



# **Privacy Policies and Procedures**

**September 2009**

**(Revised February 2010)**

## TABLE OF CONTENTS

I.	Preamble.....	2
II.	Introduction.....	3
	○ Mandate.....	3
	○ Privacy and Security.....	3
	○ Background.....	4
	○ Governance and Management.....	5
	○ Scope.....	6
III.	Legislative Framework.....	7
	○ Provincial Privacy Legislation.....	7
	○ Federal Privacy Legislation.....	8
	○ Defining Personal Information.....	9
IV.	Principles and Policies for the Protection of Personal Information.....	10
	○ Principle 1: Accountability.....	10
	○ Principle 2: Identifying Purposes.....	11
	○ Principle 3: Consent for Collection, Use, or Disclosure.....	13
	○ Principle 4: Limiting Collection.....	13
	○ Principle 5: Limiting Use, Disclosure, and Retention.....	14
	○ Principle 6: Accuracy.....	17
	○ Principle 7: Safeguards.....	18
	○ Principle 8: Openness.....	21
	○ Principle 9: Individual Access.....	22
	○ Principle 10: Challenging Compliance.....	22
V.	Appendix A: Model Code for the Protection of Personal Information.....	24
VI.	Appendix B: Definitions.....	26

**I. PREAMBLE**

In this document, the capitalized terms will have the meanings defined in Appendix B.

Please note that for the sake of comprehensiveness, there will be some duplication of information in this document.

## II. INTRODUCTION

### **Mandate**

Population Data BC is a pan-provincial, multi-institutional platform whose mission is to foster insights into human health, well-being, and development by advancing research through data and education. Population Data BC has a physical presence at Simon Fraser University (SFU), University of Victoria (UVic), and University of British Columbia (UBC). Its UBC site holds individual-level Personal Information on the basis of Information Sharing Agreements with Provincial Ministries and other public body data providers. Population Data BC does not have its own research agenda.

To date, data for research in human health, well-being, and development (at least within BC) have typically been available only within single sectors (e.g. health, education, or early childhood), and linkages have occurred only within a particular disciplinary area. A particular feature of Population Data BC is the linkage of BC population data across various sectors, such as health, education, and early childhood, for research purposes only. Access to such data creates the potential for fundamental advances in understanding the complex interplay of influences on human health, well-being, and development. Such evidence can be used to inform future social policy and investment decisions. Facilitating access to such data for public-interest research purposes, while at the same time ensuring the protection of privacy and confidentiality of individuals about whom the data pertain, is the mandate of Population Data BC.

Population Data BC enters into separate Information Sharing Agreements with government ministries and public agencies (collectively, the “Data Stewards”) for health information and other Personal Information on the population of British Columbia relating to human health, well-being and development. Personal Information which Population Data BC holds from the Data Stewards under these Information Sharing Agreements are referred to as “Data”. Each agency retains ownership of its particular Data set(s) and reviews and approves requests for access to its Data.

### **Privacy and Security**

Respecting personal privacy, safeguarding confidential information, and ensuring security are critical to Population Data BC’s mandate. To this end, Population Data BC has in place a privacy risk management framework that consists of many components, including confidentiality agreements, privacy training, a Privacy Impact Assessment, a public website with frequently asked questions and responses, accountability and advisory input, physical security, network security, and human resources controls, including the presence of a Privacy Officer. Other Population Data BC privacy and security efforts include:

- Keeping Population Data BC's privacy principles, policies, procedures and practices current and in harmony with existing legislation;
- Monitoring developments in privacy legislation, privacy enhancing technologies and public opinion, and adapting to conform as necessary;
- Meeting and exceeding recognized standards of physical, technical, and procedural Data protection and security;
- Fostering transparency and accountability and increasing awareness of Population Data BC's privacy principles, policies and procedures;
- Fostering a culture of privacy at Population Data BC;
- Supporting staff in applying Population Data BC's privacy principles, policies and procedures; and
- Supporting controlled access to, and responsible use of, Personal Information under Population Data BC's management.

Population Data BC' Privacy Officer has a number of designated roles and responsibilities, including:

- Developing and updating Population Data BC's privacy and security policies and procedures;
- Responding to internal and external enquiries or complaints about Population Data BC's privacy and security policies and procedures;
- Staying informed of relevant privacy and security developments; and
- Providing privacy and information security training to new employees, Researchers, and other stakeholders, as necessary, and providing up-to-date annual organisational privacy and information security training.

More information on Population Data BC's mandate, background, operations, and privacy and security measures is available at Population Data BC's public website, [www.popdata.bc.ca](http://www.popdata.bc.ca), and from Population Data BC's Privacy Impact Assessment, which is available upon request.

## **Background**

Public bodies in B.C., such as government agencies, routinely collect information on individuals for administrative purposes, such as making payment for services to service providers or registering student progress through the school system. This type of information is a fundamental tool for population-based, longitudinal studies in research on human health, well-being and development.

In 1990, the Centre for Health Services and Policy Research (CHSPR) at the University of British Columbia and the BC Ministry of Health Services entered into an agreement to create the BC Linked Health Database (BCLHD) – a resource designed to realize the research and planning potential of existing databases. Through significant investments from the Canada Foundation for Innovation, the BC Ministry

of Advanced Education, and the Michael Smith Foundation for Health Research, Population Data BC was established in 2008 as a platform for cross-sectoral, longitudinal, population-wide research, largely built on the BCLHD model and using the BC Linked Health Database's 15+ years of experience in successfully linking administrative health services data.<sup>1</sup>

BCLHD has facilitated over one hundred and fifty research projects on contemporary issues in applied health services and population health. CHSPR and its predecessor organisation have a 30 year history of responsible handling of sensitive Data.

