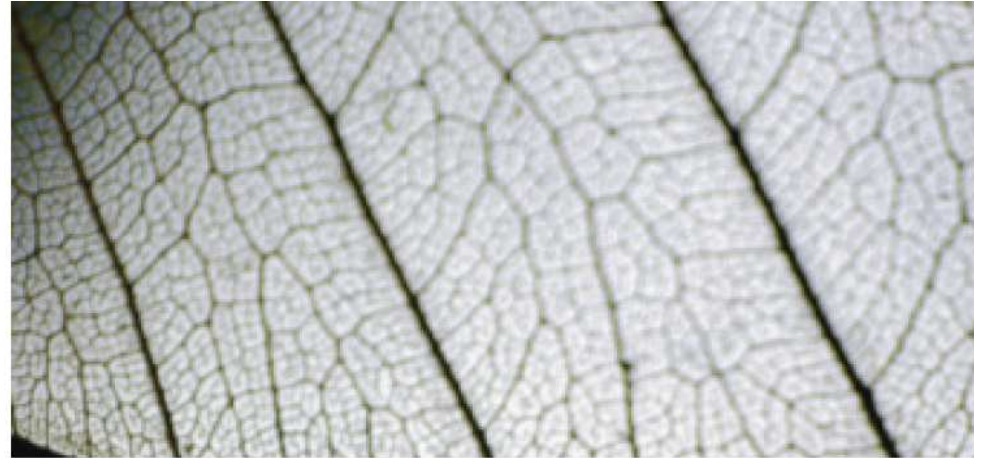


**Access***Privacy*<sup>HB</sup>



Leaders in privacy, compliance &  
information governance solutions

**Privacy Governance:  
Private Sector Governance Models  
and the Health industry**

**Pamela Snively, Managing Director**



**AccessPrivacy**HB is an integrated information governance service, complementary to the Heenan Blaikie LLP national Privacy & Information Management and Access to Information Law practices.



Adam Kardash  
Managing Director & Head



Ruth Belcher  
Managing Director



Pamela Snively  
Managing Director

We provide privacy and information management consulting services to organizations in the private, public and broader public sectors, with a special focus on industry-specific issues facing the financial services, health and business process outsourcing sectors.

## Outline

- The changing universe of data management
  - Business challenges
- Global privacy developments
  - Common themes
- Why build a privacy and information governance program?
- Governance and accountability
  - Accountability principle
  - Accountability Project
  - Accountability in the EU
- Guidance from the private sector
  - OSFI Guideline E-13 – Legislative Compliance Management [for federally regulated financial institutions]
  - Competition Bureau Information Bulletin on Corporate Compliance Programs
  - Enform Basic Safety Program for the Upstream Petroleum Industry
- Guidance from the Health Sector
- Common elements of effective governance
- Privacy and security governance in practice
- Privacy and Security Governance Framework template

## The changing universe of data management

- Global economy
- Challenge of technology
  - Internet, computer capacity, ubiquitous digital data, data analysis and use
  - Global flow and access to data
  - Remote storage and processing of data in the “cloud”
- Unrelenting security threats
- High profile data breaches involving global brands

## The changing universe of data management (cont'd)

### Privacy Commissioner Jennifer Stoddart writes on The Future of Privacy Regulation (Feb. 10, 2010):

When I took over as Privacy Commissioner, Facebook didn't exist. Neither did Twitter, Flickr, YouTube, Google Street View, Foursquare, iPods and all the many novel ways in which people now routinely connect with the rest of the world. And it's not just technology that's different; it's other drivers of change as well. Like real-time globalization, for instance, and the instantaneous worldwide flow of data. It's the way people embrace and respond to technology. Their expectations of what the technology can do for them, and at what cost. Is it desirable, for example, to buy greater convenience at the cost of less privacy? In light of these colossal changes over the past decade alone, it would be foolish to try to predict what the next decade will hold. But what we can say for certain is that the regulatory framework we have in place now for the protection of privacy and personal information is already being sorely tested. We have bent and stretched it in many different ways. And, if we don't want it to snap, we need to figure out how to fortify it for the decade ahead.

