



**CAPTURE**

Canadian platform to increase usage of real-world evidence

Plateforme canadienne pour accroître l'usage de données probantes du monde réel

# Privacy, Security, and Data Sharing of Health Promotion Interventions and Evaluations: Key Learnings from The CAPTURE Project

February 2011

**Contents**

[Contents.....2](#)

[Introduction.....3](#)

[Background.....3](#)

[The CAPTURE Platform.....3](#)

[CAPTURE’s Scoping Review.....4](#)

[Canadian Privacy Legislation.....4](#)

[International Standards: The 10 Fair Information Privacy Principles.....5](#)

[Learning from Others.....6](#)

[Literature search.....6](#)

[Environmental scan and key informant interviews.....7](#)

[Summary of best practices.....7](#)

[A best practices case study: Population Data BC.....8](#)

[Working with Partners: Information Sharing Agreements.....9](#)

[A data framework for the CAPTURE Project.....10](#)

[Acknowledgments.....11](#)

[Appendix B – Translating Principles into Policies and Procedures .....18](#)

[Appendix C – Case study: Population Data BC.....23](#)

[For more information.....26](#)

## Introduction

In early 2010, the CAPTURE Project undertook a comprehensive scoping review to lay the groundwork for developing its framework for privacy, security and data sharing. As part of the CAPTURE Project's commitment to knowledge translation and exchange, this report synthesizes and shares the key learnings from this review. It is hoped that other Canadian health data sharing initiatives can benefit from this information.

## Background

In communities across Canada, there are many programs aimed at helping people reduce their risk of developing chronic diseases such as cancer, heart disease and diabetes. These primary prevention programs focus on modifying the risk factors that lead to chronic disease, such as obesity, smoking, inactivity and unhealthy eating.

Practitioners and program managers want to offer the most effective primary prevention programs for their community. To do this, they must regularly evaluate their activities. They also recognize that they can benefit from learning about the practices and experiences of others in different communities. This “real-world” evidence is as important as academic research for helping communities plan and manage effective primary prevention programs. However, the supports to help make this happen are currently lacking.

The Canadian Platform to Increase Usage of Real-World Evidence – or the CAPTURE Project – will help chronic disease prevention practitioners and program managers learn from what they do, and share that knowledge. Funded by the Canadian Partnership Against Cancer, CAPTURE is building a web-based shared measurement and learning platform for the evaluation of health promotion programs. Health promotion practitioners will also be supported to reflect on their practice and connect with others with similar interests. The platform will support communities of practice so practitioners can more easily learn from each other.

## The CAPTURE Platform

A unique feature of the CAPTURE platform will be the collection, storage and analysis of health promotion intervention and evaluation data. The platform will collect and store both de-identified and aggregate data to allow chronic disease prevention practitioners to manage their own interventions and evaluations. The platform will also provide access to non-identifiable, aggregate data for comparisons across programs, organizations, and initiatives. Once the platform is more fully populated, protocols that allow access to data for research purposes will be developed.

CAPTURE does no direct collection of data; it acts as a data custodian, a secondary collector of data from data providers (practitioners and program managers). Data providers (called Data stewards) contributing to the platform will remain the owners of their data and are responsible for its collection according to legislative requirements in their own jurisdiction. CAPTURE's role is to act as a service provider/server host for the platform and CAPTURE repository, and to

ensure appropriate and reasonable safeguards are in place to secure the data, the platform, the server, and backups.

As a data repository, the CAPTURE Project is committed to meet or exceed legislative requirements, industry standards, and best practices for privacy and security protection.

## CAPTURE's Scoping Review

In early 2010, the CAPTURE Project undertook a comprehensive scoping review to lay the groundwork for developing its framework for privacy, security and data sharing.

Components of the review included:

- A policy and legislative requirements review
- A literature review about design, development and implementation of a privacy framework for similar initiatives
- An environmental scan of similar initiatives across Canada
- Key informant interviews with three similar Canadian initiatives
- A review of current thinking and best practices internationally and within Canada's health system

This review resulted in a strategy and approach to guide the Project moving forward.

Please note that while the CAPTURE Project is a pan-Canadian initiative, it is physically located in British Columbia. Therefore, British Columbian sources are primarily used in this document. Readers should check with resources specific to their jurisdiction. Additionally, the examples used are applicable to data holdings of the CAPTURE Project, but may not be applicable to all health data sharing initiatives.

## Canadian Privacy Legislation

The British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA) defines "Personal Information" as "recorded information about an identifiable individual other than contact information".

Every province and territory has privacy legislation (Acts) governing the collection, use, and disclosure of personal information held by private or public bodies. Many jurisdictions also have health-specific privacy legislation. These Acts, which are guided by international standards, provide the public with a right to privacy of their personal information, as well as access to view and correct their personal information. In addition, there are provisions for, and exceptions to, consent for the use and disclosure of personal information, including for research purposes. However, the conditions for use or disclosure vary in detail and stringency across jurisdictions. Oversight for the Acts is through either an independent commissioner or ombudsman authorized to receive and investigate complaints.

There are also two federal privacy Acts, which apply to federal government departments and agencies, and to federally-regulated private sector organizations.

Different Acts will apply depending on the type of organization that is collecting, using, disclosing and/or storing personal information. This includes universities, government institutions, health authorities, municipalities, private sector and non-profit organizations. See [Appendix A](#) for a listing of privacy legislation by jurisdiction.