## Governance and Management

Population Data BC operates within a multi-tier governance and management framework, which includes the following:

- The **Data Stewards Working Group** includes Data Stewards from each organisation whose Data Population Data BC administers or is soon to administer. Its objectives are to advise and support Population Data BC and to ensure that the policy and process framework for access to Data meets their privacy and security expectations. This group counsels the Advisory Board.
- The **Committee of Researchers** represents and communicates the diverse needs and viewpoints of the research community. It includes Researchers from across BC from multiple disciplinary areas. Through giving counsel to the Advisory Board, this group guides and directs both the Data resource as well as the training resource, supporting Population Data BC in fulfilling its mandate and objectives.
- The **Advisory Board** convenes on a regular (typically monthly and as needed) basis and plays a critical role in guiding Population Data BC and its operations on core issues, such as strategy, policy, funding, and security. The Advisory Board is comprised of leaders from each of the partner organisations and representation from multiple institutions.
- The **Governance Oversight Committee** is a standing committee of Population Data BC whose purpose is to guide and support the operations of Population Data BC. The Governance Oversight Committee oversees the Advisory Board and is made up of VPs of Research at BC's partner universities, two Data Stewards, two members of Population Data BC's Advisory Board, and two members of Population Data BC's Committee of Researchers.
- The **Operations Committee** plans and reviews the operational functions of Population Data BC, and ensures they are well coordinated amongst the partner universities. It is comprised of members from the University of British Columbia, Simon Fraser University, and the University of Victoria.

---

<sup>1</sup> The BC Linked Health Database (BCLHD) was developed and housed by the Centre for Health Services and Policy Research. It included Data from the Ministry of Health Services, Vital Statistics, the BC Cancer Agency and WorkSafeBC. The BCLHD successfully provided access to these Data to the research community in a privacy-sensitive manner for approved research projects. Population Data BC is largely built on the BCLHD model.

- Population Data BC's **Executive Director** and unit **Leads** are involved in the day-to-day management of Population Data BC. The Executive Director has delegated accountability and responsibility for Population Data BC's functions and is responsible to the Advisory Board and Governance Oversight Committee.

Additionally, Population Data BC is accountable to both Data Stewards and the public through signed Information Sharing Agreements.

### **Scope of these Policies and Procedures**

The principles and policies in this document apply to Population Data BC's Personal Information holdings (the Data) from various Data Stewards.

### III. LEGISLATIVE FRAMEWORK

#### Provincial Privacy Legislation

*British Columbia's Freedom of Information and Protection of Privacy Act (FIPPA)* provides individuals with privacy rights and information access with respect to information that is collected, used, disclosed or retained by public bodies in British Columbia. Individuals have two major rights under FIPPA:

1. The right to protection of the privacy of Personal Information in the custody of, or under the control of, public bodies, and
2. The right of access to records in the custody or under the control of public bodies.

Population Data BC (as a unit of the University of British Columbia, which is a public body) is defined as a public body under Schedule 1 of FIPPA. Government ministries and provincial agencies are also defined as public bodies under FIPPA. The Information Sharing Agreements between Population Data BC and the various Data Stewards are permitted under section 33 of FIPPA. Section 33 grants public bodies the authority to disclose information under various conditions, including to another public body where the information is necessary for the performance of the duties or operations of the receiving public body, and for research or statistical purposes pursuant to section 35.

Section 35(1) of FIPPA permits a public body to disclose Personal Information in its custody, or under its control, for a research or statistical purpose, providing the following conditions are met:

(a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the commissioner,

(a.1) *subject to subsection (2)*, the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in the research,

(b) any record linkage is not harmful to the individuals that information is about and the benefits to be derived from the record linkage are clearly in the public interest,

(c) the head of the public body concerned has approved conditions relating to the following:

(i) security and confidentiality;

(ii) the removal or destruction of individual identifiers at the earliest reasonable time;

(iii) the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorisation of that public body, and

(d) the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public body's policies and procedures relating to the confidentiality of Personal Information.

Subsection (2) states that subsection (1) (a.1) does not apply in respect of research in relation to health issues if the BC Information and Privacy Commissioner approves:

- (a) the research purpose,
- (b) the use of disclosed information for the purpose of contacting a person to participate in the research, and
- (c) the manner in which contact is to be made, including the information to be made available to persons contacted.

More information and a full copy of FIPPA are available at the BC Office of the Information and Privacy Commissioner, [www.oipcbc.org](http://www.oipcbc.org).

British Columbia's *Personal Information Protection Act* applies to the private sector, and does not have applicability to public bodies defined in FIPPA nor to Personal Information covered under FIPPA.

British Columbia's *E-Health (Personal Health Information Access and Protection of Privacy) Act*, introduced on April 10, 2009, provides a legislative framework for governing the collection, use and disclosure of personal health information in electronic health records that will be held in databases called Health Information Banks. Disclosure of this information will require the approval of the new Data Stewardship Committee(s), which will have stewardship over the information in these Health Information Banks. This legislation, regulating the transition of paper health records to electronic health records, is slated for gradual implementation across British Columbia beginning in 2009. Current Information Sharing Agreements with Provincial Ministries and other Data providers provide that to the extent that any Data are designated or prescribed under the *E-Health (Personal Health Information Access and Protection of Privacy) Act, SBC 2008*, a separate Information Sharing Agreement for the use of the affected information will need to be negotiated between the Provincial Ministries or Data providers and Population Data BC to ensure compliance with the new law.

### **Federal Privacy Legislation**

Canada has two federal privacy laws, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The *Privacy Act* imposes obligations on federal government departments and agencies by placing limits on the collection, use, and disclosure of Personal Information.

As of January 1, 2001, PIPEDA covered Personal Information that federally regulated private sector organisations collect, use, or disclose in the course of commercial activities. As of January 1, 2002, PIPEDA was extended to apply to Personal Information collected, used, or disclosed by these organisation, and to apply to information sold across provincial and territorial boundaries. As of January

1, 2004, PIPEDA also covered the collection, use or disclosure of Personal Information in the course of any commercial activity within a province, including provincially regulated organisations. The key element of PIPEDA is its application to commercial activities. While what constitutes “commercial activity” under PIPEDA is not entirely well defined, it is unlikely that Population Data BC’s activities would come within this legislation. Additionally, provinces may be exempted from PIPEDA if they have substantially similar legislation. British Columbia’s *Personal Information Protection Act* (discussed above) has been declared by the federal Governor in Council to be substantially similar to PIPEDA.

### **Defining Personal Information**

Population Data BC has developed and implemented policies and procedures reflecting the B.C. legislative requirements concerning collection, use, and disclosure of Personal Information.