## The changing universe of data management (cont'd)

### Business challenges

- Rapidly evolving technology and analytic techniques pose challenges to existing privacy compliance programs
  - Traditional metrics may not be enough
- Increasing compliance requirements imposed by various global regulators
  - Laws often lag behind new technologies
- Every employee poses a potential privacy risk

## Global privacy developments

### Common themes

- Jurisdictions around the world are modernising privacy regulation
  - Broad recognition of the need for a global privacy standard
  - OPC and Alberta and BC OIPC actively involved in most international initiatives on basis that future of protecting the personal information of Canadians involves international co-operation
  - Work is being done in many arenas including Spanish initiative, ISO, OECD and APEC
  - Reforms in Canada, Australia, New Zealand, Mexico and elsewhere
  - US developments include FTC Roundtables, DoC consultation, Rush Bill / Best Practices Act

## Global privacy developments

### Common themes (cont'd)

- Many jurisdictions have adopted (or are considering adopting) specific laws that require companies and/or government agencies to disclose data breaches involving personal information
  - 46 US states plus Puerto Rico and New York City
  - Germany, Australia, New Zealand, Canada (federal, Alberta, BC)
  - e-Privacy Directive 2009/136/EC (applies on a sectoral basis to ISPs and telcos)

## Global privacy developments

### Common themes (cont'd)

- Monetary penalties for non-compliance with privacy and safeguarding standards are becoming the norm
  - US (HIPAA/HITECH Act, FINRA), UK, Germany, Australia
  - Increasingly significant fines
    - €1.1 million (C\$1.6 million) levied against German Railways Operator Deutsche Bahn AG
    - UK Financial Services Authority (FSA) fines the UK branch of Zurich Insurance Plc (Zurich UK) £2,275,000 (C\$3.5 million) for failing to have adequate systems and controls in place to prevent the loss of customers' confidential information
    - Florida Attorney General fines Fidelity National Information Services subsidiary, Certegy, \$975,000 for failing to have real-time privileged-user monitoring in place

## Global privacy developments

### Common themes (cont'd)

- Increasingly prescriptive safeguarding standards are being imposed, with broad reach
  - Identity Theft Red Flags Rule
  - Massachusetts Information Security Regulations
  - Nevada & Washington have recently passed legislation that mandates compliance with Payment Card Industry Data Security Standard (PCI DSS) for businesses that accept payment cards
  - HITECH Act

## Global privacy developments

### Common themes (cont'd)

- Privacy regulators more active with investigations, audits and enforcement activities
  - Increasingly coordinating efforts across jurisdictions to address common concerns
  - Jacob Kohnstamm, Chair of the Dutch Data Protection Authority:

“We live in a globalized world with new technologies providing infinite possibilities for sharing and re-using information globally. Privacy has thereby also become a global issue. If we want to continue to protect the privacy rights of our national citizens, it is essential that we work together internationally.”

## Global privacy developments

### GPEN

- Recent establishment of Global Privacy Enforcement Network (GPEN)
  - Canada is a founding member of GPEN
  - Joint letter to Google, April 19, 2010, signed by data protection authorities in Canada, France, Germany, Israel, Italy, Ireland, Netherlands, New Zealand, Spain and the UK expressing concerns about privacy issues related to Google Buzz

## Global privacy developments

### Google Buzz and international collaboration

## Privacy Commissioner Jennifer Stoddart in her appearance before the ETHI Committee (Oct. 19, 2010):

We recognize that addressing this global challenge will demand agility and resourcefulness on the part of all privacy authorities. That is why, when Google disregarded privacy rights in the rollout of its Google Buzz social networking service last February, we opted for an innovative alternative to our conventional tools of audit and investigation. Instead, we led nine other data protection authorities from around the world in an unprecedented and highly effective tactic: The joint publication of an open letter that urged Google and other technology titans entrusted with people's personal information to incorporate fundamental privacy principles directly into the design of new online services.

## Global privacy developments

### Google Buzz and international collaboration (cont'd)

## Privacy Commissioner Jennifer Stoddart in her appearance before the ETHI Committee (Oct. 19, 2010):

We are engaging with global partners in numerous other ways as well. Last month, for instance, we joined other data protection authorities from around the world to establish the Global Privacy Enforcement Network, which aims to bolster compliance with privacy laws through better cross-border co-operation. Later this month at an international conference of data protection and privacy commissioners, I will be co-sponsoring a resolution that would see privacy considerations become embedded into the design, operation and management of information technologies.

## Global privacy developments

### GPEN (cont'd)

- GPEN's mission is to:
  - discuss the practical aspects of privacy law enforcement co-operation
  - share best practices in addressing cross-border challenges;
  - work to develop shared enforcement priorities
  - support joint enforcement initiatives and awareness campaigns
- Current GPEN members include Canada, US, Australia, France, Germany, Ireland, Israel, Italy, The Netherlands, New Zealand, Slovenia, Spain, United Kingdom
- New website at <https://www.privacyenforcement.net/>

## Global privacy developments

### Summary

- Personal information is an increasingly regulated asset
- For organizations that operate across borders, complying with these various regulations poses significant challenges
- Global flow of data challenges the way we have traditionally approached information protection and tests existing notions of jurisdiction and cross-border co-operation
- 2010 has been a year for taking stock of privacy