## **International Standards: The 10 Fair Information Privacy Principles**

In Canada, there is a voluntary national standard for the protection of personal information – the [CSA Model Code for the Protection of Personal Information](#) – which was developed by the Canadian Standard Association in collaboration with business, consumer organizations and governments.

This code is the 10 Fair Information Privacy Principles (FIPs), which underlie most privacy legislation developed around the world. These 10 principles represent the highest standards from which to base privacy best practices, and are frequently used to form the foundation of privacy and security policies. They are also used to align privacy practices across national, territorial, and provincial boundaries.

### *Principle 1: Accountability*

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

### *Principle 2: Identifying Purposes*

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

### *Principle 3: Consent*

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.

### *Principle 4: Limiting Collection*

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

### *Principle 5: Limiting Use, Disclosure and Retention*

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfillment of those purposes.

### *Principle 6: Accuracy*

Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

### *Principle 7: Safeguards*

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

*Principle 8: Openness*

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

*Principle 9: Individual Access*

Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

*Principle 10: Challenging Compliance*

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

See [Appendix B](#) for how these principles were applied to the CAPTURE Project to provide the foundation for developing policies and procedures.

## Learning from Others

There are a number of Canadian organizations and initiatives that manage the collection, storage and analysis of personal health information and program data. The CAPTURE Project sought to learn from others' experiences by conducting a literature search, an environmental scan of similar initiatives, and key informant interviews.

### Literature search

The scoping review included a limited literature search. The following articles and references were identified as the most relevant for the CAPTURE Project's deliberations about how to design, develop and implement its platform, repository and operational policies and procedures:

- **Building a Pan-Canadian Primary Care Sentinel Surveillance Network: Initial Development and Moving Forward**<sup>1</sup> (July-August 2009)
- **COACH Guidelines for the Protection of Health Information**<sup>2</sup> published by Canada's Organization for the Advancement of Computers in Health (2009)
- **North American Association of Central Cancer Registries: Surveillance Data Access and Confidentiality Protection in Canadian Cancer Registries**<sup>3</sup> (April 2002)
- **Key Steps for Responding to a Privacy Breach**<sup>4</sup> published by the Office of the Information and Privacy Commissioner for Canada (2006)
- **CIHR Best Practices for Privacy in Health Research**<sup>5</sup> published by the Canadian Institutes of Health Research (September 2005)

<sup>1</sup> <http://www.jabfm.com/cgi/reprint/22/4/412>

<sup>2</sup> [http://coachorg.com/publications/privacy\\_&\\_security\\_guidelines/about\\_the\\_guidelines.htm](http://coachorg.com/publications/privacy_&_security_guidelines/about_the_guidelines.htm)

<sup>3</sup> [www.naacrr.org/filesystem/pdf/BanffReport7-10-02.pdf](http://www.naacrr.org/filesystem/pdf/BanffReport7-10-02.pdf)

<sup>4</sup> [http://www.priv.gc.ca/information/guide/2007/gl\\_070801\\_02\\_e.cfm](http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.cfm)

<sup>5</sup> <http://www.cihr-irsc.gc.ca/e/29072.html>

- **Data, Data, Everywhere: BC Linked Health Database<sup>6</sup>**, Centre for Health Services and Policy Research at UBC (April 2005)
- **Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Personal Health Information<sup>7</sup>** published by the Canadian Institute for Health Information (2007)

### *Environmental scan and key informant interviews*

The CAPTURE Project completed an environmental scan of relevant initiatives and conducted a number of key informant interviews to determine the real-life practices currently in use.

The organizations and initiatives that were reviewed include:

- BC Generations Project – [www.bcgenerationsproject.ca](http://www.bcgenerationsproject.ca)
- Human Early Learning Partnership (HELP) – [www.earlylearning.ubc.ca](http://www.earlylearning.ubc.ca)
- Interdisciplinary Capacity Enhancement (ICE): advancing the science to reduce tobacco use – [www.ice.crchum.qc.ca](http://www.ice.crchum.qc.ca)
- Population Data BC – [www.popdata.bc.ca](http://www.popdata.bc.ca)
- Rick Hansen Spinal Cord Injury Registry – [www.rickhansenregistry.org](http://www.rickhansenregistry.org)
- School Health Action, Planning and Evaluation System (SHAPES) – [www.shapes.uwaterloo.ca](http://www.shapes.uwaterloo.ca)

### *Summary of best practices*

Across the literature review, environmental scan and interview, the CAPTURE Project identified overall alignment of policies and practices for privacy, security and data sharing. There were some variations in scope between initiatives; some were primary collectors of personal information, while others acted as secondary collectors of data. This resulted in specific privacy issues for each initiative and, predictably, some variations in practices. However, this review process demonstrated generally consistent themes for privacy, security and data sharing. The following features, processes, and requirements were identified as part of a comprehensive privacy and security risk management framework:

1. A Privacy Officer to oversee and monitor compliance, maintain up-to-date policies, and manage day-to-day operations related to privacy, security and data sharing
2. Staff privacy training on an annual basis
3. Staff confidentiality agreements
4. Information Sharing Agreements with data stewards

<sup>6</sup> <http://www.chspr.ubc.ca/research/data/cprn>

<sup>7</sup> [http://www.cihi.ca/cihiweb/dispPage.jsp?cw\\_page=RC\\_10\\_E](http://www.cihi.ca/cihiweb/dispPage.jsp?cw_page=RC_10_E)