Schedule 1 of FIPPA defines “Personal Information” as “recorded information about an identifiable individual”, including:

- “tombstone” Data (name, age, sex, race, etc.);
- Identifying numbers, symbols or other particulars assigned to an individual;
- The individual’s fingerprints, blood type, or inheritable characteristics;
- Information about the individual’s health care history, including a physical or mental disability.

FIPPA does not prescribe what qualifies as “identifiable information”. However, it is generally recognized that an appropriate standard to apply is that “information is non-identifiable only if the information in issue cannot be used, linked, matched or manipulated ‘by a reasonably foreseeable method’ to identify the Data subject’s identity.”<sup>2,3</sup>

While Population Data BC processes Data so as to reduce their identifiability, some Data may be disclosed to or by Population Data BC which contain identifiable information, in accordance with Information Sharing Agreements and Research Agreements. Given this, Population Data BC treats *all* Data it holds and discloses as “Personal Information” and applies the same privacy protection standards required under FIPPA to all the Data, regardless of whether the Data contain personal identifiers or not.

---

<sup>2</sup> As defined in Ontario’s now-withdrawn Bill 159 and cited by BC’s Information and Privacy Commissioner, in a presentation to the Canadian Institute Conference, June 19, 2001, [http://www.oipc.bc.ca/publications/speeches\\_presentations/speech\\_04.html](http://www.oipc.bc.ca/publications/speeches_presentations/speech_04.html). Last accessed August 6, 2009.

<sup>3</sup> Ontario’s *Personal Health Information Protection Act*, 2004, section 4(2): “identifying information” means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. 2004, c. 3, Sched. A, s. 4 (2).

#### IV. PRINCIPLES AND POLICIES FOR THE PROTECTION OF PERSONAL INFORMATION

The principles outlined in this statement are based on the Canadian Standards Association’s *Model Code for the Protection of Personal Information* CAN/CSA-Q830-96 (the “CSA Code”). This Model Code, as adapted for Population Data BC, offers a principled approach to the detailed requirements found in BC FIPPA. This code is Schedule 1 to the federal *Personal Information Protection and Electronic Documents Act* and is included in this document as Appendix A.

Population Data BC follows these principles for the protection of Personal Information and the specific requirements set out under FIPPA in the handling of all Data it holds. This document will be reviewed every two years to ensure that the principles and policies are relevant and reflect current legislation and best practice. Population Data BC’s privacy policy is presented below.

##### 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.***

Policies and procedures for ensuring the confidentiality and security of Data held at Population Data BC are strictly enforced. The primary aim of these policies is to respect the privacy of users and the requirements of the providers of the Data, and to protect against loss, destruction or unauthorized uses.

Policies	Related Procedures
<p>Policy 1.1 Population Data BC (UBC) resides under the legal umbrella of the University of British Columbia, which has ultimate legal accountability for it. Operations and facilities at Population Data BC’s other sites (i.e. SFU and UVic) will, in kind, come under the legal umbrella of their respective universities.</p>	<p>Procedure 1.1</p> <ol style="list-style-type: none"> <li>1. All legal contracts to which Population Data BC (UBC) is party will be reviewed by legal advisors of the University of British Columbia for compliance with applicable legislation and UBC policies. Legal contracts to which Population Data BC (SFU) and Population Data BC (UVic) are parties will be reviewed by legal advisors of their respective universities.</li> </ol>
<p>Policy 1.2 Population Data BC’s Executive Director has ultimate operational accountability and responsibility for Population Data BC’s operations and its compliance with these principles for the protection of Personal Information. The Executive Director</p>	<p>Procedure 1.2</p> <ol style="list-style-type: none"> <li>1. Population Data BC’s Systems and Security Manager is responsible for and oversees the physical and technical security measures in place to protect Data and reports to the Executive Director.</li> <li>2. The Privacy and Policy Lead (who also acts as the Privacy Officer) is responsible for, and oversees compliance with, privacy requirements and the development and</li> </ol>

<p>is responsible to the Advisory Board and Governance Oversight Committee. Designated Population Data BC unit Leads have responsibility for the day-to-day management of various functions of Population Data BC and report to the Executive Director.</p>	<p>management of privacy and security policies and procedures.</p> <ol style="list-style-type: none"> <li>3. Only a limited number of personnel are authorized to work with Data.</li> <li>4. All staff will be oriented in the principles of privacy and Data protection at Population Data BC and must sign a confidentiality agreement prior to gaining access to Data.</li> </ol>
<p><b>Policy 1.3</b> Population Data BC’s Privacy and Policy Lead (i.e., Privacy Officer) is responsible for management of privacy matters and privacy compliance within the organization.</p>	<p><b>Procedure 1.3</b></p> <ol style="list-style-type: none"> <li>1. The Privacy Officer will:             <ol style="list-style-type: none"> <li>a. Develop, review, and/or revise Population Data BC’s policies and procedures as necessary to ensure compliance with FIPPA and contractual privacy and security obligations of Population Data BC;</li> <li>b. provide privacy and information security training;</li> <li>c. ensure confidentiality agreements are in place for all staff and Researchers; and</li> <li>d. respond to privacy-related developments and issues as they arise, including privacy complaints and requests for information access, and report issues and policy decisions to the Executive Director.</li> </ol> </li> </ol>

**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.***

Population Data BC is a custodian of Personal Information previously collected by provincial ministries and other public body Data providers (the “Data Stewards”). Population Data BC is permitted to link those Data for research purposes and to provide linkable Data for approved research projects. Population Data BC does not engage in primary collection of Data.

The following policies therefore relate to the identification of purposes for the use, disclosure and retention of secondary Data.

