RD0500 – INFORMATION REQUESTS FOR RESEARCH

Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dãkelh Dené, Ktunaxa, Nlaka'pamux, Secwépemc, St'át'imc, Syilx, and Tŝilhqot'in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

1.0 PURPOSE

To protect Interior Health (IH) information used for the purpose of Research including: access, use, disclosure, Privacy and Confidentiality, security, retention and destruction.

2.0 DEFINITIONS

TERM	DEFINITION
Confidentiality	The duty to ensure that personal information is kept private and is accessible only to authorized persons.
Control	The legal authority to manage a record throughout its life cycle, including restricting, regulating and administering its use or disclosure.
Custody	Physical possession of a record; may not have Control of the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security.
Data Set	A collection of information used for the purpose of Research, including human biological materials.
Data Steward	The employee identified as the person responsible for managing information according to IH policies, including developing relevant operational procedures for accessing and using the information. These individuals are typically program leaders who have planning and policy level responsibilities for information within their areas and management responsibilities, including but not limited to: information access, use, disclosure (including requests for records received under the Freedom of Information and Protection of Privacy Act (FIPPA), information quality assurance and improvement).

RD0500 – INFORMATION REQUESTS FOR RESEARCH

TERM	DEFINITION
General Health Information Sharing Agreement (GHISA)	An agreement that establishes a common legal, policy and governance framework for the sharing of health information and ancillary personal information within the public healthcare system in British Columbia (GHISA). The parties to the agreement are the Ministry of Health and the six health authorities.
Identifiable Information	Information that may reasonably be expected to identify an individual, alone or in combination with other available information, also known as personal information. It includes but is not limited to: • Name, address or telephone number • Race, national or ethnic origin, colour, or religious beliefs or associations • Age, sex, sexual orientation, marital status or family status • Personal health number, identification number, symbol or other particular assigned to them • Fingerprints, blood type, or inheritable characteristics • Health care history, including a physical or mental disability • Information about their educational, financial, criminal, or employment history • Personal views or opinions, except if they are about someone else • Anyone else's opinions about themselves
Information Sharing Agreement (ISA)	A written agreement between two or more parties outlining the terms and conditions for the parties to collect, use or disclose personal information in cases where consent for use has not been obtained.
Information Sharing Plan (ISP)	An Information Sharing Plan sets out details with respect to an information sharing situation under the GHISA, including the data involved (health information and health-related information, personal information and non-personally Identifiable Information), the parties, how data will be managed and secured, and the authorities for collection, use and disclosure.
Information Types	Categories of information include: • Anonymized information – the information is irrevocably stripped of direct identifiers, a code is not kept to allow future re-linkage, and risk of re-identification of individuals from remaining indirect identifiers is low or very low. • Anonymous information – the information never had identifiers associated with it (e.g., anonymous surveys) and risk of identification of individuals is low or very low.

RD0500 – INFORMATION REQUESTS FOR RESEARCH

TERM	DEFINITION
	• Coded information – direct identifiers are removed from the information and replaced with a code. Depending on access to the code, it may be possible to re-identify specific participants (e.g., the Principal Investigator retains a list that links the participants' code names with their actual name so data can be re-linked if necessary). • Directly identifying information – the information identifies a specific individual through direct identifiers (e.g., name, social insurance number, personal health number). • Indirectly identifying information – the information can reasonably be expected to identify an individual through a combination of indirect identifiers (e.g., date of birth, place of residence or unique personal characteristic).
Privacy	The right of an individual to determine what information about themselves may be collected, used, and shared with others.
Research	An undertaking intended to extend knowledge through a disciplined inquiry and/or systematic investigation.
Researcher	A person conducting a disciplined inquiry and responsible for the conduct of the Research.

3.0 POLICY

3.1 The use of Identifiable Information for Research must comply with all applicable federal and provincial privacy legislation including, but not limited to:

- Freedom of Information and Protection of Privacy Act, RSBC 1996, Chapter 165, Part 3, Division 2, Section 33 (33.3h) (FIPPA); and
- E-Health (Personal Health Information Access and Protection of Privacy) Act. SBC 2008, Chapter 38 (E-Health Act).

