A Modern Effective Regulatory Approach to Demonstrating Accountability

WELCOME AND INTRODUCTIONS

Chief Privacy and Legal Officer;
Corporate Secretary, ICES //
Special Counsel, Osler's

Director of Health
Policy, Information and Privacy
Commissioner of Ontario

WELCOME AND INTRODUCTIONS

NTD: We will consolidate the speaker slides to one slide. This will be changed before we submit the draft on May 3.

President, RGS Management Consulting Services

Moderator

AGENDA OUTLINE

I. Session Outline
II. Welcome and Introductions
III. Speaker 1 – Rosario Cartagena
    i. The Privacy Regulatory Environment
    ii. Demonstrable Accountability
    iii. An Effective Compliance Program to Demonstrate Accountability
    iv. ICES Case Study
IV. Speaker 2 – Andrew Drummond
    i. Background
    ii. IPC Review Process
    iii. Elements of How Organizations Demonstrate Accountability
    iv. Automation of Reporting

V. Speaker 3 - Robin Gould-Soil
    i. [Leveraging Technology to Meet Privacy Obligations]
    ii. [Considerations When Implementing Technology]
VI. Questions and Answers
VII. Closing Remarks

The Privacy Regulatory Environment

- Patchwork of federal and provincial laws
  - over 30 privacy statutes in Canada
- A key privacy regulatory expectation includes demonstrating accountability
  - Organizations must establish privacy policies and procedures, but also must show how those policies and procedures are being complied with

Demonstrable Accountability

"The concept of demonstrable accountability in privacy law is dynamic and evolving…

Accountability — organizations being responsible for the personal information in their possession and implementing policies and procedures accordingly — is a cornerstone of Canadian private-sector and health privacy laws.

In 2012, Canadian privacy commissioners announced their expectation for organizations under investigation to be able to demonstrate their comprehensive privacy programs….such as requiring internal policies, transparency and privacy impact assessments under an enforcement regime…

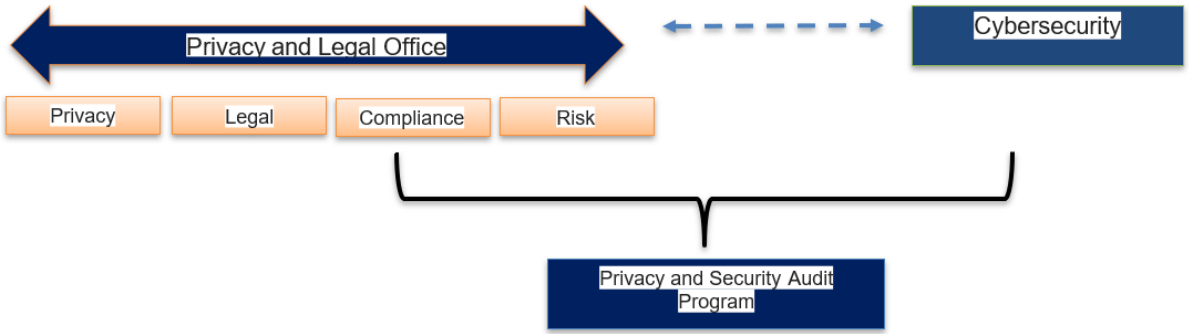
Globally, demonstrable accountability has developed significantly over the last decade. The concept appears in legislation in Brazil, Singapore and Australia, and in the European Union's General Data Protection Regulation (GDPR), among other legal sources. Not only do regulators expect companies to demonstrate their robust privacy programs, but shareholders, the media and the general public demand that these organizations be held accountable and act responsibly in the ways in which they store and use data…..

One challenge regulators face is preventing accountability from becoming a simple tick-the-box exercise. Being a data-responsible organization means more than just producing certain documentation, although it can be difficult to simultaneously have an active, robust program and to innovate and deliver value through the use of data. Moving beyond a system of compliance as society's views on data and privacy evolve, to one where companies have flexibility to find new ways to use data creatively and to demonstrate their accountability, will be a large part of the conversation going forward."

Demonstrable accountability: Quebec's Bill 64 amendments and privacy governance (osler.com)

Building An Effective Compliance Program to Demonstrate Accountability

- Initially manual (non-automated)
- Accountability demonstrated through Privacy and Security Audit Program and IPC Triennial Review



Case Study

- Unique status under PHIPA
- Three-Year Reviews by the IPC
- Manual for the Review and Approval of Prescribed Persons and Prescribed Entities (over 200 pages)

Challenges for the Operationalization of Demonstrable Accountability

- 108 Policies, Procedures
  - Privacy
  - Information Security
  - Human Resources
  - Organizational
- Indicators
- Privacy and Security Audit Program
- PIAs, TRAs, Logs
- Operational Activity: 1000 Projects / Year + Corporate Projects across 7 sites in the province
- Global privacy and security changing rapidly
- Need to remain agile and provide services to clients

Perspectives from the Regulator

- How we expect organizations to demonstrate accountability
- Pros and cons of using technology/automation to meet accountability obligations

Perspectives from the Regulator: Background

- Ontario's PHIPA allows disclosure of personal health information **without consent** to organizations named in regulation to perform system-level analysis or to hold registries to facilitate the provision of health care.
- To enable confidence that this non-consent framework is appropriately protective, PHIPA requires that the Commissioner "review and approve the practices and procedures" every three years.
- To enable the "review and approval", the IPC created the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*, which lays out in detail the expectations we have in order to grant that approval.