5. Limited collection of information necessary to fulfill the intended purpose
6. Retention of information only for as long as needed and securely destroyed when no longer required
7. A Research Ethics Board (REB) to oversee secondary use of information and provide appropriate approvals for research
8. A Data Access Request process for research access to data
9. Technical security safeguards such as Secure Socket Layer (SSL) technology; secure on-site storage and off-site backup; restricted access to authorized personnel; encryption of stored data; dedicated secure servers; firewalls; audit trails; passwords; 128-bit encryption for transmission of data; and compliance with ISO27002 requirements for information security
10. Multi-zone data facilities with layers of protection including locks and alarms; video surveillance; re-enforced walls/doors; and restricted access
11. Separation of identifiers from content data
12. Use of de-identified, aggregate information to achieve objectives
13. Where data linkage occurs, identifiers are removed and replaced with a unique identifier to allow linkages under strictly controlled conditions
14. Public communication on a website, including policies and frequently asked questions
15. A Privacy Impact Assessment<sup>8</sup>
16. Privacy and security policies aligned with the 10 Fair Information Principles
17. A privacy toolkit to be used by data custodians, which includes any relevant consent forms, public communication, policies and procedures, and agreements.

### ***A best practices case study: Population Data BC***

Guiding principles and best practices can provide high-level direction for the development of an organization's policies and procedures around privacy, security and data sharing. The next step for an organization is to embed these concepts into its day-to-day operations.

The information gathered by the CAPTURE Project on Population Data BC's practices provides a useful, real-life example of how this can be done. Population Data BC's comprehensive

---

<sup>8</sup> A Privacy Impact Assessment (PIA) is a best practice risk management exercise that identifies and documents privacy issues and risks under applicable legislation, related to the personal information collection, use and disclosure by a project, initiative or organization. It is used to inform and to communicate with senior executive, stakeholders, partners, the public, and the Privacy Commissioner of the intended and actual information management practices in place and of the due diligence performed. PIAs also offer a method for documenting work flows and data flows, proposed recommendations and mitigation strategies to reduce privacy and security risks, and for ensuring senior executive are aware of these risks and sign-off prior to implementation.

approach to privacy, security and data sharing is seen across the organization's operations, including:

- Governance
- Information Sharing Agreements
- Data holdings
- A framework for data access requests
- Privacy and security

The Population Data BC case study is provided in [Appendix C](#).

### **Working with Partners: Information Sharing Agreements**

Information Sharing Agreements (ISAs)<sup>9</sup> are an essential tool for identifying the accountabilities of different parties in the use, sharing, and access to data, both identifiable and aggregate. They provide a clear articulation of expectations, roles and responsibilities between parties. Information Sharing Agreements enhance the transparency and accountability of the parties involved with respect to data flows of personal information and how the privacy of individuals is being protected.

ISAs are especially critical for exchanges between a public body and another jurisdiction, even if they are already authorized/required by legislation. Before doing so, it must define the conditions under which it is prepared to participate in the sharing, and demonstrate a commitment to monitoring compliance over time.

Information Sharing Agreements generally include the following, though the content of each agreement may vary depending on the requirements of each initiative:

- The names of the parties
- Purpose of the agreement
- The legal authority for sharing or exchange of information
- Ownership of information
- Contact name (e.g. designated data steward)
- Details of what information is to be shared
- How the information is used and disclosed
- Research purpose and requirements

---

<sup>9</sup> The purpose an Information Sharing Agreement is to document the terms and conditions of the exchange of certain personal information by the Parties, in compliance with applicable legislation.

- The mechanism for sharing
- How accuracy and quality of information is maintained
- Confidentiality and privacy
- Security and access
- Retention and destruction
- Any additional responsibilities of the parties including
- Privacy breach and security incident management
- Modifications
- Dispute resolution
- Termination for breach or convenience
- Consequences of improper use or disclosure
- Periodic audits for compliance
- Indemnification
- Limitation of liability
- Representations and warranties
- Governing law

It is important to note that ISAs must always be tailored to address the nuances of each project or initiative. ISA development can benefit from expert advice, such as legal counsel. A number of guidelines for ISA development are available on the web.

### **A data framework for the CAPTURE Project**

The CAPTURE Project's collection, use, disclosure and retention of personal information is governed by the *BC Freedom of Information and Protection of Privacy Act*. It is subject to the independent oversight of the Information and Privacy Commissioner for British Columbia.

The CAPTURE Project's scoping review resulted in a plan for a framework for privacy, security and data sharing. Although the Project is still refining the scope and details for data sharing, this framework plan will guide the CAPTURE project team in making design, development and implementation decisions that ensure compliance with legislation and principles and the adoption of industry standards and best practices for privacy, security and data sharing.

Key elements include:

1. The adoption of the internationally-recognized 10 Fair Information Privacy Principles as the basis for the CAPTURE Project's privacy and security policies;
2. Establishing comprehensive information sharing and terms of use agreements;
3. Identifying data holdings and the purposes for collection, use and disclosure;
4. Ensuring that the appropriate technical and physical security safeguards are in place;
5. Communicating CAPTURE's privacy practices with stakeholders, including the public.

The CAPTURE Project recognizes that achieving and maintaining excellence in privacy and security compliance is an ongoing process requiring attention on a day-to-day basis. Once the framework is implemented, the Project will initiate continually monitor it and review every two years to ensure that its policies and procedures are relevant, up-to-date and reflect current best practices.

For more information about the CAPTURE Project's information privacy practices, please contact [privacy@thecaptureproject.ca](mailto:privacy@thecaptureproject.ca).