Policies	Related Procedures
<p><b>Policy 2.1</b> Data Stewards are responsible for ensuring that the legal authority exists for the collection of Personal Information. Under</p>	<p><b>Procedure 2.1</b></p> <ol style="list-style-type: none"> <li>1. Information Sharing Agreements are signed with the Data Steward(s) outlining the terms and conditions binding upon Population Data BC in the</li> </ol>

<p>section 33 of FIPPA, designated public bodies are permitted to disclose Personal Information to another public body (e.g., Population Data BC) where the information is necessary for the operations or functions of the receiving public body and for research or statistical purposes.</p>	<p>holding, using, disclosing or retaining of Data received from the Data Steward(s) for authorized and legitimate research or statistical purposes.</p> <ol style="list-style-type: none"> <li>2. Population Data BC encourages Data Stewards to inform individuals that their Personal Information will be used for research and statistical purposes, under controlled conditions, as authorised by law.</li> </ol>
<p>Policy 2.2 Population Data BC houses and protects Data to support research in human health, well-being, and development that is in the public interest.</p>	<p>Procedure 2.2</p> <ol style="list-style-type: none"> <li>1. Population Data BC has the authority pursuant to FIPPA and related Information Sharing Agreements to engage in Data linkage for research and statistical purposes, and to disclose Data in the form of Research Extracts to Researchers in accordance with signed Research Agreements between Researchers and Data Steward(s).</li> </ol>
<p>Policy 2.3 Population Data BC only disclose Data in the form of Research Extracts to Researchers where the Data has been approved for disclosure by the appropriate Data Steward(s) and in accordance with a Research Agreement between the Researcher and Data Steward. Population Data BC, in effect, serves as an intermediary, facilitating the Data access process between Researchers and Data Stewards.</p>	<p>Procedure 2.3</p> <ol style="list-style-type: none"> <li>1. Population Data BC's Researcher Liaison staff assist Researchers with preparation of the Data Access Request (DAR) and to define their cohort, if requested. The DAR requires the Researchers to specify exactly which Data files, years of Data, and Data fields in each Data file they require, and therefore discourages the inclusion of unnecessary information in Research Extracts prepared for research.</li> <li>2. A DAR must be approved by the appropriate Data Steward(s), and a Research Agreement based on that DAR must be signed between the Researcher and Data Steward before Population Data BC will begin preparation of a Research Extract. Disclosure of the Research Extract to the Researcher will only occur in accordance with the terms and conditions of the Research Agreement signed between the Researcher and Data Steward(s).</li> </ol>
<p>Policy 2.4 Population Data BC retains the minimal amount of Personal Information in all Data files for its defined purpose.</p>	<p>Procedure 2.4</p> <ol style="list-style-type: none"> <li>1. Identifiers are stored separately from Content Data.</li> <li>2. Identifiers are used only for linkage. After linkage is complete, the Identifiers are archived in a physically secure location.</li> <li>3. Identifiers such as names or Personal Health Numbers (PHNs) are replaced with study-specific</li> </ol>

	<p>ID numbers for all research Data extracted for purposes of an approved research project. Only the study-specific ID numbers are disclosed to Researchers along with the approved Content Data.</p>
--	---

**Principle 3: Consent**

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

The obligation for obtaining consent(s) rests with those public bodies (i.e. Data Stewards) and Researchers who originally collect the Data. Population Data BC does not perform any primary collection of Personal Information and is only engaged in secondary use or secondary disclosure of Personal Information initially collected by other public bodies or individuals.

Pursuant to section 33 of FIPPA, the designated public bodies are permitted to disclose Personal Information to Population Data BC. Pursuant to Section 35 of FIPPA, Population Data BC and Researchers with approved access to Data collected by the designated public bodies are not required to seek individual consent for the use of those Data for research and statistical purposes.

Population Data BC relies on public bodies to collect Personal Information in a lawful manner and in accordance with the requirements of FIPPA. Where consent is required, Population Data BC relies on the public bodies overseeing the initial collection of Personal Information to have obtained the appropriate consent(s) required for collecting and using the Personal Information. Research ethics board review will confirm whether the consent(s) is/are appropriate for the requested uses of the Data.

**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.***

Population Data BC does not engage in any primary Data collection activities. Population Data BC holds Data collected by other public bodies and relies on those public bodies to collect the information by fair and lawful means.

In Population Data BC’s role as a Data custodian, Population Data BC requests only Data fields that are necessary for the fulfillment of its role in developing a resource for research purposes. In Population Data BC’s role as administrator of Data for research purposes, Population Data BC will assist Researchers

in requesting particular Data files via the Data Access Request, conduct data preparation, and provide only those Data in a Research Extract that have been expressly approved by the Data Steward(s).

**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.***

The following policies and procedures will be divided according to use, disclosure and retention.

Policies For Use	Related Procedures
<p>Policy 5.1 Population Data BC only uses and discloses the Data it holds for purposes authorised by the Data Stewards pursuant to signed Information Sharing Agreements, for:</p> <ol style="list-style-type: none"> <li>1. providing Researchers with Research Extracts for approved Data Access Requests; and</li> <li>2. Data linkage and related Data development projects.</li> </ol> <p>All uses are for research and statistical purposes only and are compliant with FIPPA and other applicable legislation.</p>	<p>Procedure 5.1 Data provided to Researchers must be in accordance with a signed Research Agreement between the Researcher and the Data Steward(s).</p>
<p>Policy 5.2 All Researchers who wish to access Data held by Population Data BC must submit a Data Access Request (DAR) specifically requesting those Data. Only Data deemed necessary by the Data Steward to meet the requirements of the proposed research will be approved for release to the Researcher.</p>	<p>Procedure 5.2</p> <ol style="list-style-type: none"> <li>1. The Researcher Liaison staff of Population Data BC work with Researchers and Data Stewards to facilitate the Data Access Request process by supporting Researcher(s) in the preparation of applications, ensuring all defined requirements are met, assessing completeness and clarity of the applications, and guiding Researchers throughout the process.</li> <li>2. If Researchers require additional or supplemental Data after receiving their initial Data, they will be required to submit an amendment to their DAR.</li> </ol>
<p>Policy 5.3 Population Data BC will consult with relevant privacy commissioners and/or other government officials/bodies responsible for</p>	<p>Procedure 5.3 Population Data BC actively fosters open working relationships with external agencies that provide Data, the Office of the Information and Privacy</p>