## Why build an information governance program?

- An effective information governance program can:
  - provide a means by which an organization satisfies itself that it is in compliance with the law... as well as internal policies and business requirements
  - proactively identify and mitigate privacy risks and thereby reduce the risk of non-compliance
  - contribute to maintaining a good reputation
  - be a key competitive tool for organizations
  - facilitate cross-border transfers of data
  - reduce costs related to litigation, fines, adverse publicity and the disruption of operations resulting from non-compliance

## Governance and accountability

### Accountability principle

- First established in 1980 in the Organization for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*
- Fundamental to privacy protection in the European Union (EU)
- The first principle in PIPEDA governing protection and management of data, whether it is maintained and processed by the organization or third party service providers, or domestically or outside Canadian borders
- Reflected in emerging governance such as the Madrid International Standards, ISO draft standard and the APEC privacy framework and its cross-border privacy rules
- Binding corporate rules (BCRs) that are used in the context of international data transfers also reflect the accountability principle
- How accountability is demonstrated or measured has not been clearly articulated

## Governance and accountability

### Accountability principle (cont'd)

- Accountability shifts the primary responsibility for data protection from the individual to the organization collecting and using data
  - US law is largely based on disclosure of the organization's privacy policy, notification and obtaining the individual's consent to specific uses of data
  - Individuals are responsible for determining how their data is used and shared
  - An accountability-based approach recognizes that, faced with complex technologies, business models and vendor relationships, consumers find it increasingly difficult to make well-informed privacy decisions
  - Accountability requires that organizations make responsible, disciplined decisions about data use even in the absence of traditional consent

## Governance and accountability

### Accountability principle (cont'd)

- The advantages of an accountability-based approach to data governance include:
  - helping bridge approaches across disparate regulatory systems, thereby facilitating data flows and assuring individuals a common level of data protection
  - improving confidence of individuals that their data will be protected by requiring an organization to remain accountable no matter where the information is processed
  - raising the quality of data protection by requiring that organizations be prepared to demonstrate upon request by the proper regulatory authorities that it is appropriately securing and protecting data
  - allowing for greater flexibility and directing scarce resources towards mechanisms that provide substantive privacy outcomes

## Accountability Project

- Spear-headed by the US-based Centre for Information Policy Leadership (CIPL)
- Phase I reflects on what it means for an organization to be accountable for the personal information it collects
  - Released October 2009  
[http://www.huntonfiles.com/files/webupload/CIPL\\_Galway\\_Accountability\\_Paper.pdf](http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf)
- Phase II considers how organizations can demonstrate accountability, as well as how regulators should measure accountability
  - Released October 2010  
[http://www.huntonfiles.com/files/webupload/CIPL\\_Accountability\\_Phase\\_II\\_Paris\\_Project.PDF](http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF)
- May result in a framework that global privacy regulators can use to audit compliance

## Accountability in the EU

- Article 29 Data Protection Working Party white paper on *The Future of Privacy*
  - Adopted on Dec. 1, 2009  
[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf)
- International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution
  - Adopted in a closed session at the 31<sup>st</sup> International Conference of Data Protection and Privacy Commissioners, Nov. 5, 2009  
[http://www.huntonfiles.com/files/webupload/PrivacyLaw\\_resolucion\\_madrid.pdf](http://www.huntonfiles.com/files/webupload/PrivacyLaw_resolucion_madrid.pdf)
- Article 29 Data Protection Working Party Opinion on the principle of accountability
  - Submitted to the European Commission on July 13, 2010
  - The Opinion's executive summary states:

“EU data protection principles and obligations are often insufficiently reflected in concrete internal measures and practices. Unless data protection becomes part of the shared values and practices of an organization, and responsibilities for it are expressly assigned, effective compliance will be at considerable risk, and data mishaps are likely to continue.

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf)

**Accountability in the EU** (cont'd)  
Article 29 WP's Opinion on accountability

- Express recognition of accountability as a driver for effective implementation of data protection principles
  - Reinforces existing obligations
  - Principles-based, flexible and scaleable
- Accountability proposed as a key reform to the Data Protection Directive, together with “privacy by design” and effective enforcement powers and sanctions

## Accountability in the EU

Article 29 WP's Opinion on accountability (cont'd)

- **Accountability principle**
  - Would apply to all data controllers
  - Organisations should “define and implement the necessary measures to ensure compliance with the principles and obligations of the Directive and to have their effectiveness verified periodically
  - Organisations should be able to demonstrate this on demand

## Accountability Project Phase I

- Accountability's essential elements include:
  - Organization commitment to accountability and adoption of internal privacy policies consistent with recognized external criteria
  - Mechanisms to ensure responsible decision-making about the management and protection of data and to put privacy policies into effect, including tools, training and education
  - Systems for internal, ongoing oversight and assurance reviews and external verification
  - Transparency and mechanisms for individual participation
  - Means for remediation and external enforcement

