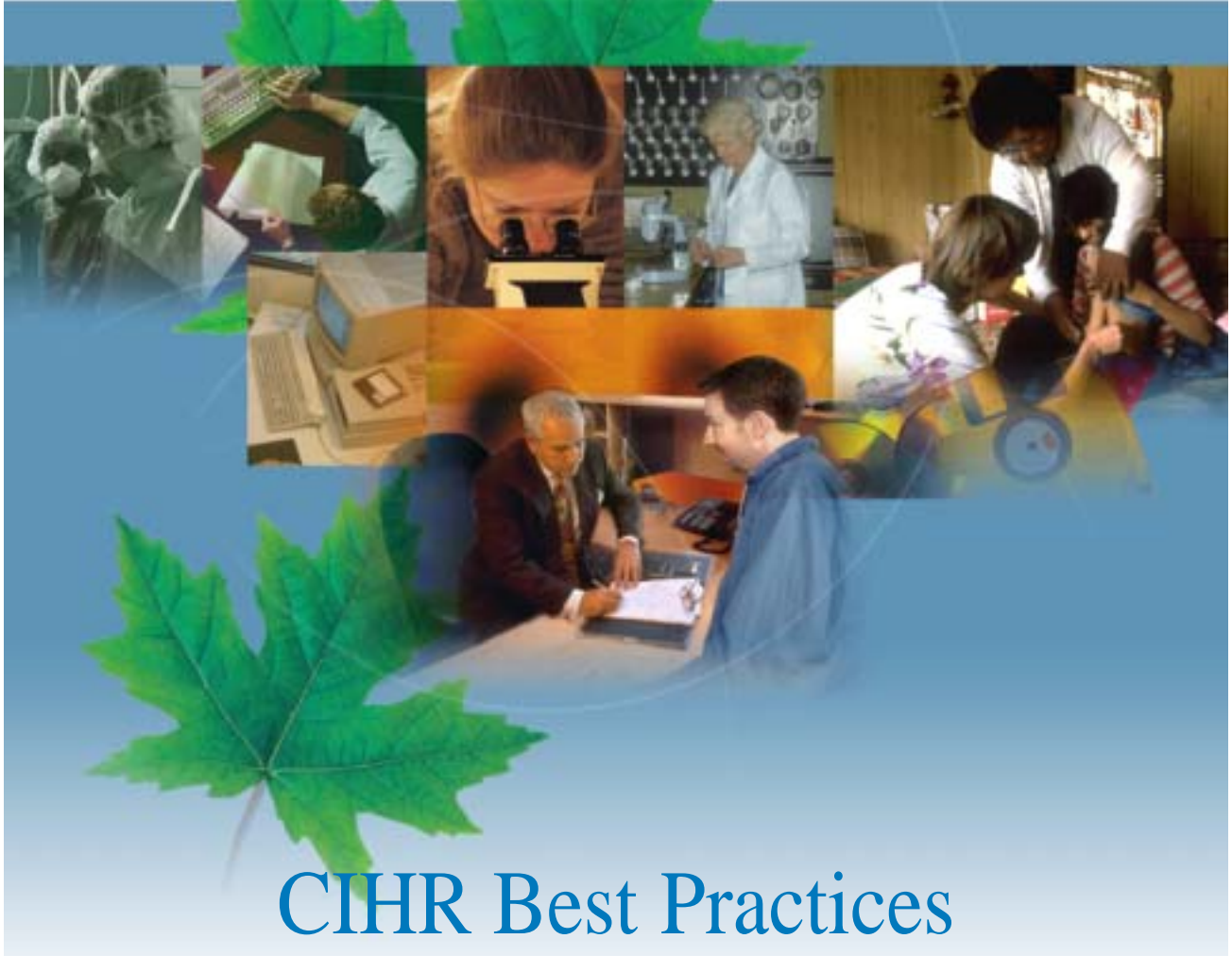




Canadian Institutes of Health Research
Instituts de recherche en santé du Canada



CIHR IRSC
Canadian Institutes of Health Research
Instituts de recherche en santé du Canada



CIHR Best Practices for Protecting Privacy in Health Research

S e p t e m b e r 2 0 0 5

For further information, please contact:
Canadian Institutes of Health Research
160 Elgin Street, 9th Floor
Address Locator 4809A
Ottawa, Ontario K1A 0W9

Telephone: (613) 941-2672
Fax: (613) 954-1800

E-mail: info@cihr-irsc.gc.ca
Web site: www.cihr-irsc.gc.ca

©Public Works and Government Services Canada, 2005
Cat. No.: MR21-63/2005E-PDF
ISBN: 0-662-41056-4

Note: Second Printing. Weblinks updated, November 2005

CIHR Best Practices for Protecting Privacy in Health Research.