### Acknowledgments

The CAPTURE Project thanks Ruth Yeo, who conducted the Privacy, Security and Data Sharing Scoping review, Ed McIvor and Heather Epstein who reviewed this document, and the organizations and individuals who contributed to its development.

- Mari-Alice Jolin and Janice Tiessen, ICE Program
- Dr. Steve Manske, SHAPES
- Suhail Marino, Population Data BC
- Dr. Marilyn Borugian, BC Generations Project
- Dr. Bev Holmes, Michael Smith Foundation for Health Research
- Gina Borza, United Way of the Lower Mainland
- Diane Smylie, Jean Tweed Centre
- Alison Osborne, Monkey Hill Health Communications

## Appendix A – Privacy Legislation by Canadian Jurisdiction<sup>10</sup>

Jurisdiction	Legislation	Entities covered by Legislation
Federal	<b><i>Privacy Act, R.S.C. 1985, c. P-21</i></b>	<ul style="list-style-type: none"> <li>Federal government institutions (any department or ministry of state of the Government of Canada listed in the schedule to the Act or any body or office listed in the schedule to the Act).</li> </ul>
	<b><i>Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5</i></b>	<ul style="list-style-type: none"> <li>Organizations that collect, use and disclose personal information in the course of a commercial activity (e.g., health care providers in private practice, pharmacies, pharmaceutical companies, etc.)<sup>3</sup> which takes place within a province unless the province has enacted legislation deemed by the Governor in Council to be substantially similar to the Act.</li> <li>Federal works, undertakings and businesses that collect, use or disclose personal information, including personal information about employees in any province or territory.</li> <li>All personal information collected, used or disclosed in cross-border commercial transactions.</li> <li>Does not apply to government institutions subject to the <i>Privacy Act</i>.</li> </ul>
British Columbia	<b><i>Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165</i></b>	<ul style="list-style-type: none"> <li>Public bodies (e.g., governmental bodies, health authorities, hospitals, mental health facilities and universities).</li> </ul>
	<b><i>Personal Information Protection Act, S.B.C. 2003, c. 63</i></b>	<ul style="list-style-type: none"> <li>All organizations (e.g., health care providers in private practice, pharmacies, pharmaceutical companies, not-for-profit organizations).</li> <li>Does not apply to personal information if <i>Freedom of Information and Protection of Privacy Act</i> applies.</li> </ul>
Alberta	<b><i>Health Information Act, R.S.A.</i></b>	<ul style="list-style-type: none"> <li>Applies to data custodians with</li> </ul>

<sup>10</sup> from the Canadian Institutes of Health Research (CIHR) and COACH Guidelines for the Protection of Health Information

Jurisdiction	Legislation	Entities covered by Legislation
	<p><b>2000, c. H-5</b></p>	<p>respect to health information (e.g., health professionals, health care facilities, regional health authorities, provincial health boards).</p> <ul style="list-style-type: none"> <li>• Legislation also impacts research ethics committees and researchers.</li> </ul>
	<p><b><i>Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25</i></b></p>	<ul style="list-style-type: none"> <li>• Public bodies (e.g., government departments, educational bodies, health care bodies and designated agencies, boards and commissions).</li> <li>• Does not apply to health information in records of a public body that is a data custodian as defined in the <i>Health Information Act</i>.</li> </ul>
	<p><b><i>Personal Information Protection Act, S.A. 2003, c. P-6.5</i></b></p>	<ul style="list-style-type: none"> <li>• All organizations, including not-for-profit, corporations, professional regulatory associations.</li> <li>• Does not apply to health information (as defined in the <i>Health Information Act</i>) where the information is collected, used or disclosed by an organization for health care purposes including health research and management of the health care system.</li> </ul>
	<p><b><i>Municipal Government Act, R.S.A. 2000, c. M-26</i></b></p>	<ul style="list-style-type: none"> <li>• Municipalities.</li> </ul>
Saskatchewan	<p><b><i>The Health Information Protection Act, S.S. 1999, c. H-0.021</i></b></p>	<ul style="list-style-type: none"> <li>• Trustees with respect to personal health information (e.g., government institutions, regional health authorities, health professionals, health care organizations, professional regulatory bodies).</li> <li>• Legislation also impacts researchers.</li> </ul>
	<p><b><i>The Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01</i></b></p>	<ul style="list-style-type: none"> <li>• Government institutions (e.g., government departments, Crown Corporations, designated provincial boards, bodies and agencies).</li> <li>• Does not apply to information that constitutes personal health information as defined in <i>The Health Information Protection Act</i>.</li> </ul>
	<p><b><i>The Local Authority Freedom of</i></b></p>	<ul style="list-style-type: none"> <li>• Local authorities (e.g., municipalities,</li> </ul>

