ROGERS cybersecure catalyst

Protecting Data and Privacy Considerations

December 2025

Mike Gropp

OSEP, OSCP, GSEC, GCIH
mike.gropp@torontomu.ca

Senior Cybersecurity Advisor
Rogers Cybersecure Catalyst,
Toronto Metropolitan University

ROGERS cybersecure catalyst | Corporate Training

Agenda

- Welcome + introductions
- Why data protection and privacy matter for immigrants, refugees, and your programs
- Key Canadian and Ontario privacy rules and funder expectations
- Assess our own data lifecycle
- Common risk areas for your organization
- Practical safeguards you can implement in the next 3 months
- Resources and Q&A

Introductions in the chat

Expectations

Why does data protection and privacy matter?

Cybersecurity Threat Types

Regulatory Landscape

Personal Information Protection and Electronic Documents Act (PIPEDA)

- **Purpose:** Protect personal information in commercial activities across Canada.
- **Applies to:** Most private-sector businesses in Canada.
- **Key Principles (in Schedule 1):**
  - **Principle 4.1:** Accountability for personal information management.
  - **Principle 4.3:** Consent for collecting, using, disclosing personal information.
  - **Principal 4.7:** Security safeguards for protecting personal information.
  - **Sections in the Act 10.1-10.3:** Obligations for reporting data breaches.
- **Practical Implications:** Requires businesses to implement strong data protection measures and to report breaches.

General Enhancements Introduced by the Digital Privacy Act (DPA)

- **Purpose:** Update and strengthen PIPEDA with additional protections and clarity.
- **Key Changes:**
  - **Age of Consent (Section 6.1):** Clarifies that consent is valid only if the individual can reasonably understand the consequences of the collection, use, or disclosure of personal information.
  - **Business Transactions (Sections 7.2 & 7.3):** Details on how personal information can be handled without consent during business transactions to ensure business continuity and proper due diligence.
  - **Disclosure to Authorities (Section 7(3)c.1):** Allows disclosure of personal information to government institutions for law enforcement and national security without the individual's consent.

DPA (cont’)

- **Key changes (con’t)**
  - **Breach Notification Requirements (Sections 10.1 to 10.3):** Introduces mandatory breach notification rules when a breach poses a significant risk of harm to individuals.
  - **Employment Relationship Management (Section 7.3):** Permits organizations to handle personal information without consent when establishing, managing, or terminating an employment relationship.
- **Practical Implications:** Organizations are required to enhance data handling protocols, ensure clarity of consent, manage employee information in compliance with the Act, and follow strict breach notification procedures.

Bill C-27: Enhancing Canada's Digital and AI Regulation (Did not come into force)

Consumer Privacy Protection Act (CPPA):

- **Purpose:** Would have enhanced protection of personal information in commercial activities.
- **Provisions:**
  - Introduced stricter consent mechanisms and transparency requirements.
  - Established new rights for individuals to request deletion and data mobility.

Personal Information and Data Protection Tribunal Act:

- **Purpose:** Would have created a new tribunal to hear appeals on decisions made by the Privacy Commissioner under CPPA.
- **Provisions:**
  - Provided a formal process for penalizing non-compliance.
  - Strengthened enforcement of privacy laws.

Bill C-27: Enhancing Canada's Digital and AI Regulation (con’t)

Artificial Intelligence and Data Act:

- **Purpose:** Would have regulated AI systems to mitigate risks related to high-impact AI systems across international and interprovincial trade and commerce.
- **Provisions:**
  - Required certain measures to prevent biased outputs and risks of harm.
  - Mandated public reporting and transparency of AI systems.
  - Established prohibitions on using illegally obtained personal information in AI systems.

Ontario's Personal Health Information Protection Act (PHIPA)

- **Purpose:** Govern the collection, use, and disclosure of personal health information.
- **Applies to:** Health care providers and organizations in Ontario.
- **Key Sections:**
  - **Section 13:** Requires health information custodians to take steps to ensure that records are secure.
  - **Section 21:** Governs the consent and capacity for health information.
  - **Sections 29-36:** Conditions for the collection of personal health information.

PHIPA (con’t)

- **Key Sections (con’t)**
  - **Section 37:** Outlines the use of personal health information.
  - **Sections 38-49:** Set forth rules for the disclosure of health information**.**
- **Practical Implications:** Entities must implement robust security measures, manage consents, and ensure lawful use and disclosure of health data.