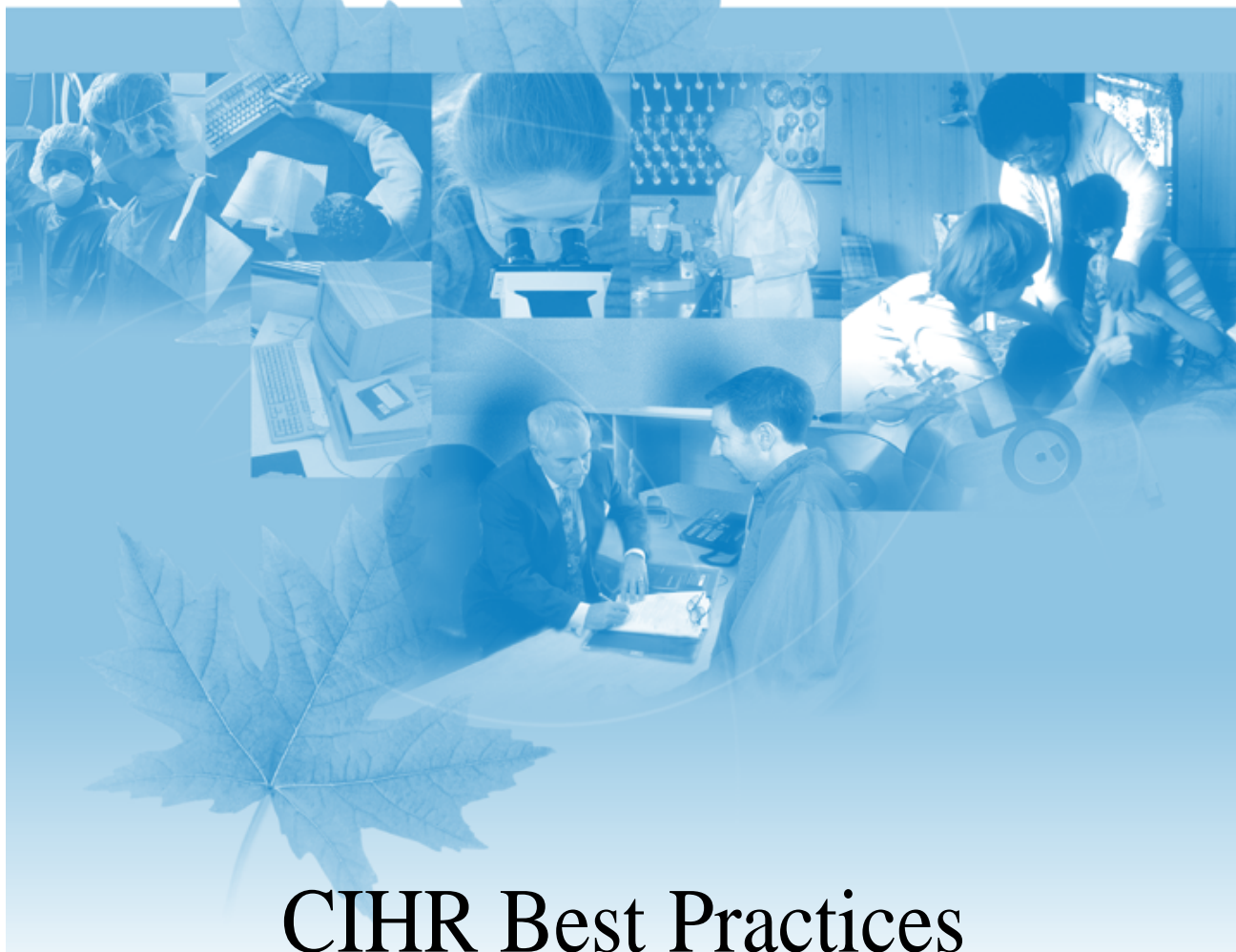




Canadian Institutes of Health Research
Instituts de recherche en santé du Canada



CIHR IRSC
Canadian Institutes of Health Research
Instituts de recherche en santé du Canada