Jurisdiction	Legislation	Entities covered by Legislation
	<b><i>Information and Protection of Privacy Act, S.S. 1990-91, c. L-27.1</i></b>	<p>universities, regional health authorities, special care homes, designated boards, commissions and bodies).</p> <ul style="list-style-type: none"> <li>• Does not apply to information that constitutes personal health information as defined in <i>The Health Information Protection Act</i>.</li> </ul>
<b>Manitoba</b>	<b><i>The Personal Health Information Act, C.C.S.M., c. P-33.5</i></b>	<ul style="list-style-type: none"> <li>• Trustees with respect to personal health information (e.g., health professionals, health care facilities, public bodies (including government departments and universities), health services agencies).</li> <li>• Legislation also impacts health information privacy committees, the institutional research review committees and researchers.</li> </ul>
	<b><i>The Freedom of Information and Protection of Privacy Act, C.C.S.M., c. F-175</i></b>	<ul style="list-style-type: none"> <li>• Public bodies (e.g. universities, certain hospitals, regional health authorities, municipalities, government departments and agencies).</li> <li>• Does not apply to personal health information to which the <i>Personal Health Information Act</i> applies.</li> </ul>
<b>Ontario</b>	<b><i>Personal Health Information Protection Act, S.O. 2004, c. 3</i></b>	<ul style="list-style-type: none"> <li>• Health information custodians, and agents of health information custodians, with respect to personal health information (e.g., Ontario Ministry of Health and Long-Term Care, public health units, hospitals, health care practitioners who provide health care, long-term care facilities, pharmacies, medical laboratories, ambulances, community health and mental health programs whose primary purpose is health care, Canadian Blood Services).</li> <li>• Legislation also provides rules for research ethics boards, health data institutes, prescribed registries, persons who provide goods and services that enable a custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, recipients of health information (e.g.</li> </ul>

Jurisdiction	Legislation	Entities covered by Legislation
		<p>researchers, employers and insurers).</p> <ul style="list-style-type: none"> <li>The legislation also applies to all persons with respect to the collection, use and disclosure of the health number.</li> </ul>
	<p><b><i>Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F-31</i></b></p>	<ul style="list-style-type: none"> <li>Institutions (e.g., ministries, agencies, boards and most commissions of the government of Ontario, community colleges).</li> <li>Where a health information custodian is also an institution under the <i>Freedom of Information and Protection of Privacy Act</i> "FIPPA") or a part of an institution under FIPPA, FIPPA continues to apply to such a health information custodian only in some circumstances.</li> <li>Where a FIPPA institution is not a health information custodian, only FIPPA applies, even where information at issue is health information.</li> </ul>
	<p><b><i>Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56</i></b></p>	<ul style="list-style-type: none"> <li>Institutions (e.g. municipalities, boards of health, designated agencies, boards, commissions, corporations or other bodies)</li> </ul>
Quebec	<p><b><i>An Act respecting Access to documents held by public bodies and the protection of personal information, R.S.Q., c. A-2.1</i></b></p>	<ul style="list-style-type: none"> <li>Public bodies (e.g., universities, CEGEP network of higher education institutions, health care facilities, government departments and agencies).</li> </ul>
	<p><b><i>An Act respecting the Protection of personal information in the private sector, R.S.Q., c. P-39.1</i></b></p>	<ul style="list-style-type: none"> <li>Persons carrying on an enterprise (e.g., health care providers in private practice, pharmacies and private research companies).</li> </ul>
New Brunswick	<p><b><i>Protection of Personal Information Act, S.N.B. 1998, c. P-19.1</i></b></p>	<ul style="list-style-type: none"> <li>Public bodies (e.g., government departments, school boards, regional health authorities).</li> </ul>
Nova Scotia	<p><b><i>Freedom of Information and Protection of Privacy Act, S.N.S. 1993, C. 5</i></b></p>	<ul style="list-style-type: none"> <li>Public bodies (e.g., universities, hospitals, government departments and agencies).</li> </ul>
	<p><b><i>Municipal Government Act, S.N.S. 1998, c. 18</i></b></p>	<ul style="list-style-type: none"> <li>Municipalities.</li> </ul>

Jurisdiction	Legislation	Entities covered by Legislation
<b>Prince Edward Island</b>	<b><i>Freedom of Information and Protection of Privacy Act</i>, R.S.P.E.I., c. F-15.01</b>	<ul style="list-style-type: none"> <li>Public bodies (e.g., government departments, agencies, boards, designated education and health bodies).</li> </ul>
<b>Newfoundland and Labrador</b>	<b><i>Access to Information and Protection of Privacy Act</i><sup>5</sup>, S.N.L. 2002, c. A-1.1</b>	<ul style="list-style-type: none"> <li>Public bodies (e.g., universities, health boards, municipalities, government departments).</li> </ul>
<b>Yukon</b>	<b><i>Access to Information and Protection of Privacy Act</i>, R.S.Y. 2002, c. 1</b>	<ul style="list-style-type: none"> <li>Public bodies (e.g., government departments, agencies, boards, commissions and corporations).</li> </ul>
<b>Northwest Territories</b>	<b><i>Access to Information and Protection of Privacy Act</i>, S.N.W.T. 1994, c. 20</b>	<ul style="list-style-type: none"> <li>Public bodies (e.g., government departments, agencies, boards).</li> </ul>
<b>Nunavut</b>	<b><i>Access to Information and Protection of Privacy Act</i>, S.N.W.T. 1994, c. 20, as duplicated for Nunavut by s. 29 of the <i>Nunavut Act</i>, S.C. 1993, c. 28</b>	<ul style="list-style-type: none"> <li>Public bodies (e.g., government departments, agencies, boards).</li> </ul>



## Appendix B – Translating Principles into Policies and Procedures

CAPTURE must establish a Privacy and Security Policy for the protection of personal information following the fair information principles and the requirements set out under FIPPA in the management of data it holds. The purpose of the Privacy and Security Policy is to respect the privacy of users and the requirements of the data providers (data stewards), and to protect against unauthorized access, use, disclosure, and destruction.