## Accountability Project Phase I (cont'd)

### Essential elements of accountability

- **Commitment to accountability**
  - An organization must implement policies linked to appropriate external criteria, deploy mechanisms to act on those policies, and monitor those mechanisms
  - Policies and the plans to put them into effect must be approved at the highest level of the organization
  - Performance against those plans must be visible to senior management

## Accountability Project Phase I

### Essential elements of accountability (cont'd)

- Tools, training and education
  - An organization must establish performance mechanisms to implement privacy policies, including:
    - tools to facilitate decision-making about appropriate data use and protection (e.g., privacy impact assessments)
    - training for employees who are involved in the collection, processing and protection of information

## Accountability Project Phase I

### Essential elements of accountability (cont'd)

- Ongoing oversight
  - An organization must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data
  - Monitoring must assess risks across the data life cycle – from its collection, to its use, to its destruction
  - Monitoring must apply to third party service providers to ensure that privacy obligations are met no matter who and where the data is processed
  - Resources should be allocated where the risk to the individual is greatest

## Accountability Project Phase I

### Essential elements of accountability (cont'd)

- Transparency
  - An organization's information procedures must be transparent and communicated in a publicly available privacy policy or notice as well as through the use of icons, videos and other mechanisms
  - Individuals should have the ability to see the data or types of data that the organization collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate (subject to certain exceptions)

## Accountability Project Phase I

### Essential elements of accountability (cont'd)

- Remediation

- An organization should establish a privacy policy that includes a means to address harm to individuals caused by failure of internal policies and practices
- The organization should identify an individual who serves as the first point of contact for resolution of disputes and establish a process by which privacy complaints are reviewed and addressed

## Accountability Project Phase II

### Common accountability measures

- Approaches to accountability include both regulatory and voluntary components
  - Voluntary tier: Going above and beyond minimum legal requirements
- “One size does not fit all”
  - Big / small; high risk / low risk
  - Must be tailored to the organisation’s business model, data holdings, technologies and applications, and the risks to privacy they raise for individuals
- Focus on effectiveness
  - Not box-ticking
- Accountable organisations should be prepared to demonstrate their programs when asked

## Accountability Project Phase II

### Common accountability measures (cont'd)

There are nine common fundamentals that an accountable organisation should implement:

1. Policies
2. Executive oversight
3. Staffing and delegation
4. Education and awareness
5. Ongoing risk assessment and mitigation
6. Program risk assessment oversight and validation
7. Event management and complaint handling
8. Internal enforcement
9. Redress

## Guidance from the public sector

- OPC 2009 Audit of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) refers to a “privacy management framework,” i.e, “the checks and controls in place to ensure that personal information is managed appropriately”
- “A model privacy management framework for federal departments has yet to be established,” however core elements include:
  - effective governance;
  - clear accountability;
  - a process for managing privacy breaches;
  - identification and management of privacy risks; and
  - ongoing compliance monitoring and awareness training

[http://www.priv.gc.ca/information/pub/ar-vr/ar-vr\\_fintrac\\_200910\\_e.pdf](http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_fintrac_200910_e.pdf)

## Guidance from the private sector

- Preliminary letter of findings issued against Google Inc. (Oct. 19, 2010)
- OPC finds Google contravened Canadian privacy law when it inappropriately collected personal information from unsecured wireless networks in neighbourhoods across Canada
- Recommendations:

“While I am pleased that Google has taken under review its processes and procedures that could impact privacy, I would nonetheless like the organization to ensure that these controls are complemented by an overarching governance model embodying all privacy issues pertaining to the design of internal/external products and services.”

**Guidance from the private sector** (cont'd)  
**Preliminary letter of findings issued against Google**

- Privacy Commissioner recommended that Google:
  - enhance privacy training to foster compliance amongst all employees
  - ensure it has a governance model in place to comply with privacy laws, including controls to ensure that necessary procedures to protect privacy are followed before products are launched
  - designate an individual or individuals responsible for privacy issues and for complying with the organization's privacy obligations

[http://www.priv.gc.ca/media/nr-c/2010/let\\_101019\\_e.cfm](http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm)

## Guidance from the private sector (cont'd)

- OSFI Guideline E-13 – Legislative Compliance Management (LCM)

[http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/E13\\_2003\\_Final\\_e.pdf](http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/E13_2003_Final_e.pdf)

- 2008 Competition Bureau Information Bulletin on Corporate Compliance Programs

[http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/vwapj/Compliance-Bulletin-090808-Final-e.pdf/\\$FILE/Compliance-Bulletin-090808-Final-e.pdf](http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/vwapj/Compliance-Bulletin-090808-Final-e.pdf/$FILE/Compliance-Bulletin-090808-Final-e.pdf)