3.2 IH has a legal and ethical responsibility to manage the information within its Custody and Control in a manner that promotes confidence amongst its various stakeholders and in accordance with applicable legislation.

3.3 In the course of performing a Research project, a Researcher may collect Identifiable Information including personal health information from Research participants as defined in FIPPA and the E-Health Act. The Researcher and IH will not use or disclose such Identifiable Information except with the knowledge and written consent of the Research participant as set out in an

informed consent form, or as approved by the Interior Health Research Ethics Board under a waiver of consent, or as prescribed by law.

3.4 If the Researcher is also an IH employee, they must abide by IH information and security policies including *AR0400 Privacy and Management of Confidential Information* for access to IH information for the purpose of Research. IH employees are not allowed to use their access to IH information systems granted for their employee role for purposes outside of that role without the approval.

3.5 The Researcher and IH must use reasonable care to protect the Identifiable Information against loss, theft, unauthorized access, copying, or modification per IH policies.

3.6 Subject to the requirements of the IH Research Ethics Board (IH REB) approval, the Researcher retains the Identifiable Information only as long as necessary to fulfil the approved Research purpose. When the Research purpose is complete, the Researcher takes appropriate and reasonable care to destroy, erase and make the Identifiable Information anonymous, and to prevent unauthorized access to the de-identified information.

3.7 IH completes an Information Sharing Agreement (ISA) with the Researcher when Identifiable Information of participants is to be released without the consent of those participants, including instances where data linkage involved in the Research project could lead to re-identification of an individual. This may also include the signing of a Confidentiality undertaking with IH.

3.8 IH uses standard provincial processes under the General Health Information Sharing Agreement (GHISA) for the protection of Identifiable Information to be released for multi-jurisdictional Research projects in British Columbia through an Information Sharing Plan (ISP).

3.9 IH information used as data for a Research project is not released. Research cannot commence until a certificate of Institutional Approval to Conduct a Research Project has been issued. The certificate is issued once IH REB ethical approval (if required), IH operational approval and all other contract requirements for the research project have been completed.

4.0 PROCEDURES

4.1 Researcher Responsibilities

4.1.1 Requests information from IH for the purpose of Research and ensures compliance with the *Tri-Council Policy Statement: Ethical Conduct of*

Research Involving Humans (TCPS2) for the use of Identifiable Information, including to:

- Safeguard information entrusted to them and not misuse or wrongfully disclose it;
- Describe measures for meeting Confidentiality obligations and explain any reasonably foreseeable disclosure requirements in application materials they submit to the IH REB and during the consent process with prospective participants; and
- Provide details to the IH REB regarding their proposed measures for safeguarding information for the full life cycle of the Research: its collection, use, storage, dissemination, retention and/or disposal.

4.1.2 Satisfies the IH REB that the secondary use of Identifiable Information when consent is not obtained from participants meets the criteria of TCPS2 and FIPPA.

4.1.3 Obtains IH REB approval prior to carrying out data linkage, unless the Research relies exclusively on publicly available information. The application for ethical approval describes the data to be linked and the likelihood that Identifiable Information is created through the data linkage.

4.1.4 Obtains IH operational approval for the use of IH information from the appropriate Data Steward and/or IH Administrator.

4.1.5 Reviews the information request with the IH Research Department and completes a Research data request form if required.

4.1.6 Completes an ISA with IH if requested by the Research Department.

4.1.7 Ensures that all Research team members are aware of the importance of maintaining the Confidentiality of collected or transferred Identifiable Information and that IH Research team members complete the IH Information Privacy and Security training module.

4.1.8 Protects all IH information released to their possession for the purpose of Research according to the standards set out in IH policies *AR0200 Information Security* and *AR0400 Privacy and Management of Confidential Information*.