Content and features of the Privacy and Security Policy and Procedures should include, but is not limited to, the following considerations:

Principle	Policies	Procedures
<p><b>Principle 1: Accountability</b> An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.</p>	<ul style="list-style-type: none"> <li>• The CAPTURE Advisory Board will provide privacy governance and oversight to the project</li> <li>• A Privacy Officer will be designated</li> <li>• All staff must receive privacy training and be aware of the Privacy Policy and Procedures</li> <li>• All agreements and legal contracts should be reviewed by legal advisors</li> <li>• CAPTURE will establish Privacy and Security Policies including a Privacy Breach Management policy</li> <li>• CAPTURE users will agree to acceptable use policies through a Terms of Use Agreement</li> <li>• CAPTURE staff will sign a Confidentiality Agreement</li> </ul>	<ul style="list-style-type: none"> <li>• The Privacy Officer will provide privacy, security and data sharing oversight regarding the handling of personal information; ensure policies and procedures are up-to-date; respond to privacy breaches and complaints; conduct Privacy Impact Assessments; facilitate agreements and manage day-to-day responsibilities for privacy.</li> <li>• An external privacy advisor may be engaged to provide advice, act as a sounding board, and conduct periodic privacy audits to monitor compliance.</li> <li>• Procedures will be in place to manage privacy breaches to CAPTURE data.</li> </ul>
<p><b>Principle 2: Identifying Purposes</b> The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.</p>	<ul style="list-style-type: none"> <li>• Data Stewards are responsible for ensuring that the legal authority exists for the disclosure of personal information.</li> <li>• Secondary use for research may be in-scope (process to be defined)</li> </ul>	<ul style="list-style-type: none"> <li>• Information Sharing Agreements must be in place between CAPTURE and data steward(s) for the holding, using, disclosing and retaining of data received from Data Steward(s).</li> <li>• Data Stewards should inform individuals that their personal information may be entered, stored and aggregated for use through CAPTURE.</li> <li>• CAPTURE has the authority pursuant to FIPPA and</li> </ul>

Principle	Policies	Procedures
		<p>under Information Sharing Agreements to engage in research in accordance with signed Research Agreements and with prior written approval of a Research Ethics Committee (process to be defined).</p>
<p><b>Principle 3: Consent</b> The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.</p>	<ul style="list-style-type: none"> <li>• CAPTURE does not perform any direct collection of personal information and is only engaged in the secondary use or secondary disclosure of personal information initially collected by Data Steward(s) and under the terms and conditions of an Information Sharing Agreement.</li> </ul>	<ul style="list-style-type: none"> <li>• CAPTURE relies on Data Steward(s) to collect personal information in a lawful manner and in accordance with jurisdictional legislation.</li> <li>• Where consent is required, CAPTURE relies on the Data Steward(s) to obtain appropriate consent for collection, use and disclosure of personal information</li> <li>• Research Ethics Committee will confirm whether the consent is appropriate for the requested uses of data (process to be defined).</li> </ul>
<p><b>Principle 4: Limiting Collection</b> The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.</p>	<ul style="list-style-type: none"> <li>• CAPTURE only receives data elements that are necessary for the fulfilment of its role in supporting the dissemination of interventions, evaluations, and learnings about chronic disease prevention programs.</li> </ul>	<ul style="list-style-type: none"> <li>• CAPTURE will define what data elements it requires and which are necessary to fulfill its role and mandate.</li> <li>• CAPTURE will design and develop the platform to comply with the principle of 'least information'.</li> </ul>
<p><b>Principle 5: Limiting Use, Disclosure and Retention</b> Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfillment of those purposes</p>	<ul style="list-style-type: none"> <li>• CAPTURE only uses and discloses data for purpose authorized by the Data Steward(s) pursuant to signed Information Sharing Agreements</li> <li>• If secondary use for research is contemplated, researchers who wish to access data held by CAPTURE must submit a request which will be reviewed and approved by CAPTURE and an established Research Ethics Committee.</li> <li>• Only a limited number of authorized CAPTURE staff with controlled and monitored access will be permitted to access the data.</li> <li>• CAPTURE will retain the minimal amount</li> </ul>	<ul style="list-style-type: none"> <li>• Personal identifiers will be stored separately from Content Data.</li> <li>• Information Sharing Agreements signed with Data Steward(s) will specify only CAPTURE staff in certain roles may access data (e.g. for ongoing support, maintenance, back-ups, problem resolution)</li> <li>• Access to personal identifiers and content data will be restricted physically and technically.</li> <li>• CAPTURE will establish a Research Agreement and process for extracting data to ensure that only approved data is disclosed.</li> <li>• Information Sharing Agreement between CAPTURE and Data Stewards should outline the uses, conditions for sharing, storage, retention and destruction of data.</li> </ul>