- Enform Basic Safety Program for the Upstream Petroleum Industry

[http://enform.ca/media/3729/irp9\\_final\\_july2003.pdf](http://enform.ca/media/3729/irp9_final_july2003.pdf)

## Guidance from the private sector (cont'd)

### OSFI Guideline E-13 – LCM

- Conveys OSFI's expectations of federally regulated financial institutions (FRFIs) regarding controls through which they manage regulatory risk inherent in their activities
  - Expressly includes “Other Legislation” that may have a critical impact on the FRFIs reputation and/or safety and soundness, such as PIPEDA

## Guidance from the private sector

### OSFI Guideline E-13 – LCM (cont'd)

- Key LCM control elements include:
  - Identification, assessment, communication & maintenance of applicable regulatory requirements
  - Day-to-day compliance and oversight procedures that include monitoring and reporting procedures through which significant problems are identified, escalated and resolved
  - Internal audit or other independent validation of the effectiveness of an adherence to the LCM framework and key controls
  - Compliance oversight and internal audit reports to senior management and the board
  - Adequate documentation to demonstrate how regulatory risk is managed
  - Regular review and improvement to address changes in regulatory risks, products, activities and corporate structure

## Guidance from the private sector

### OSFI Guideline E-13 – LCM (cont'd)

- Role of board of directors
  - Board to approve LCM framework and ensure it is established and maintained
- Role of compliance oversight function
  - Designated role of Chief Compliance Officer independent of the line of business
  - Sufficient stature and authority in the organization
  - Necessary mandate, resources and access to the CEO and board of directors to achieve an appropriate control outcome
  - Significant issues are escalated to business operations management, senior management and the board as appropriate

## Guidance from the private sector

### OSFI Guideline E-13 – LCM (cont'd)

- Role of senior management
  - Implement the LCM framework throughout the FRFI in a manner that is tailored to the needs of each area
  - Ensure that appropriate policies and procedures are developed and applied effectively, and that all staff understand their responsibilities for compliance
  - Ensure that significant recommendations concerning issues of non-compliance or control improvements are acted upon in a timely way
- Role of internal audit (or other independent review function)
  - Validate the effectiveness of and adherence to the LCM Framework by risk-based testing on a rotational or other regular basis
  - Review function should be independent of the activities it reviews
  - Significant review findings and recommendations should be reported as appropriate to business operations management, senior management and the board
  - Actions taken in response to significant recommendations should be monitored

## Guidance from the private sector (cont'd)

### Competition Bureau Information Bulletin on Corporate Compliance Programs

- Conveys the Competition Bureau's expectations regarding "credible and effective corporate compliance programs designed to ensure compliance with the *Competition Act*... ."

"A good corporate compliance program helps to identify the boundaries of permissible conduct, as well as identify situations where it would be advisable to seek legal advice. Moreover, in some cases, courts have recognized a credible and effective compliance program as a mitigating factor when assessing remedies in the event of a breach."

## Guidance from the private sector

Competition Bureau Information Bulletin on Corporate Compliance Programs (cont'd)

- Key compliance control elements include:
  - Senior management involvement and support
  - Compliance policies and procedures
  - Training and education
  - Monitoring, auditing and reporting mechanisms
  - Consistent disciplinary procedures and incentives

## Guidance from the private sector

### Competition Bureau Information Bulletin on Corporate Compliance Programs (cont'd)

- Senior management should:
  - identify and assess the principal risks faced by the business and implement appropriate systems to manage such risks
  - foster a culture of compliance by playing an active and visible role in promoting its program
  - periodically reinforce its message by actively enforcing the program
  - communicate with the board of directors and report on compliance program issues such as progress and breaches
- A member of senior management should be appointed as a compliance officer, responsible for ensuring compliance and for dealing with questions and concerns pertaining to compliance

## Guidance from the private sector

### Competition Bureau Information Bulletin on Corporate Compliance Programs (cont'd)

- Documented policies and procedures:
  - are critical to a compliance program's success
  - should be widely available to all employees in a readily accessible format
  - should include examples to demonstrate the relevance of the policies and procedures to the employees' daily activities
  - should be updated when required to reflect material changes to the business or the law
    - Reasonable measures should be taken to promptly notify employees of such changes
- Organizations should consider requesting employees sign a certification letter stating that they have read and understood the compliance program in place

## Guidance from the private sector

### Competition Bureau Information Bulletin on Corporate Compliance Programs (cont'd)

- Training and education:
  - should demonstrate to staff, in a practical way, how compliance policies and procedures affect their daily activities
  - should allow employees the opportunity for extensive discussion on questions and answers
  - must be evaluated regularly to ensure effectiveness
- Senior management should play an active role in delivering compliance messages to employees:
  - by undertaking the necessary compliance training
  - by sending memoranda or e-mails supporting the compliance program and referring to the program in presentations and during other speaking opportunities