4.1.9 Notifies IH at the first reasonable opportunity if Identifiable Information is stolen, lost, or accessed by unauthorized persons, and shall cooperate in informing the individual(s) whose personal information has been compromised, in accordance with legal requirements.

4.1.10 Retains the original Research data for a minimum of five years after publication, or such period as required by funding agencies, or by IH policy *AL0700 Records - Retention, Storage and Destruction of*.

4.1.11 Completes an IH Certificate of Destruction for the source data as proof of destruction of IH information in their possession on completion of the Research project. The mode of destruction will comply with conditions of the ISA and any other agreements executed for the Research project.

4.2 Research Department Responsibilities

4.2.1 Reviews the Data Set request received from the Researcher, verifies the specifications of the request, and identifies the output format and data transfer requirements.

4.2.2 Consults with the Information Privacy and Security Office on any Privacy and security concerns related to Research.

4.2.3 Identifies if an ISA is required and initiates the agreement process if one is required. Files copies of the executed agreement in the Research study file.

4.2.4 Reviews the availability and feasibility of the Data Set request with the Data Steward and/or Data Consultant.

4.2.5 Coordinates the release of the Data Set to the Researcher using a secure data transfer process after the certificate of Institutional Approval to Conduct a Research Project is issued.

4.3 Data Services and Analytics Responsibilities

4.3.1 Data Management identifies the Data Steward(s) for each Data Set requested.

4.3.2 Data Steward reviews the request, including feasibility and quality of the Data Set, and gives approval to retrieve the data for testing.

4.3.3 Data Consultant reviews the Data Set availability, data element specifications, identifies Data Services and Analytics resources required, and extracts the Data Set.

4.3.4 Data Steward provides operational approval for the data request.

4.4 IH Research Ethics Board Responsibilities

4.4.1 Considers the ethical implications for the management of Identifiable Information throughout the Research project including:

- Type of Identifiable Information to be collected;
- Purpose for which the Identifiable Information will be used;
- How the Identifiable Information will be controlled, accessed, disclosed, and de-identified;
- Limits on the use, disclosure and retention of the Identifiable Information;
- Any anticipated secondary uses of Identifiable Information from the Research;
- Any anticipated linkage of Identifiable Information with other data about Research participants, whether those data are contained in public or in personal records;
- Administrative, technical and physical safeguards and practices in place to protect the Identifiable Information including de-identification strategies and managed linkages to identifiable data: and
- How accountability and transparency in the management of Identifiable Information will be ensured and maintained.

4.4.2 Consults with the Information Privacy and Security Office on any Privacy and security concerns related to Research.

4.4.3 Provides an IH Certificate of Destruction for the Primary Investigator to complete for the IH source data on closure of the Research project.

4.5 Information Privacy and Security Responsibilities

4.5.1 Consults with the IH REB on any Privacy and security concerns related to Research.

4.5.2 May conduct electronic audits to monitor access to and use of IH systems for Research purposes.

4.5.3 In collaboration with IH REB and any other parties they deem necessary, oversees suspected or confirmed information Privacy and/or security breaches related to information released for Research purposes.

5.0 REFERENCES

- Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*. (December 2022).
- E-Health (Personal Health Information Access and Protection of Privacy) Act. SBC 2008, Chapter 38.
- Freedom of Information and Protection of Privacy Act (FIPPA). RSBC 1996, c. 165.
- Interior Health. (2023). Administrative Policy Manual: *AR0100 Acceptable Use of Digital Information Systems*.
- Interior Health. (2020). Administrative Policy Manual: *AR0200 Information Security.*
- Interior Health. (2023). Administrative Policy Manual: *AR0400 Privacy and Management of Confidential Information.*
- Interior Health. (2022). Administrative Policy Manual: *AL0700 Records – Retention, Storage and Destruction Of.*
- Interior Health. (2023) Research Department Policy Manual: *RA0700 Confidentiality of Information.*
- Office of the Information and Privacy Commissioner for British Columbia. (2018). Guidance Document: *Access to Health Data for Research.*