Principle	Policies	Procedures
	<p>of personal information for its defined purpose(s).</p> <ul style="list-style-type: none"> <li>• CAPTURE will retain data provided by Data Steward(s) as specified in the Information Sharing Agreement.</li> <li>• CAPTURE will periodically review whether the data continues to be needed.</li> <li>• Where CAPTURE determines it is no longer needed, data will be securely destroyed as per the Information Sharing Agreement.</li> <li>• CAPTURE will consult with relevant Privacy Commissioners and government bodies prior to undertaking any data sharing that is deemed to be exceptional or precedent-setting in scope.</li> </ul>	<ul style="list-style-type: none"> <li>• CAPTURE will work collaboratively with its partners and stakeholders including those individuals or organisations that provide data (Data Stewards), and the Office of the Information and Privacy Commissioner for BC (OIPC BC).</li> </ul>
<p><b>Principle 6: Accuracy</b> Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.</p>	<ul style="list-style-type: none"> <li>• As CAPTURE holds data initially collected by Data Steward(s) it is the responsibility of the Data Steward(s) to ensure the accuracy of the data collected and subsequently submitted to the CAPTURE repository.</li> <li>• CAPTURE will update its data holdings upon receipt of updated data from Data Steward(s).</li> <li>• CAPTURE will perform quality checks to ensure that data received is complete.</li> </ul>	<ul style="list-style-type: none"> <li>• Data received by CAPTURE from Data Steward(s) will be reviewed to ensure completeness and consistency.</li> <li>• CAPTURE will incorporate new data as soon as possible to make the most recent data available for CAPTURE users.</li> </ul>
<p><b>Principle 7: Safeguards</b> Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.</p>	<ul style="list-style-type: none"> <li>• CAPTURE will utilize reasonable physical safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use of modification of Data.</li> <li>• CAPTURE will utilize reasonable technical safeguards to protect against loss, theft, unauthorized access, disclosure, copying, or use of modification of Data.</li> <li>• CAPTURE will comply with ISO27002</li> </ul>	<ul style="list-style-type: none"> <li>• CAPTURE will ensure a secure physical area with locks, alarms, monitored electronic access, separately locked and alarmed server room.</li> <li>• CAPTURE will utilize technical security safeguards such as: <ul style="list-style-type: none"> <li>○ Isolated network with firewall protection</li> <li>○ Separate logins and passwords</li> <li>○ Two factor authentication</li> <li>○ Audit logs monitored for intrusion detection</li> </ul> </li> </ul>

Principle	Policies	Procedures
	<p>standards for information security</p> <ul style="list-style-type: none"> <li>• CAPTURE will utilize administrative safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use, and modification of data.</li> </ul>	<ul style="list-style-type: none"> <li>○ and attempts</li> <li>○ at unauthorized access</li> <li>○ Access granted on a 'need to know' basis</li> <li>○ All data backed up on secure servers and encrypted media</li> <li>○ Encrypted back up media in a secure off-site location</li> <li>• CAPTURE staff will complete privacy awareness training</li> <li>• All CAPTURE staff will sign a confidentiality agreement</li> <li>• CAPTURE staff will only have access to data on a 'need to know' and 'least privilege' basis in accordance with their job functions</li> <li>• A limited number of CAPTURE staff will be authorized to handle the data.</li> <li>• All accesses to data will be logged in an audit trail that is routinely monitored</li> <li>• All data transfers to CAPTURE will be via encrypted secure file transfers</li> </ul>
<p><b>Principle 8: Openness</b> An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.</p>	<ul style="list-style-type: none"> <li>• CAPTURE will maintain a public website for informing stakeholders, partners, and the public of its purpose and mandate</li> <li>• CAPTURE will post its Privacy and Security Policies on its website or make them available upon request.</li> <li>• CAPTURE will keep relevant oversight authorities, the general public, stakeholders and participants aware of its privacy and security practices and how it protects the data to the highest reasonable level of standards</li> </ul>	<ul style="list-style-type: none"> <li>• CAPTURE will make its Privacy and Security Policies available on its website or upon request.</li> <li>• CAPTURE will provide FAQs on its website related to its privacy and security practices</li> <li>• Queries will be directed to the designated Privacy Officer</li> </ul>
<p><b>Principle 9: Individual Access</b> Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal</p>	<ul style="list-style-type: none"> <li>• Pursuant to Information Sharing Agreements with Data Steward(s), all requests from individuals (public) for access to or correction of data must be</li> </ul>	<ul style="list-style-type: none"> <li>• If contacted, CAPTURE will inform individuals that they must directly contact the primary data collector (Data Steward).</li> </ul>

Principle	Policies	Procedures
<p>information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.</p>	<p>referred to the original collector of the data.</p> <ul style="list-style-type: none"> <li>Only relevant Data Steward(s) have the authority to release information they have collected (CAPTURE does not have legal authority to do so).</li> </ul>	
<p><b>Principle 10: Challenging Compliance</b>  An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.</p>	<ul style="list-style-type: none"> <li>Concerns regarding CAPTURE's compliance with FIPPA, its Privacy Policy, and Information Sharing Agreements with Data Steward(s) will be sent directly to the designated CAPTURE Privacy Officer.</li> </ul>	<ul style="list-style-type: none"> <li>All complaints will be logged, reviewed and followed up by the Privacy Officer.</li> <li>Should the Privacy Officer's response not be satisfactory, complaints will be escalated to the Office of the Information and Privacy Commissioner for BC.</li> <li>CAPTURE will work to improve any policies, procedures or practices where areas for improvement are identified.</li> </ul>

## Appendix C – Case study: Population Data BC

### **Background**

Population Data BC offers a platform to facilitate research access to a large collection of health care, health services and population health data, and an education and training service that supports researchers on use of these data. Its primary role is to act as the central entry point for access to pan-provincial population data to facilitate research in Canada using BC data.

Current data holdings include health care and health service records, population, early childhood development, work place and demographic data and occupational data. Population Data BC continues to expand its data holdings and is working to bring in datasets from education and the environment. Population Data BC staff provides researchers with support and advice in creating data access applications and a streamlined and transparent data application process.

Population Data BC works in collaboration with several partner organizations: the UBC Centre for Health Services and Policy Research; the UBC Human Early Learning Partnership (HELP); the UBC School of Environmental Health; the SFU Faculty of Health Sciences; the Child and Family Research Institute, and the UVIC Spatial Sciences Laboratory.