## Guidance from the private sector

Competition Bureau Information Bulletin on Corporate Compliance Programs (cont'd)

- **Monitoring, auditing and reporting mechanisms:**
  - help prevent and detect misconduct
  - educate staff
  - provide both employees and managers with the knowledge that they are subject to oversight
  - help identify areas of risk, areas where additional training is required and areas where new compliance issues may require new policies and/or procedures to be developed
  - determine the compliance program's overall efficacy
- **Senior management must investigate compliance issues raised and take the necessary steps to stop ongoing and prevent future non-compliance**

## Guidance from the private sector

### Competition Bureau Information Bulletin on Corporate Compliance Programs (cont'd)

- **Monitoring**
  - Refers to the ongoing procedures implemented to prevent non-compliance
    - Depending on the risks, periodic or continuous monitoring may be necessary
  - Identify employees who are exposed to a heightened risk (i.e., based on roles and responsibilities, previous issues and misconduct)
  - May support a due diligence defense should litigation arise
- **Auditing**
  - May be periodic, *ad hoc* or event-triggered
  - Designed to identify non-compliance and ensure any necessary mitigating steps have been taken

## Guidance from the private sector

Competition Bureau Information Bulletin on Corporate Compliance Programs (cont'd)

- Reporting

- Employees must be encouraged to freely report conduct that they believe contravenes the law or an organization's policy
- The program should identify clearly which actions require reporting, and when and to whom they should be reported
- An effective reporting system can be achieved in different ways, including by:
  - implementing a confidential reporting system
  - endorsing an open-door policy
  - promoting an anonymous hotline
  - identifying legal counsel as compliance resources

## Guidance from the private sector

### Competition Bureau Information Bulletin on Corporate Compliance Programs (cont'd)

- Consistent disciplinary procedures and incentives:
  - are important for deterrence purposes
  - demonstrate the seriousness with which the organization views conduct in a breach of the law
- Compliance should be considered for the purposes of employee evaluations, promotions and bonuses
- Appropriate and consistent disciplinary actions (up to and including dismissal and even legal action) should be taken for failing to comply with the compliance program or the law
  - Disciplinary actions should also be taken against managers who fail to take reasonable steps to prevent or detect misconduct

## Guidance from the private sector (cont'd)

### Enform Basic Safety Program for the Upstream Petroleum Industry

- Conveys Enform's expectations of the upstream petroleum industry regarding controls through which they manage safety
- Applies regardless of size (scaleable)

## Guidance from the private sector

### Enform Basic Safety Program for the Upstream Petroleum Industry (cont'd)

- Key safety control elements include:
  - Management involvement and commitment
    - Safety policy, guiding principles, safety responsibilities, management communication, monitoring
  - Hazard identification and risk control
    - Inspections, reporting, risk assessment, risk mitigation
  - Rules and standard work procedures
    - Legislative compliance, safety rules, enforcement
  - Training
    - Safety orientation, on-the-job training
  - Communication
    - Transfers safety program “from paper to practice”
  - Incident and accident reporting and investigation
  - Audit protocol

## Common Elements of Effective Governance

### Summary

- Board and senior management involvement and support
- Member of senior management appointed as chief compliance (privacy) officer
- Clear accountability including consistent disciplinary procedures and incentives
- Documentation including policies and procedures to demonstrate how (privacy) risks are identified and managed
- Monitoring and reporting procedures through which significant problems (including privacy breaches) are identified, escalated and resolved
- Internal audit or other independent validation of the effectiveness of the (information governance) program and key controls
- Training and education

## Guidance from the health sector

### Governance challenges

- Increasingly complex technological data sharing arrangements, including shared data repositories, are straining pre-existing structures for accountability
- Canadian privacy legislation does not expressly contemplate (let alone flesh out) collective accountability for health information
- The party designated to contract with technology parties on behalf of a number of health entities clearly plays an important role but also strains current legislative definitions
- Multi-purpose, ever-expanding data repositories are testing traditional notions of meaningful consent and, quite possibly, are creating too much focus on the mechanics of consent
- Even assuming clarity around legal authority and consent, there is an absence of clear, consistent data governance principles and practices
- The limited deployment of strong, comprehensive governance programs is relegating many data sharing projects to a very slow grind, with frustratingly slow progress

## Guidance from the health sector

### PHIPA

- Ontario Health Legislation actually legislates good governance where consent is impractical
- Prescribed entities under s.45(1) of *Ontario's Personal Health Information Protection Act* (PHIPA)
  - Commissioner must be satisfied that the entity has appropriate practices and procedures in place to protect the privacy of the individuals whose personal health information it receives
  - The sharing entity (HIC) also has an obligation to ensure that the entity has in place such practices
  - The overall governance structure is subject to review by the Commissioner every 3 years

## Privacy and security governance in practice

Canadian Institute for Health Information

Created in 1994, CIHI is a not for profit organization mandated by the Ministries of Health across Canada to:

- Coordinate the development and maintenance of an integrated approach to Canada's health information system; and
- Provide and coordinate the provision of accurate and timely information required to:
  - establish sound health policy;
  - effectively manage the Canadian health care system; and,
  - generate public awareness about factors that affect good health.