<p>privacy protection prior to undertaking any Data preparation that is deemed to be exceptional or precedent-setting in scope, scale, methods of linkage, procedures for obtaining consent, or other factors.</p>	<p>Commissioner of BC (OIPC), and the Office of the Chief Information Officer (OIC).</p>
<p><b>Policy 5.4</b> Only a limited number of authorised personnel with restricted access are permitted to work with the Data.</p>	<p><b>Procedure 5.4</b></p> <ol style="list-style-type: none"> <li>1. Information Sharing Agreements signed with Data Steward(s) specify only individuals in certain job roles that may access Data. Only personnel in such roles may be granted restricted access to the Data.</li> <li>2. Access to Identifiers and Content Data is restricted (both physically and electronically) to designated personnel.</li> <li>3. Access to the high security Red Zone, where work on Data is performed, is restricted to personnel on an “as needed basis” only.</li> </ol>
<p><b>Policies for Disclosure</b></p>	
<p><b>Policy 5.5</b> Population Data BC will only disclose Data to Researchers where such disclosure has been authorized by the relevant Data Steward(s) in accordance with a Research Agreement signed between the Data Steward(s) and Researcher.</p>	<p><b>Procedure 5.5</b></p> <ol style="list-style-type: none"> <li>1. Population Data BC will review the Research Agreement and all related paperwork to ensure that only approved Data are disclosed and that all relevant conditions of disclosure have been met.</li> </ol>
<p><b>Policy 5.6</b> Population Data BC programmers will only extract Data once a signed Research Agreement has been received. Population Data BC will only disclose the Data requested and approved by the Data Steward(s).</p>	<p><b>Procedure 5.6</b></p> <ol style="list-style-type: none"> <li>1. Once Population Data BC’s Researcher Liaison staff receive a signed Research Agreement and the Researcher has signed the Population Data BC Services Agreement, the Researcher Liaison staff will notify the Data Services Unit to begin Data preparation.</li> <li>2. Population Data BC programmers in the Data Services Unit will only prepare the Data approved in the Research Agreement and in accordance with the Research Agreement.</li> </ol>
<p><b>Policy 5.7</b> Population Data BC will inform Researchers of the correct use, storage, and destruction of Data, and of the requirements of publishing research using the Data. These terms and conditions will also be stipulated</p>	<p><b>Procedure 5.7</b></p> <ol style="list-style-type: none"> <li>1. Population Data BC’s Researcher Liaison staff will discuss Data handling requirements with Researchers upon granting access to, or delivery of, the Data prepared for an approved research project and are also available for</li> </ol>

<p>in Research Agreements.</p>	<p>ongoing dialogue.</p> <ol style="list-style-type: none"> <li>2. Data, including Personal Information, are not to leave Population Data BC's Secure Research Environment (SRE) unless they are aggregated.</li> <li>3. All material intended for publication involving the Data must first be reviewed and approved for publication by the appropriate Data Steward(s) prior to publication of the Researcher's findings to ensure the anonymity of the Data. Material must be submitted to the Data Steward(s) at least 45 days prior to the intended publication date. Cell sizes may not be less than five as per standard guidelines for aggregation of data.</li> </ol>
<p>Policies for Retention</p>	
<p>Policy 5.8 Research Extracts are stored centrally in Population Data BC's Secure Research Environment (SRE), unless other provisions are expressly allowed by the Data Steward(s) and provided for in the Research Agreement.</p>	<p>Procedure 5.8</p> <ol style="list-style-type: none"> <li>1. Only Researchers named on the Research Agreement are granted access to the Research Extract on the SRE.</li> <li>2. On a case-by-case basis and only as approved by the Data Steward(s), Researchers may be provided with the Research Extract in encrypted form on discs. In this scenario, Data protection measures similar to those provided by the SRE may be required by the Data Steward(s) of the Researcher(s).</li> </ol>
<p>Policy 5.9 Where Researchers are provided a Research Extract on encrypted media as expressly provided for in a Research Agreement and authorized by the applicable Data Steward(s), they are required to return or destroy the Data at the completion of the research project in accordance with the Research Agreement.</p>	<p>Procedure 5.9</p> <ol style="list-style-type: none"> <li>1. Requirements for returning and/or destroying Data are discussed with Researchers upon delivery of Data and stipulated in the Research Agreement to which Researchers are party.</li> <li>2. Researcher Liaison staff will remind Researchers of impending expiry dates in Researcher Agreements and requirements of proper destruction or return of Data.</li> <li>3. Where Researcher Liaison staff become aware of a failure to return Data or other unauthorized retention or improper or inadequate destruction of Data by a Researcher, they will inform the applicable Data Steward(s) promptly.</li> </ol>
<p>Policy 5.10 Population Data BC retains Data provided by</p>	<p>Procedure 5.10 Information Sharing Agreements between</p>

<p>Data Stewards for research purposes for as long as specified in Information Sharing Agreement(s) with Data Stewards. Population Data BC will conduct periodic reviews to examine whether the Data disclosed to Population Data BC continues to be needed. Where Population Data BC determines that certain Data are no longer needed, that Data will be securely destroyed as per the Information Sharing Agreement(s).</p>	<p>Population Data BC and Data Stewards not only detail the uses and conditions under which Data are provided to Population Data BC, they also detail the conditions and requirements for Population Data BC's storage, retention, and destruction of Data.</p>
--	---

**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.***

Population Data BC relies on the Data Stewards engaged in primary Data collection to ensure that Personal Information is accurate, complete and up-to-date at the time of collection.