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

- **Purpose:** Regulate the collection, use, disclosure, and access to personal information by Ontario municipalities.
- **Applies to:** Ontario municipalities.
- **Key Sections:**
  - **Sections 4-5:** Detail the public's right to access municipal records, with certain protections for privacy.
  - **Section 27-33:** Governs the rules for collection, use, and disclosure of personal information.
- **Practical Implications:** Municipalities are required to implement policies and practices that protect personal information, ensure transparency, and maintain public trust through secure handling and access protocols.

Cybersecurity Considerations for Municipal Systems and Critical Infrastructure

- Federal guidelines emphasize cybersecurity's importance in managing municipal systems and protecting critical infrastructure.
- Robust security measures are essential to safeguard interconnected municipal operations and infrastructure.
- **Relevant Guidelines/Legislative Provisions:**
  - **National Strategy for Critical Infrastructure:** Guides the protection and resilience of critical infrastructure across sectors.
  - **Public Safety Canada's Action Plan for Critical Infrastructure:** Sets out strategies for enhancing the resilience of vital assets and systems.
- These frameworks support municipalities in implementing cybersecurity practices to defend against threats and ensure continuity of services.

Protection of Critical Cyber Systems Under Bill C-8

Overview: Bill C-8 introduces the Critical Cyber Systems Protection Act to enhance security of systems vital to national security and public safety.

Obligations for Operators:

- **Cyber Security Programs:** Must establish, implement, and maintain comprehensive programs.
- **Risk Mitigation:** Required to manage supply-chain and third-party risks.
- **Incident Reporting:** Mandatory reporting of cybersecurity incidents to the Communications Security Establishment .
- **Compliance with Directives:** Operators must follow directives issued by regulators .

Protection of Critical Cyber Systems Under Bill C-8 (con't)

Information Exchange and Enforcement

- **Information Sharing:** Allows sharing among regulators, provinces, and international partners, with strict confidentiality rules.
- **Enforcement:** Establishes compliance and penalty mechanisms for non-compliance.

Impact on Critical Infrastructure

- Enhances resilience and security of critical infrastructure against cyber threats.
- Ensures continuity of essential services such as telecommunications, energy, banking, and transportation.

Health Sector: Personal Health Information Protection Act

Specific Protections Unique to PHIPA:

- **Detailed Consent Requirements:** PHIPA requires explicit consent mechanisms for the collection, use, and disclosure of personal health information, ensuring patient awareness and involvement.
- **Patient Access Rights:** Patients have extensive rights to access and amend their health information, promoting transparency and patient control over personal data.
- **Health Information Networks:** Provisions for the use of electronic health records within health information networks to ensure secure and efficient handling of health data.

Takeaways

- Be clear why you collect client data and do not collect more than you need
- Get meaningful consent where required and be honest about who will see the data
- Put reasonable safeguards in place (technical, physical, and procedural)
- Give people a way to access or correct their information
- Have a process for handling and, if needed, reporting breaches

Data Lifecycle Assessment

Data Lifecycle Assessment Steps

1. List key data types you handle

1. Map the life cycle

1. Mark high risk flows

1. Connect to OPC’s 10 Principles

Step 1: List key data types you handle

- Immigration documents and ID (passports, PR cards, refugee claimant documents)
- Contact details (phone, WhatsApp, email, addresses)
- Case notes about trauma, violence, precarious status
- Program data (attendance lists, workshop registration forms)
- Health related information (mental health, disability, medication if applicable)

Step 2: List key data types you handle

- How do we collect it? (paper, Google Forms, email, WhatsApp, CMS, IRCC portal)
- Where is it stored? (local drives, cloud service, USB, CRM, paper cabinets)
- Who has access and from what devices? (staff laptops, personal phones, volunteers)
- Who do we share it with? (IRCC, other agencies, funders, landlords, lawyers)
- How long do we keep it and how do we destroy it?

Step 3: Mark high risk flows

- Staff using personal Gmail to send scanned passports to funders.
- WhatsApp or Facebook Messenger used to send safety-sensitive information for women fleeing violence.
- Case notes copied into personal notebooks or stored in unencrypted Word files on home computers.
- Zoom meetings where participant lists and chat logs are auto-saved to personal devices.