## Privacy and security governance in practice

### CIHI Stats

- CIHI has 27 data holdings with data from all jurisdictions in the country. On average CIHI receives close to:
  - 3.2 million records a month on drug data alone
  - 250,000 hospital records a month (specifically, from the Discharge Abstract Database)
  - Roughly 30 thousand Ontario mental health records per year
  - And data on 24 health professions (eg, doctors, nurses, physio and occupational therapists)

## Privacy and security governance in practice

### CIHI Stats (cont'd)

- CIHI has grown tremendously – from 150 employees in 1994 to a little over 750 in 2010
- CIHI has 6 offices across Canada and 32 Location Independent Workers – a highly mobile workforce
- From a privacy perspective, these numbers translate into sensitive personal health information about Canadians, and present risks to consider and manage

## Privacy and Security Governance Framework

Drivers	<b>Legal / Statutory</b>	Listings of applicable legislation and other recognized external criteria. Describe how applicable legislative requirements are identified, assessed, communicated and maintained.
	<b>Trust &amp; Confidence /Reputation</b>	Confidence of relevant government bodies, key stakeholders, public, users, etc.
	<b>Vision/Mandate</b>	Include Vision, Mission, Values, Strategic Direction documents, statements from code of conduct and privacy policy.
Governance Structure	<b>Organizational Structure</b>	Describe, starting with role of Board of Directors and senior management, Privacy Officer(s), committees, privacy and security functions.
	<b>Accountabilities</b>	Individual accountabilities for privacy and security including position descriptions and written mandates for relevant committees. Describe disciplinary procedures and incentives (eg. employee evaluations).
	<b>Policy Architecture</b>	Description/Chart of policy framework and coordination between privacy and security functions.
Risk Management	<b>Risk Identification Tools</b>	List tools to facilitate decision-making about appropriate data use and protection including PIA, TRA, Vulnerability Assessment, Penetration Testing, Flagging Mechanisms, etc.
	<b>Risk Mitigation and Acceptance Protocol</b>	Describe process whereby identified risks are either accepted or action plans to mitigate them are put into effect, including any follow-up process. Who decides which recommendations are accepted and based on what criteria?
	<b>Link to Compliance Monitoring</b>	Describe how action plans are linked into the compliance monitoring program to ensure that new mitigation strategies are monitored.
	<b>Benchmarking</b>	List any informal or formal benchmarking, including industry standard certifications (ISO).
	<b>Business Continuity /Disaster Recovery</b>	Describe Business Continuity Plan; Technology Recovery Plan and integration of privacy considerations.
Program Controls	<b>Policies</b>	List all privacy and information handling policies including frequency of review.
	<b>Standards/Procedures</b>	List all standards and procedures that relate to privacy and information handling.
	<b>Training and Awareness</b>	Describe privacy and security training policies including privacy and security orientation and ongoing training; other training resources (internal website, newsletter, awareness activities). Describe how privacy policies/standards/procedures are communicated to employees.
	<b>Retention and Destruction</b>	Describe policies, standards and processes.
	<b>Consent Management</b>	Describe policies and procedures that address the consent to be obtained for any collection, use or disclosure of personal information.
	<b>Breach Management Protocol</b>	List all policies, procedures, protocols and committees related to breach management.
	<b>Agreements</b>	List standard templates for data-sharing, outsourcers, clients, service providers, employees.
	<b>Third Party Vendor Management</b>	Describe vendor management program, outsourcing or policies including related procurement standards, etc.
	<b>Transparency</b>	List all publicly available documents including privacy policy, privacy notices or statements, brochure, website information, published PIA results. Describe policies on access and correction as well as dispute resolution and remediation.
Compliance & Reporting	<b>Ongoing Compliance Monitoring</b>	Describe risk-based monitoring program including application to third party service providers, as appropriate.
	<b>Audit</b>	List any internal or external audits conducted related to privacy and information handling.
	<b>Reporting</b>	List all reporting requirements, including to business operations management, senior management and the board as well as clients.