Perspectives from the Regulator: IPC Review Process

- Prior to 2023, organizations submitted a *Report* and data on required *Indicators*, describing compliance with the Manual
  - Comprehensive but shallow review
- Post 2023, new *Manual*, with a new focus on how we expect the organizations to demonstrate accountability:
  - IPC chooses (at its sole discretion) a subset of policies and procedures to review in close detail, based on a risk-based approach.
  - Organizations still submit indicators
  - Organizations are entitled to submit “Statements of Requested Exception”

Perspectives from the Regulator:
Elements of How Organizations Demonstrate Accountability

- Review of subset of policies/procedures
  - Do they do what the Manual says they must, in a manner appropriate to the organization?
- Indicators
  - What is happening on the ground? Are the policies and procedures effective in ensuring appropriate safeguards for the non-consent-based collection and use of PHI? Are there strange, inappropriate, confusing, or anomalous counts?
- Statements of Requested Exception
  - Where the requirements of the Manual are not being met, why not? How and when will the organization come into compliance? What are the risks in the interim, and how are they being managed? Is the organization doing something "against" the requirements but meeting the expectations at the same or higher standard?

Each of these three sets of materials can point out where further "spot checks" or investigations might be useful or informative.

In all situations, the IPC solely determines whether the organizations have adequately demonstrated that they meet legislative and regulatory accountability requirements.

Perspectives from the Regulator: Automation of Reporting

- The indicators are highly detailed, and provide the regulatory insight into how the organization is actually fulfilling its requirements.
  - We can drill down to see whether they are actually meeting their own policy requirements
  - We can look at anomalous indicators and query further
  - We can identify areas of risk that the organizations may not have thought of
- To conduct our work properly, we **need** accurate indicator data.
- Automation can take out a lot of on-the-spot interpretive work that can create unintended questions.
- On the downside, automation can also “lock in” misinterpretation from the start, and a lot of care must be taken to avoid “garbage in, garbage out” scenarios.

Leveraging Technology to Meet Privacy Obligations – What Problem are you trying to solve

Privacy Program Management	•Governance and Accountability •Assessment Management •Consent Management •Incident Response •Individuals Rights • Reporting
Compliance Risk Management	•Regulatory Watch •Legislation Impact assessments on current watch •Policy Management •Advice and Consultations •Risk and Control Assessment •Policy Management •Testing of Controls •Reporting
Enterprise Privacy Management	•Data Discovery •Data Mapping •De-identification/Pseudonymity •Vendor Management •Synthetic Data

Considerations When Implementing Technology (Automate or Not)

Considerations

- Privacy office organization
- Ownership and accountability
- Organization volumes
- Current challenges
- Budget
- Benefits and Consequences

What Should the Technology Do?

- Improve the ability to demonstrate compliance
- Reduce or stabilize FTE count – drive capability
- Provide consistency
- Usability and can satisfy your business requirements
- Flexible and adaptable to meet your business needs
- Grow with your needs

Vendor Evaluation Criteria

- Ease of Use
- How much is out-of-the-box versus customization
- Functionality
- Integrations
- Security Requirements
- Users of the solution – Internal / Customer-facing
- Technology Architecture
- On prem / Cloud / As a Service
- Pricing and Costs
  - Licencing Costs
  - Implementation Cost
- Support after implementation – Supplier, Integrator support, in-house
- Environments – Production, Development, Q&A
- Training
- Crisis Management

Common Mistakes

- Missing business requirements or intra-dependencies with other groups
- Have not spoken to the technology group to understand the current tools available
- Change management
- Not engaging the right people to help select the technology
- Vendor reviews not conducted
- Separating the sales pitch from the reality

Case Study:
How we have (will) Enable Automation at ICES

- Process included:
  - Mapping business requirements
  - Considering IPC requirements and expectations
  - RFP process and vendor selection

RESOURCE LIST

- The Manual for the Review and Approval of Prescribed Persons and Prescribed Entities
- Getting Accountability Right with a Privacy Management Program, Office of the Privacy Commissioner of Canada
- [To be developed.]

HOW DID THINGS GO? (WE REALLY WANT TO KNOW)

Did you enjoy this session? Is there any way we could make it better? Please let us know by filling out a speaker evaluation.

1. Open the Cvent Events app.
2. Enter **IAPP CPS24** (case and space sensitive) in search bar.
3. Tap “Schedule” on the bottom navigation bar.
4. Find this session. Click “Rate this Session” within the description.
5. Once you’ve answered all three questions, tap “Done”.

Thank you!