the day this section comes into force. 2004, c. 3, Sched. A, s. 45 (3).

Review by Commissioner

(4) The Commissioner shall review the practices and procedures of each prescribed entity every three years from the date of its approval and advise the health information custodian whether the entity continues to meet the requirements of subsection (3). 2004, c. 3, Sched. A, s. 45 (4).

Authorization to collect

(5) An entity that is not a health information custodian is authorized to collect the personal health information that a health information custodian may disclose to the entity under subsection (1). 2004, c. 3, Sched. A, s. 45 (5).
The Office of the Information and Privacy Commissioner (Ontario) ("IPC") has developed a 136 page Manual* that sets the bar very high for health privacy accountability.

The Manual sets a long list of required policies (next slide).

In addition to the required policies, the Manual sets out specific requirements for:

- Privacy and Security Governance and Accountability Frameworks
- Detailed, comprehensive logging, documentation and record keeping

http://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=8417
Policies Required by the IPC Manual

- Privacy
- Ongoing Review of Privacy & Security Policies
- Transparency
- Collection of PHI
- Statements of Purpose of Dataholdings
- Limiting Access to PHI
- Use of PHI
- Disclosure of PHI for Research
- Disclosure of PHI for other reasons
- Execution of Data Sharing Agreements
- Executing Agreements with Third Party Service Providers re PHI
- Linkage of Health Records
- De-Identification and Aggregation
- Privacy Impact Assessments
- Privacy Audits
- Privacy and Security Breach Management
- Privacy Complaints and Inquiries

- Information Security
- Secure Retention of PHI
- Secure Retention of PHI on mobile devices
- Secure Transfer of PHI
- Secure Disposal of PHI
- Passwords
- Maintaining & Reviewing System Control and Audit Logs
- Patch Management
- Change Management
- Back-up and Recovery
- Acceptable Use of Technology
- Security Audits
- Privacy & Security Training and Awareness
- Confidentiality Agreements
- Termination or Cessation of Employment
- Discipline and Corrective Action
Accountability and Privacy Governance

• Major shift in privacy regulatory expectations for organizations
  • “Accountability” concept has matured from checkbox compliance to holistic concept of privacy governance
  • Canadian privacy regulatory authorities at the forefront internationally of movement towards “Accountability” model
Accountability and Privacy Governance in the Private Sector

• “Getting Accountability Right with a Privacy Management Program”
  • Joint guidance issued by Office of the Privacy Commissioner of Canada, and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia
• Guidance document crystallizes privacy governance expectations of the regulators
• Concept of a Program
Core Program Compliance – Program Controls

• Personal Information Inventory – Data Lifecycle
• Risk Assessment
• Policies
• External Communication
• Service Provider Management
• Breach Management
• Training and Education
• Monitoring, Oversight and Review
Risk Assessment Tools

- Ethical Considerations and Identification of Stakeholders
- Personal Information Inventory – risk report
- Data Flow Maps - sensitive data/highest risk first
- Privacy Impact Assessment (PIA) and beyond
- Threat Risk Assessment (TRA)
- Initial review and then annual legislative compliance review
- Monitors for legislative developments, new findings or orders, or developments in regulatory guidance
- Overall Project Delivery
Risk Assessment Program

- Risk assessment and risk mitigation design input into new or modified projects - Privacy by Design (PBD)
- (Ethical) Risk Review Committee
- Risk mitigation measures – Action plans - Oversight
- Privacy Officer review and approval process in respect of all new or modified projects or processes
- Evergreen methodology
- Audit and compliance Function
External Communication

• Privacy Notice/Statement
• Procedure for (easily) informing individuals of:
  1. Their privacy rights
  2. Basic program controls
• Individuals to understand purpose of collection, use and disclosure as well as basic safeguards and retention period (cross-border transfers)
• Contact information for questions/complaints
Service Provider Management

• Contractual or other arrangements in place. Consider:
  • Transborder data flows
  • Security
  • Breaches
  • Monitoring
  • Training
  • Restrictions on sub-contracting
  • Audits
  • Due Diligence
Compliance Monitoring

• Critical component of risk management
• Evidence is critical for compliance
• Compliance monitoring vs. program monitoring
• Monitoring adherence to policies and procedures
• Self-Assessments/Internal Audit
• Metrics
  • Whether training is occurring and whether it is effective
  • Confidentiality agreements are signed
  • Contracts are in place
  • Risk assessments are completed
  • Recommendations implemented
Training and Awareness - General Requirements

• Mandatory for all employees **before** they access personal information
• Covers privacy policies and procedures, tailored to specific needs of employee
• Regular, recurrent training
• Employees sign agreement to comply with the policies and program controls
• (Regulators say that budget must be set aside to train the Privacy Officer)
Key Elements of a Breach Response Protocol

- The person responsible for managing breaches must be identified.
- The four baseline steps recommended by Canadian privacy regulatory authorities are:
  1. Containment
  2. Evaluating the Risks
  3. Notification
  4. Prevention
- A critical first step is “Reporting”
- Test the protocol
Organizational Structure

- Critical for the success of the program
- Buy-in from the top and throughout the organization
- Program credibility; Privacy Office Influence
- Facilitate and build-in monitoring and oversight
- Foster awareness (culture of privacy)
- Proper departmental integration (Legal, Procurement, Information Security, Human Resources, Marketing, Public Affairs, etc.)
Wrap Up

QUESTIONS?
Contact Information

Pamela Snively
Managing Director, AccessPrivacy
416.862.6694
psnively@osler.com

Samara Starkman
Director, Privacy & Access
CancerCare Ontario
416.217.1279
samara.starkman@cancercare.on.ca