**Privacy and Security Governance Framework**

<b>Drivers</b>	
<b>Legal / Statutory</b>	List applicable legislation and other recognized external criteria. Describe how applicable legislative requirements are identified, assessed, communicated and maintained.
<b>Trust &amp; Confidence /Reputation</b>	Confidence of relevant government bodies, key stakeholders, public, users, etc.
<b>Vision/ Mandate</b>	Include Vision, Mission, Values, Strategic Direction documents, statements from code of conduct and privacy policy.

**Privacy and Security Governance Framework**

<b>Governance Structure</b>	
<b>Organizational Structure</b>	Describe, starting with role of Board of Directors and senior management, Privacy Officer(s), committees, privacy and security functions.
<b>Accountabilities</b>	Individual accountabilities for privacy and security including position descriptions and written mandates for relevant committees. Describe disciplinary procedures and incentives (eg. employee evaluations).
<b>Policy Architecture</b>	Description/Chart of policy framework and coordination between privacy and security functions.

**Privacy and Security Governance Framework**

<b>Risk Management</b>	
<b>Risk Identification Tools</b>	List tools to facilitate decision-making about appropriate data use and protection including PIA, TRA, Vulnerability Assessment, Penetration Testing, Flagging Mechanisms, etc.
<b>Risk Mitigation and Acceptance Protocol</b>	Describe process whereby identified risks are either accepted or action plans to mitigate them are put into effect, including any follow-up process. Who decides which recommendations are accepted and based on what criteria?
<b>Link to Compliance Monitoring</b>	Describe how action plans are linked into the compliance monitoring program to ensure that new mitigation strategies are monitored.
<b>Benchmarking</b>	List any informal or formal benchmarking, including industry standard certifications (ISO).
<b>Business Continuity /Disaster Recovery</b>	Describe Business Continuity Plan; Technology Recovery Plan and integration of privacy considerations.

**Privacy and Security Governance Framework**

<b>Program Controls</b>	
<b>Policies</b>	List all privacy and information handling policies including frequency of review.
<b>Standards/Procedures</b>	List all standards and procedures that relate to privacy and information handling.
<b>Training and Awareness</b>	Describe privacy and security training policies including privacy and security orientation and ongoing training; other training resources (internal website, newsletter, awareness activities). Describe how privacy policies/standards/procedures are communicated to employees.
<b>Retention and Destruction</b>	Describe policies, standards and processes.

**Privacy and Security Governance Framework**

<b>Program Controls (cont'd)</b>	
<b>Consent Management</b>	Describe policies and procedures that address the consent to be obtained for any collection, use or disclosure of personal information.
<b>Breach Management Protocol</b>	List all policies, procedures, protocols and committees related to breach management.
<b>Agreements</b>	List standard templates for data-sharing, outsourcers, clients, service providers, employees.
<b>Third Party Vendor Management</b>	Describe vendor management program, outsourcing or policies including related procurement standards, etc.
<b>Transparency</b>	List all publicly available documents including privacy policy, privacy notices or statements, brochure, website information, published PIA results. Describe policies on access and correction as well as dispute resolution and remediation.

**Privacy and Security Governance Framework**

<b>Compliance &amp; Reporting</b>	
<b>Ongoing Compliance Monitoring</b>	Describe risk-based monitoring program including application to third party service providers, as appropriate.
<b>Audit</b>	List any internal or external audits conducted related to privacy and information handling.
<b>Reporting</b>	List all reporting requirements, including to business operations management, senior management and the board as well as to clients.

## Privacy and security governance in practice

### The practical impact on program management

- Provides a coherent and comprehensive approach to enterprise-wide privacy and security management for any organization;
- Identifies, clarifies and sets out accountability hierarchically and across lines of business;
- Enables effective integration and coordination of privacy and security policies;
- Offers a snapshot that identifies all existing policies and practices – “It tells the story about how you handle information”;
- Equips decision-makers, privacy and security officers, and the entire governance structure with a holistic view of the organization’s information management practices;
- Helps identify policy gaps, as well as any areas of overlap and/or inconsistency; and
- Facilitates continuous improvement.

## Privacy and security governance in practice

### Keeping it vital

Privacy and security risks shift and change over time so the framework must:

- be a living document, updated as your organization's privacy and security programs evolve and mature;
- be informed by best practices for privacy, security and information management across the public and private sectors;
- be approved and endorsed by the highest levels within your organization; and
- be communicated, adopted, implemented, promoted – and be well understood at all levels within your organization.

## Privacy and security governance in practice

Final tips: Making it happen...

1. Consolidate existing documentation – you may have more than you know; look in other departments, too
2. Do an inventory/analysis of what you have – looking for gaps and overlaps
3. Identify senior management champions early – establish the business need
4. Design your framework
5. Create an action plan to develop your framework
6. Develop a comprehensive roll-out strategy using as many medi/fora as possible

# Thank you

Please feel free to contact us with any questions at:

[psnively@heenan.ca](mailto:psnively@heenan.ca)