Policies	Related Procedures
<p>Policy 6.1 As Population Data BC Data holdings include only Data initially collected by other public bodies, those doing the primary Data collection are responsible for the accuracy of the Data collected. Population Data BC will update its Data holdings upon receipt of updated Data from the Data Steward. <i>Note: Data collected for research or statistical purposes are not subject to the same standards of accuracy, completeness, and current relevance as those applying to Data for clinical uses.</i></p>	<p>Procedure 6.1</p> <ol style="list-style-type: none"> <li>1. Data received by Population Data BC from Data Stewards are reviewed for completeness and consistency.</li> <li>2. Population Data BC endeavors to incorporate new Data files as soon as possible to provide the most recent available Data for research purposes.</li> </ol>
<p>Policy 6.2 Upon receipt of Data from Data Stewards, Population Data BC staff performs consistency and quality checks to ensure that the Data received are complete, and that the Data appear to be accurate.</p>	<p>Procedure 6.2</p> <ol style="list-style-type: none"> <li>1. Data received by Population Data BC from Data Stewards are reviewed for completeness and consistency.</li> <li>2. Population Data BC endeavors to incorporate new Data files as soon as possible to provide the most recent</li> </ol>

	available Data for research purposes.
<p>Policy 6.3 Prior to disclosure of Data in the form of a Research Extract to Researchers, Population Data BC reviews the Data for completeness and consistency and ensures that only approved Data are released.</p>	<p>Procedure 6.3</p> <ol style="list-style-type: none"> <li>1. Population Data BC’s Researcher Liaison staff perform a check of the Research Extract before delivery to Researchers. This check entails comparing the Research Extract against the Research Agreement to ensure only approved Data are released and that the requirements of the Research Agreement are met.</li> <li>2. Population Data BC’s Researcher Liaison staff maintain on-going dialogue with Researchers to answer queries and remain informed about potential Data quality problems.</li> </ol>

**Principle 7: Safeguards**

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

Population Data BC has established a high level of physical, technical, and organizational security for all Data in its custody, meeting or exceeding well-recognized ISO 27002 requirements for information security. In September 2009, an external third party consultant was engaged to conduct a systems and security review of Population Data BC information security practices and confirmed its security strengths and safeguards against ISO requirements.

While Population Data BC differentiates between Data that include personally identifying information (or potentially personally identifying information) (i.e. Identifiers) and Data that do not (i.e. Content Data), all Data are considered to be highly sensitive and are protected with appropriate safeguards.

Policies	Related Procedures
<p>Policy 7.1 Population Data BC will utilize stringent <b>physical</b> safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use, or modification of Data.</p>	<p>Procedure 7.1</p> <ol style="list-style-type: none"> <li>1. Population Data BC maintains a secure physical area with several layers of physical protection, including locked and alarmed premises, monitored electronic access to high security zones, video surveillance at entrances to high security zones, and a separately locked and alarmed server room</li> </ol>

	<p>within a high security zone.</p>
<p>Policy 7.2 Population Data BC will utilize stringent <b>technological</b> safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use, or modification of Data.</p>	<p>Procedure 7.2</p> <ol style="list-style-type: none"> <li>1. Population Data BC protects all Data in a manner that is consistent with evolving best practices for managing sensitive Data.</li> <li>2. Population Data BC’s Red Zone network is logically moated. There is no direct connection from the Red Zone network to any other networks. No Data are able to enter or leave the Red Zone without a two-step authentication process and an audit trail.</li> <li>3. Access to Population Data BC facilities, systems and networks will be logged electronically. Logs are monitored on a regular basis for intrusion detection and attempts at unauthorized use.</li> <li>4. Access to Data will require two-factor authentication, granted only to specially authorised personnel on a “need to know” basis.</li> <li>5. Data are stored on an isolated computer network at Population Data BC, protected by firewalls. Content Data and Identifiers are stored separately from each other in encrypted, logical areas, and accessed only by authorised programmers. Separate logins are required for each, thus creating an audit trail.</li> <li>6. All information and Data are backed-up on secure servers and encrypted media, protected by locks and alarms within a high security zone. Encrypted backup media are also stored in a secure off-site location, as per internal policies and procedures.</li> </ol>
<p>Policy 7.3 Population Data BC will utilize stringent <b>organizational</b> safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use or modification of Data.</p>	<p>Procedure 7.3</p> <ol style="list-style-type: none"> <li>1. All Population Data BC personnel must undergo privacy and information security training, annually and upon being newly hired.</li> <li>2. Researchers must undergo privacy training prior to gaining access to a Research Extract.</li> <li>3. All Population Data BC personnel and</li> </ol>

	<p>Researchers must sign confidentiality agreements.</p> <ol style="list-style-type: none"> <li>4. Population Data BC personnel will have access to Data and to secured zones only on an “as needed” basis. Only the Systems and Security Manager, and a small number of specially trained programmers involved in Data linkage, are authorised to handle the Data. Separate logins are required for access to Identifiers and Content Data.</li> <li>5. Access to all Population Data BC systems leaves an audit trail, which is monitored on a regular basis.</li> <li>6. Researchers wishing to access Data must sign a Research Agreement binding them to conditions governing use of the Data, security arrangements, assurances regarding disclosure, and requirements to return/destroy any copies of the Data.</li> <li>7. To deter loss, theft, copying, and unauthorised access, Researchers will typically be required to access Research Extracts on Population Data BC’s Secured Research Environment (SRE). On a case-by-case basis and only as approved by the Data Steward(s), Researchers may be provided with the Research Extract in encrypted form on discs. In this scenario, Data protection measures similar to those provided by the SRE may be required by the Data Steward(s) of the Researcher(s).</li> <li>8. If Population Data BC suspects a breach of the Research Agreement, Population Data BC will investigate and notify the relevant Data Steward(s).</li> </ol>
<p><b>Policy 7.4</b> Population Data BC enforces stringent safeguards for the transfer of Data, from both Data Stewards into Population Data BC’s secured facilities, and from Population Data BC to Researchers for approved research projects.</p>	<p><b>Procedure 7.4</b></p> <ol style="list-style-type: none"> <li>1. All Data transfers to Population Data BC will be via encrypted secure file transfers.</li> <li>2. Researcher access to Research Extracts will be via the SRE, with limited exceptions. On a case-by-case basis and only as approved by the Data Steward(s), Researchers may be provided with the Research Extract in encrypted form on discs. In this scenario, Data protection measures similar to those</li> </ol>

	provided by the SRE may be required by the Data Steward(s) of the Researcher(s).
--	--

**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.***

Population Data BC makes information about its policies and procedures relating to the management and protection of Personal Information readily available either on its website or upon request.