CIHR Best Practices for Protecting Privacy in Health Research

S e p t e m b e r 2 0 0 5

Canada



Table of Contents

Acronyms	v
CIHR Privacy Advisory Committee: Recommendations	1
Privacy Best Practices: 10 elements in summary form	4
How to navigate the document: Areas of special interest	14
Introduction	
CIHR's mandate	15
Goals	15
Statement of values	16
Scope of application	18
Commitment to continuous learning and review	19
Privacy Best Practices: 10 elements	
How to read these elements	21
Element #1 Determining the research objectives and justifying the data needed to fulfill these objectives	23
Element #2 Limiting the collection of personal data	29
Element #3 Determining if consent from individuals is required	37
Element #4 Managing and documenting consent	45
Element #5 Informing prospective research participants about the research	53
Element #6 Recruiting prospective research participants	63
Element #7 Safeguarding personal data	73
Element #8 Controlling access and disclosure of personal data	77
Element #9 Setting reasonable limits on retention of personal data	85
Element #10 Ensuring accountability and transparency in the management of personal data	87

Appendices

A-1	CIHR Privacy Advisory Committee: Members	96
A-2	Drafting process and consultations in 2004	98
A-3	Real world case studies and links to the elements	100
A-4	Diversity of health research and future considerations	103
A-5	Selected documents and web links	108
A-6	Glossary.....	110
A-7	Tables of concordance with privacy legislation.....	113
	Explanatory note	114
	Application of Canadian privacy legislation	115
	For Element #1	118
	For Element #2	119
	For Element #3	121
	• Conditions for use and disclosure for research purposes without consent	
	For Element #4	129
	• Part 1 – Consent requirement and elements of consent	
	• Part 2 – Consent by substitute decision makers	
	For Element #5	135
	• Provision of all information relevant to voluntary and informed consent	
	For Element #6	138
	• Statutory prohibitions to secondary use/disclosure of personal information to contact individuals to participate in research	
	For Element #7	140
	• Part 1 – General safeguarding requirements	
	• Part 2 – Requirement for a privacy impact assessment	
	For Element #8	147
	• Part 1 – Data matching/linkage provisions	
	• Part 2 – Data-sharing agreements for research purposes	
	For Element #9	153
	• Retention and destruction of personal information	
	For Element #10	157
	• Part 1 – Accountability and transparency	
	• Part 2 – Statutory references to research ethics boards	



Acronyms

CIHR	Canadian Institutes of Health Research
CSA	Canadian Standards Association
ICH GCP	International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use- Good Clinical Practice: Consolidated Guideline
NCEHR	National Council on Ethics in Human Research
NIH	National Institutes of Health (United States of America)
NSERC	Natural Sciences and Engineering Research Council of Canada
PAC	CIHR Privacy Advisory Committee
PRE	Interagency Advisory Panel on Research Ethics
REB	Research Ethics Board
RMGA	Quebec Network of Applied Genetic Medicine
SSHRC	Social Sciences and Humanities Research Council of Canada
TCPS	Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, <i>Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans</i> , 1998 (with 2000, 2002, 2005 amendments)
U.S.	United States of America



CIHR Privacy Advisory Committee¹

RECOMMENDATIONS

Background

Recognizing that one of the key ethical challenges for the health research community is to appropriately protect the privacy of those individuals whose information is used for research purposes, CIHR has promoted and initiated dialogue with the broad health research community on a range of privacy-related matters for many years. In particular, a multi-stakeholder workshop in November 2002 entitled *Privacy in Health Research: Sharing Perspectives and Paving the Way Forward* resulted in a number of recommendations, including that CIHR initiate the development of privacy best practices and promote the harmonization of privacy laws and policies that impact on health research.

Privacy Advisory Committee

Following on these recommendations, CIHR established a Privacy Advisory Committee (PAC) in 2003 to advise CIHR on the development of privacy best practices for health research, and on strategies for consultation, communication and knowledge translation. The Committee's mandate ends with the public release of the Privacy Best Practices in 2005.

PAC members are drawn from across Canada and include an international advisor. They represent themselves, not their organizations or institutions. Members bring the perspectives of the following interested groups: privacy commissioners, research ethics boards, health researchers, voluntary health organizations, patients/consumers, policy-makers, data providers, law/ethics, Aboriginal communities, and health service providers. Ex-officio members are drawn from key groups involved in developing or implementing research ethics policy/regulations, namely the Interagency Advisory Panel for Research Ethics, the National Council on Ethics in Human Research, Health Canada, and the Social Sciences and Humanities Research Council of Canada. The Natural Sciences and Engineering Research Council of Canada was invited to appoint a member on PAC but preferred to assume a consultative role. PAC members agreed by consensus to have the CIHR Ethics Office chair the Committee in the role of facilitator.

An earlier version of the current document was the subject of public consultations through 2004. The current document was revised based on feedback received.

¹ Privacy Advisory Committee members are listed in Appendix A-1.