Step 4: Connect to OPC's 10 Principles

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure, and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

Discussion: Common Risks

Hot Topics

Third-party Risk: Questions to ask your vendors

1. What data about clients and staff does this vendor actually store?
2. Where is the data stored geographically? (Canada only, US, global)
3. What contractual language exists on security, breach notification, and data deletion on contract end?
4. How can we export and delete data if we leave the service?

Shadow IT & AI: Examples

- Staff paste a client's refugee narrative into a public generative AI tool to "improve" a letter to IRCC
- Intake worker uses a free AI translation site to translate documents with names, addresses, and legal status
- A funder-required reporting spreadsheet is uploaded to an AI tool for analysis, exposing hundreds of client records

Q&A

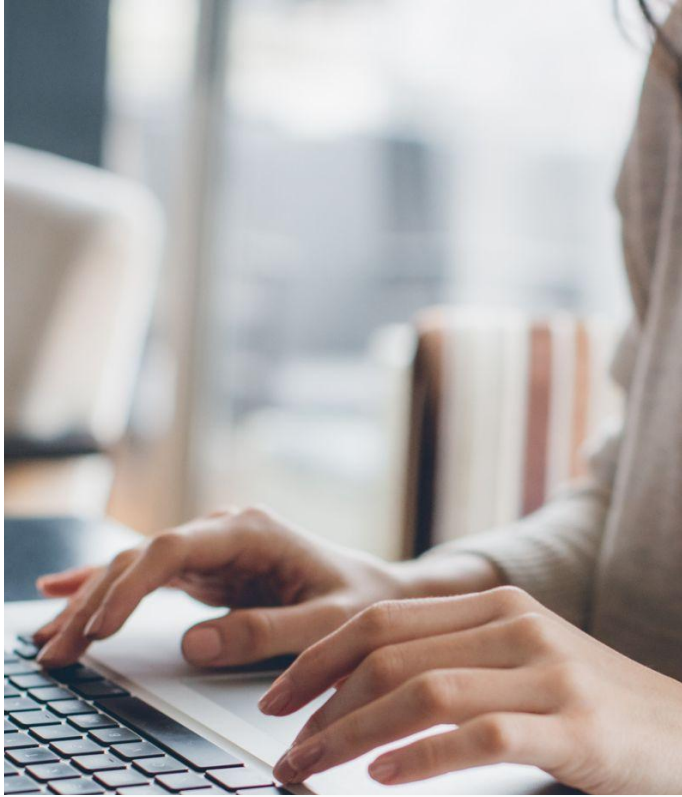
Okta Catalyst Cyber Clinic

Free, foundational cyber support for non-profits

One of the first of its kind in Canada, the Catalyst Cyber Clinic provides free cybersecurity support to under-resourced and vulnerable non-profit and social impact organizations in Canada. The Clinic is staffed by learners and graduates from Catalyst cyber training programs who, as Cyber Consultants, gain practical, real-world work experience while empowering vulnerable organizations to secure themselves.

The Clinic will launch its **first cohort in 2025, connecting 20 new training graduates with 5 non-profits for a 3 month engagement.**

We are a proud member of The Consortium of Cybersecurity Clinics



Toronto Metropolitan University

ROGERS cybersecure catalyst

okta

Resources

Resources: Immigrant & settlement sector privacy/security

- Data Ethics Protocols for Immigrant Serving Organizations and Newcomer Privacy Protection (research project, Toronto Metropolitan University)
- OCASI webinar: Cybersecurity and Privacy Awareness for IRCC funded organizations (with recording and slides)
- OCASI Client Management System (OCMS) overview, including privacy and confidentiality features
- OCMS description for the immigrant and refugee serving sector (SettlementAtWork)
- AMSSA 2 part webinar series: Introduction to Privacy and Security for B.C.'s Settlement and Integration Sector

Resources: Canadian nonprofits, charities, and cyber risk

- The Cybersecure Catalyst Cyber Clinic
- Carleton University, “Ready or Not: Data suggests charities in Canada vulnerable to data security threats”
- Imagine Canada, “What newly available data tells us about cybersecurity in Canadian nonprofits”
- Canadian Centre for Nonprofit Digital Resilience (CCNDR)

SettlementAtWork.Org

Upcoming Webinars
January 21, 2026: Baseline Cybersecurity Controls
March 11, 2026: Secure Use of Artificial Intelligence

Info@settlmentatwork.org

Continue the Conversation on SettleNet

https://oca.si/cyber