Policies	Related Procedures
<p>Policy 8.1 Population Data BC makes information about its policies and procedures relating to the management and protection of Personal Information readily available on its website or upon request. Enquiries are welcome.</p>	<p>Procedure 8.1</p> <ol style="list-style-type: none"> <li>1. Population Data BC provides information relating to Data security and privacy on its website. Details about Population Data BC Data holdings, including what they are and the purposes for which they may be used and/or accessed, are reported on Population Data BC’s public website. A webpage of frequently asked questions (FAQs) and responses are also available on this website. Links to resources such as the Office of the Information and Privacy Commissioner are also highlighted.</li> <li>2. Population Data BC’s Privacy Impact Assessment will also be made publically available upon request.</li> <li>3. Individuals who contact Population Data BC to make an enquiry will be directed to Population Data BC’s Privacy Officer, who will:               <ol style="list-style-type: none"> <li>a. Provide information on Population Data BC’s policies and procedures; and/or</li> <li>b. Direct the individual to other resources if necessary.</li> </ol> </li> <li>4. All enquiries will be logged and assessed by Population Data BC’s Privacy Officer to guide development of further privacy documentation as required.</li> <li>5. Documentation relating to Data security</li> </ol>

	and privacy will be reviewed and updated regularly or as required.
--	--

**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.***

Data provided by Data Stewards and held by Population Data BC may only be used with approval by the Data Stewards for research purposes only. Population Data BC cannot grant individuals access to this Data and will refer them to the Data Steward(s) responsible for the collection of the Data to process their request.

Policies	Related Procedures
<p>Policy 9.1 Pursuant to Information Sharing Agreements with Data Stewards, all requests from individuals for access to any Data must be referred to the Data Steward as the original collector of the Data held by Population Data BC. Because Population Data BC only holds and administers this Data for research purposes, it cannot grant individuals access to Personal Information within Data files provided by Data Stewards. Only the relevant Data Stewards have this authority.</p>	<p>Procedure 9.1 1. If contacted by individuals requesting access to their Personal Information, or expressing concern about its accuracy, Population Data BC will inform individuals that they must directly contact the primary collection agency. If the Data Steward has advised Population Data BC of the name or title and contact information of the official to whom such requests are to be made, Population Data BC will also provide that official's name or title and contact information to the individual making the access request.</p>

**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 responsible for the organization's compliance.***

An individual will be able to address a challenge concerning compliance with the above principles to the designated individuals accountable for Population Data BC's compliance.

Policies	Related Procedures
Policy 10.1	Procedure 10.1

<p>Concerns regarding Population Data BC’s compliance with its privacy policy may be sent directly to the Privacy Officer of Population Data BC. All communication of this nature will be reviewed by the Executive Director, the Privacy Officer, and the Systems and Security Manager. If deemed necessary, they will be brought to the attention of the Principal of UBC’s College for Interdisciplinary Studies (CFIS) and the Office of the University Counsel. Where challenges are found to be justified, they will be addressed directly. This may include changing practices if needed.</p>	<ol style="list-style-type: none"> <li>1. All complaints will be logged and reviewed by the Privacy Officer to determine whether the complaint constitutes a breach or omission in Population Data BC’s policies and procedures, and to consider improvements in its processes.</li> <li>2. Should the Privacy Officer’s response not be satisfactory, complaints can be escalated to the Principal of UBC’s College for Interdisciplinary Studies or to the Office of the University Counsel.</li> <li>3. Population Data BC will work with the Office of the Information and Privacy Commissioner to improve Population Data BC’s policies and procedures where areas for improvement are identified.</li> </ol>
<p><b>Policy 10.2</b> Internal complaints about suspected breaches of Population Data BC’s privacy policies and procedures will be reviewed by Population Data BC’s Privacy Officer and the Executive Director.</p>	<p><b>Procedure 10.2</b></p> <ol style="list-style-type: none"> <li>1. Population Data BC personnel concerned about possible breaches of Population Data BC’s privacy policies and procedures can either directly inform Population Data BC’s Privacy Officer or their direct supervisor, who will be responsible for bringing the matter to the attention of the Privacy Officer.</li> <li>2. The Privacy Officer will review the complaint and, where appropriate, strategies for improvement will be developed in consultation with the Executive Director and unit Leads.</li> </ol>

## **APPENDIX A: MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION**

The principles outlined in this statement are based on the Canadian Standards Association's Model Code for the Protection of Personal Information CAN/CSA-Q830-96 (the "CSA Code"), which was recognised as a national standard in 1996. The code addresses the ways in which organisations collect, use, and disclose Personal Information. It also addresses the rights of individuals to have access to their Personal Information and to have it corrected if necessary.

The CSA Code's ten principles are:

### **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.

## APPENDIX B: DEFINITIONS

**“Advisory Board”** refers to the board overseeing Population Data BC from a strategic and operational perspective, reporting to the Governance Oversight Committee.

**“Breach” or “Breach of Security”** refers to any unauthorized access, collection, use, modification, disclosure, destruction, disposal, storage, or loss of information or property held by, in the custody of, or belonging to Population Data BC, and includes unauthorized access to Population Data BC premises.

**“CHSPR”**: Centre for Health Services and Policy Research.

**“Confidential Information”** refers to all information held by, in the custody of, or belonging to Population Data BC that is not in the public domain.

**“Content Data”** refers to the data held by Population Data BC that contain person specific information which may be disclosed in the context of a research project. These may include data that are also considered an Identifier. Examples include educational attainment scores, hospital discharge codes, or compensation claim codes.

**“Content Data Group”** refers to a logical unit of, and thus technical separation of, Content Data. The boundaries may vary. At UBC, because of the secure environment within Population Data BC, all Content Data is expected to be handled together as a single Content Data Group. Management of a given CDG may be done by subset of Population Data BC itself (i.e. UBC’s Data Services Unit or Population Data BC - SFU,) or by an external public entity.

**“Content Data Group ID”** refers to a generated number that is unique to an individual in a specific Content Data Group.

**“Data”** refers to any information used for research or statistical purposes, including Personal Information, which is disclosed to Population Data BC by Data Stewards under an Information Sharing Agreement.

**“Data Access Request”** refers to the formal application document for data through Population Data BC. Components of this application form include information on the researchers, the research questions, the proposed methodology, and details of the proposed cohort and data requested.

**“Population Data BC Cost Recovery Estimate”** refers to the cost recovery estimate provided by Population Data BC and signed by the Researcher, covering costs relating to data application coordination, data preparation and checking, and provision of approved data.