### **Privacy Governance**

Population Data BC has a designated staff member responsible for privacy and contracts/agreements. Approximately half of this individual's role is spent on internal privacy practices and issues, while the other half is dedicated to the coordination and management of contracts and agreements.

Population Data BC has established a Data Stewards Working Group comprising representatives from each organization contributing data to Population Data BC. This is an active group that meets every three months to agree on common standards, advise and support Population Data BC and to ensure that privacy and security expectations are met.

### **Information Sharing Agreements with Data Providers**

Population Data BC enters into separate Information Sharing Agreements with each data provider (e.g. government ministries and public agencies) for what is typically individual-level personal information on the population of British Columbia relating to human health, well-being and development. Extensive effort was put into the development of the Information Sharing Agreement template, which involved several legal counsels. For each data sharing scenario, the ISA template is modified to take into consideration any additional legislative requirements or conditions that may apply. Substantial time is often required to achieve the final ISA with a data provider.

Each data provider (as Data Steward) must continue to adhere to their applicable legislative requirements, including any consent and/or notification requirements for collection, use and disclosure.

## **Data Holdings**

Once the Information Sharing Agreement with data providers has been completed, Population Data BC receives an extract of identifiable data from each data source. Upon receipt, and if not separated already, Population Data BC separates the Identifiers from Content Data. Both Identifiers and Content Data are encrypted and stored on separate secure servers located in a multi-zone secure environment, and access to the servers and to the data is restricted to a limited number of individuals. The same high level of privacy and security standards is applied regardless of whether the data is individually identifiable or not.

## **Data Access Request Framework**

The Research Data Access Framework was developed and approved by Population Data BC and by all Data Stewards with data currently held in Population Data BC. It is a “living document,” which is periodically reviewed and updated to incorporate new legislative or government policy requirements.

To access data, eligible researchers must submit a Data Access Request form for approval by the public body responsible for the data requested through Population Data BC. Population Data BC supports and guides this process and ensures that all the required documentation and information is included. All requests must be accompanied with proof of an ethics review. Populations Data BC then forwards the completed requests to the relevant Data Steward(s) for review and approval. Additional requirements or conditions may be imposed by the Data Steward(s) on a project specific basis. Population Data BC helps to facilitate the adjudication process, but has no role in decision making.

Once the request is approved, each researcher must sign a Research Agreement with each data provider. In addition, each researcher must successfully complete an on-line privacy tutorial before the requested data extract is provided to them. This 30-minute training module covers privacy principles and legislation; the privacy and security requirements of the Research Agreement; and Population Data BC’s requirements.

Population Data BC staff prepare the extract of the requested data, and ensure that the data is adequately de-identified. With limited exceptions, the research extracts are stored on a Secure Research Environment provided by Population Data BC. Access is provided via encrypted Virtual Private Network (VPN) services, through a firewall, and with a SecurID token for authentication. Access is restricted to those listed on the Research Agreement. Researchers are not permitted to download any individual-level data to any local drive. Researchers must also reside in Canada to get access.

Researchers must only use the data for the research questions approved by the Data Steward in the Research Agreement. The data extract is made available for a limited time (default is two years) with possibility of extension with approval of the public bodies. Any changes to the research questions, researchers or timeframes, must be submitted to Population Data BC for review and approval by the public bodies.

## **Privacy and Security**

As Population Data BC stores an extensive amount of individual-level data in one physical location, it has developed a comprehensive privacy risk management framework that includes:

- A Privacy Impact Assessment
- Privacy Policies and Procedures that follow the 10 Fair Information Principles
- Compliance with ISO27002 requirements for information security
- Compliance with the BC Government Core Policies and Procedures for Information Security
- External systems and security review
- Commitment to ongoing auditing
- Frequently Asked Questions
- Staff confidentiality agreements
- Staff privacy training
- The appointment of the Privacy and Contracts Lead to oversee privacy compliance, maintain up-to-date policies and procedures (reviewed and updated annually), and manage agreements and contracts.

Population Data BC has a highly secure, restricted data facility with a multi-zone environment. Extensive physical, technical and administrative security measures have been installed and implemented including reinforced walls, alarm system, limited physical entry, video surveillance, high security re-enforced doors, as well as network security and IT human resource controls. All data is backed up nightly, with data encrypted before sent to the back-up server.

All Population Data BC staff receive annual, mandatory privacy training, and sign a Staff Confidentiality Agreement upon employment.

Population Data BC has conducted a Privacy Impact Assessment (PIA). An external Systems and Security Review was also conducted. Each data provider also completes their own PIA and Security Threat and Risk Assessment (in some cases this is a legislative requirement), either before or after the ISA is signed.

Population Data BC has sought consultation with the Office of the Information and Privacy Commissioner for BC (OIPC) to keep them apprised of plans and practices and to ensure there are no significant concerns. A senior member of the office of the BC Chief Information Officer also sits on the Data Stewards Working Group.

## For more information

### **The CAPTURE Project**

Simon Fraser University  
8888 University Drive  
WMC Room 2805  
Burnaby, BC V5A 1S6

Telephone: 778.782.6707

Fax: 778.782.3055

Website: [www.thecaptureproject.ca](http://www.thecaptureproject.ca)

Email: [info@thecaptureproject.ca](mailto:info@thecaptureproject.ca)

Privacy: [privacy@thecaptureproject.ca](mailto:privacy@thecaptureproject.ca)