Recommendations

The following recommendations are intended to promote the effective implementation of these Privacy Best Practices in the health research community and to ensure that these best practices continue to respond to the evolving nature of health research and challenges of privacy protection.

Continuous learning and evaluation

- These Privacy Best Practices must continue to evolve to reflect improved practices and innovative solutions over time, and to reflect and influence ongoing legislative developments. Recognizing that important issues have yet to be addressed (see *Key Outstanding Issues*), these should be tackled by developing supporting modules with the active engagement of the relevant communities and through targeted research.
- There should be an assessment of the impact that the Best Practices will have over time on research ethics board decision-making and researcher practice. Mechanisms should be put in place to enable this assessment. These mechanisms should include a formal process, such as a CIHR Standing Committee, to assess implementation and the need for improvement of the Best Practices over time. A web tool should be considered for channelling research findings and capturing practical experiences to inform the ongoing evolution of the Best Practices.

Implementation strategy

- These Privacy Best Practices should be revised in two years. With ongoing feedback and evaluation, PAC expects that the Best Practices will be adapted, as necessary, for the purpose of becoming mandatory CIHR funding policy. These Best Practices should also be referred to the Interagency Advisory Panel on Research Ethics with a view to encouraging their eventual application, in revised form, as Tri-Agency funding policy. For this to happen, the social science perspective needs to be strengthened.

Support for implementation

- Underpinning the implementation strategy for these Privacy Best Practices, there should be a strong emphasis on the importance of training and education support for institutions, research ethics boards and researchers. CIHR should consider developing a web-based document as an educational resource.
- In addition, institutions should be encouraged to provide adequate support for the infrastructure needed to implement and operationalize these Best Practices on a systematic basis. PAC recommends that there be a line item in the budget of researchers' grant applications to

accurately reflect the increased cost involved in adhering to these Best Practices so as to enhance commitment and feasibility.

Harmonization of oversight framework

- There should be continuing efforts by CIHR to support and influence the federal, provincial and territorial legislative harmonization agenda as well as the development of a national system of research ethics oversight.

Key outstanding issues

- Privacy concerns related to the transnational flow of data need to be addressed. These could include clear interpretive provisions and the development of coherent and reciprocal minimum standards to be included in international data transfer agreements.
- A separate process or initiative should be undertaken to develop a policy framework for the physical collection, use and storage of human biological specimens (in contrast to the personal information that may be derived from those specimens) as these are critically important and complex areas of activity that are having increasing importance in research.
- As one important means of responding to public concerns over potential unauthorized uses of personal information gathered for research, CIHR should consider raising discussion among stakeholders and governments about the desirability and feasibility of introducing in Canada instruments such as the Certificates of Confidentiality issued in the United States to protect sensitive information on research participants from forced disclosure.²

² Under section 301(d) of the U.S. *Public Health Service Act* (42 U.S.C. 241(d)) the Secretary of Health and Human Services may authorize persons engaged in biomedical, behavioral, clinical, or other research to protect the privacy of individuals who are the subjects of that research. This authority has been delegated to the National Institutes of Health (NIH) and other Health and Human Services Agencies. Certificates of Confidentiality may be granted for studies collecting information that, if disclosed, could have adverse consequences for research participants, such as damage to their financial standing, employability, insurability, or reputation. A Certificate allows the investigator and others who have access to research records to refuse to disclose identifying information on research participants in any civil, criminal, administrative, legislative, or other proceeding, whether at the federal, state, or local level. See U.S. Office of Human Subject Protection – Guidance online at <http://www.hhs.gov/ohrp/humansubjects/guidance/certconf.htm>.



Privacy Best Practices

10 ELEMENTS IN SUMMARY FORM

These Privacy Best Practices are intended to provide guidance for the health research community in Canada on the application of fair information principles to research involving personal information, and to assist in the interpretation of the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (TCPS) by offering additional detail and practicality.

In turn, as these Best Practices evolve in light of practice, they have the potential to inform the ongoing development of the TCPS and relevant laws and policy.

These Privacy Best Practices do not replace existing laws, policies and professional codes of conduct that apply to certain types of personal information, designated organizations and/or specific kinds of activity.

Privacy Best Practices

The Elements are presented in summary in this section to provide a quick reference for the reader. Full descriptions of each Element along with links to selected excerpts from the TCPS are in the main body of this document.

Tables of Concordances are included in the Appendices to supplement key provisions in the Elements with cross-references to related requirements under Canadian privacy

legislation. The Tables should be used only as preliminary guidance. The application of the information in the Tables to a particular research project should be determined in consultation with a legal advisor.