**“Data Steward”** refers to a public body that has ultimate responsibility for a given data source. In practice, an individual is typically named as having the authority to approve or reject research requests involving that data, typically called “the / a Data Steward.”

**“FIPPA”** refers to British Columbia’s *Freedom of Information and Protection of Privacy Act* [RSBC 1996].

**“Geomatics”** refers to the discipline of gathering, storing, processing, and delivery of geographic information, or spatially referenced information.

**“High Security Zones”** refer to the Red and Purple Zones.

**“ID Matrix”** refers to the mapping that Population Data BC maintains between IDs from all Content Data Groups to each other. The ID Matrix does not contain any Personal Information.

**“Identifier Management Unit”** is a unit within Population Data BC that is responsible for collecting, holding, and linking Identifiers. This unit is part of the Data Services Unit.

**“Identifier” or “Identifier Data”** refers to information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. (Ontario PHIPA 2004, C.3, Sched. A.s.4 (2)). In the case of Population Data BC, Identifiers describe individuals and are used to facilitate linkage, and include fields such as name, date of birth, 6-digit post code, and Personal Education Number.

**“Information Sharing Agreement”** refers to a legal agreement that allows for the periodic transfer of data between a Data Steward and Population Data BC and holding of the data by Population Data BC.

A **“Lead”** is a manager of Population Data BC. The Leads of Population Data BC include the following:

- Lead, Systems and Security (or commonly referred to as Systems and Security Manager)
- Lead, Data Services Unit
- Lead, Business Process Management
- Lead, Privacy, Policy, and Contract Development (also referred to as the Privacy Officer)
- Lead, Communications
- Lead, Education and Training Unit

**“Linkage” or “Probabilistic Linkage”** involves connecting records referring to the same individual across different sources. Identifiers such as names, birth dates and postal codes are used to create the best matches between known information and new information.

**“Linkage ID”** refers to a generated number that is unique to an individual referenced during linkage resolution.

**“Management”** refers to Population Data BC’s Executive Director and unit Leads

**“Medium Security Zone”** refers to the Yellow Zone.

**“Partners” or “Collaborators”** refers to the following organizations:

- UBC Centre for Health Services and Policy Research (CHSPR)
- UBC Human Early Learning Partnership (HELP)
- UBC School of Environmental Health (SOEH)
- SFU Faculty of Health Sciences (FHS)
- UVic Spatial Sciences Lab (SSL)
- Child and Family Research Institute
- Children and Women’s Hospital

**“Password” or “Passphrase”** refers to a sequence of characters that allows entry into a restricted system.

**“Personal Information”** means recorded information about an identifiable individual other than contact information (Schedule 1 of BC *Freedom of Information and Protection of Privacy Act* 1996.)

**“Personnel” or “personnel”** refers to all persons who work for Population Data BC, including employees, contractors, consultants, temporaries and other workers at Population Data BC, regardless of the amount of time they have been or will be working with Population Data BC. For greater clarification, this shall include Management and staff.

**“Population Data BC Services Agreement”** refers to a formal agreement signed between Population Data BC and the Researcher prior to receipt of data, outlining terms and conditions of Research Extract provision and use of the Secure Research Environment.

**“Population Directory”** refers to a table that Population Data BC maintains that includes all the individuals about whom Population Data BC has information. This includes Personal Information such as name, address, date of birth, and other relevant Identifiers. This table is updated with receipt of each new data extract and is the basis for record linkages. It is expected that the Population Directory will cover the entire BC population.

**“Project Member”** refers to the Researcher(s) and other individuals specifically identified in an approved Data Access Request as requiring access to the Research Extract; an individual who has completed and signed a confidentiality pledge under the Research Agreement.

**“Purple Zone”** is the highly secure, restricted physical environment where all Population Data BC servers are located. This resides within the Red Zone; however, access controls for this area are even more limited.

**“Record ID”** refers to a generated number unique to each record received from a Data Steward.

**“Red Zone”** in physical terms is a highly secure space accessible only to named persons who work on the individual-level data on “Red Zone” terminals. In network terms, it is the moated environment that is present within the physical Red Zone, unconnected to the outside world.

**“Research Agreement”** refers to an agreement between a Researcher and Data Steward(s) for the use of specific fields of data for specific research projects and outlining obligations associated with that access.

**“Research Extract” or “Research Data Extract”** refers to data that are extracted in conjunction with an approved Data Access Request and Research Agreement for the purpose of disclosure to a Researcher.

**“Researcher”** refers to a person who is a student, teacher or researcher either enrolled at or employed by any of the following institutions: a) universities as defined in the *Universities Act*, R.S.B.C. 1996, c. 468, b) colleges, university colleges, and Provincial institutes as defined under the *Colleges and Institutions Act*, R.S.B.C. 1996, c. 52, c) the open university continued under the *Open Learning Agency Act*, R.S.B.C. 1996, c. 409, d) Royal Roads University continued under the *Royal Roads University Act*, R.S.B.C. 1996, c. 409, e) any other institutions offering public post-secondary education services that

may be described in the statutes above, and f) other comparable institutions in other jurisdictions worldwide.

**“Secure Research Environment”** refers to a study-specific space on a central server at Population Data BC, where Research Extracts are stored and analyses can be done remotely using Virtual Private Networking.

**“Study ID”** refers to a person specific number, unique to each Research Extract and appended to each record within a Research Extract.

**“Trusted Third Party for Linkage” or “TTPL”** refers to an independent, neutral body that does not have stewardship over the data being linked, as referenced in the September 2005 Canadian Institute for Health Research’s Privacy Best Practices (<http://www.cihr-irsc.gc.ca/e/29072.html>). Population Data BC is such a TTPL.

**“University”** shall mean the university at which the functions or activities are undertaken and enforced.

**“Video Surveillance”** refers to the use of cameras and associated technologies to create recorded images of physical activity.

**“Yellow Zone”** in both physical and network terms refers to the semi-secure environment where Population Data BC staff and external Researchers work. Programmers may have a Yellow Zone networked computer within the Red Zone that allows them to connect to the internet or email.