ELEMENT #1: Determining the research objectives and justifying the data needed to fulfill these objectives

At the outset of the research design process, and as thoroughly as possible given the proposed research method, researchers should:

- identify and document research objectives and questions as a basis for determining what data will be needed;
- anticipate and document research questions related to the primary research objective, which might become relevant after the initial data analyses; and
- anticipate and document likely future uses of the data, including possible collaborations with other researchers or possible commercial uses.

In the case of a *database created for general research purposes*, researchers should define the scope and purpose in a way that will be meaningful for research ethics boards (REBs) and any prospective research participants,

even if the boundaries are at a relatively general level. This is an opportunity to be as open and transparent as possible about the proposed research, and to reassure research participants and REBs that although future research purposes are not specified in detail, data management, storage and use will occur within a defined framework, including review and approval by an REB.

If appropriate, setting up an *advisory committee* drawn from the scientific community, other relevant areas (such as ethics, policy, or information technology) and those affected by the condition or health event under study, can assist in defining the scope and strategic priorities for a research project in the context of both short and long-term initiatives.

All potential relevant and useful research questions cannot always be foreseen at the outset of a research project. For example, researchers using *inductive methods* of research may discover an “emergent” research approach through encounters with and in collaboration with research participants. In such research, the development of research questions and procedures is an ongoing process. While planning their research, researchers should attempt to foresee both obvious and emerging issues related to privacy. These should be included in the submission to an REB. Researchers should also document for an REB any amendments to the protocol and consequent privacy protection strategies emerging over the course of the study.

ELEMENT #2: Limiting the collection of personal data

Researchers should plan to collect personal data only as necessary for the research. The amount of personal information collected and the level of identifiability and sensitivity of this information should be restricted to what is necessary to achieve the research objectives.

Consider first whether individually identifiable data are needed, or whether non-identifiable data or aggregate data would serve the research objectives (e.g. data on individuals grouped by age or some other meaningful variable).

For research involving *secondary use of data* for research, if identifiable data are required for the research, direct identifiers should be avoided or concealed to the extent that is reasonably practical (e.g. as soon as a data linkage has been completed). Data without direct identifiers can be:

- *coded* to allow a trace-back to individuals, by means of:
 - *single-coding* (the researcher has the key to the code to link the research data back to direct identifiers, which are held separately); or
 - *double-coding* (an increased level of confidentiality protection over single coding because the data holder does not give the researcher the key to re-identify individuals); or

- *without a code*, if the capacity to trace the research data or results back to individuals is not required for the research purpose.

Even if the direct identifiers in shared data have been removed or coded, consider how to *minimize the collection or sharing of potentially identifying data elements*.

For *inductive data collection*, for example where open-ended interview techniques are used, the extent of personal data to be collected may not always be foreseeable in detail at the outset of the interview. In these cases, the ongoing negotiation of consent with research participants is the best way to ensure that the privacy of individuals and the community is being appropriately protected.

ELEMENT #3: Determining whether consent from individuals is required

Voluntary and informed consent from legally competent individuals or authorized third parties is a fundamental principle in research involving humans, and specifically for the use of their personal data.

Under specified circumstances, given a satisfactory rationale by the researcher, an REB may approve the waiver of a consent requirement, or a partial waiver of some elements of a consent requirement. According to TCPS Article 2.1(c), the REB must find and document that:

- ̄(i) The research involves no more than minimal risk to the subjects;
- (ii) The waiver or alteration is unlikely to adversely affect the rights and welfare of the subjects;
- (iii) The research could not practicably be carried out without the waiver or alteration;
- (iv) Whenever possible and appropriate, the subjects will be provided with additional pertinent information after participation; and
- (v) The waived or altered consent does not involve a therapeutic intervention."

In addition to REB approval, access to personal data for research without consent will be subject to specific legal requirements in relevant jurisdictions.

When a research objective requires the *collection of personal information directly from individuals to whom the data belong and linking to other sources to form a combined file*, consent should be sought for both types of data collection at the time of direct contact with prospective research participants.

For secondary use of data for research, an REB should consider the following factors in determining whether a research proposal meets the requirements for waiver of consent:

- necessity of personal data for the research purposes;
- potential harms and benefits of the research;
- inappropriateness or impracticability of consent;

- expectations of individuals;
- views of relevant groups;
- legal requirements; and
- openness (informing the public).

These factors, and the description in the Elements, expand on TCPS Article 2.1(c)(i)- (iii).

An REB may determine that seeking consent from individuals is *inappropriate* because there is potential harm to individuals from direct contact, or contact with individuals is not permitted under a previous data-sharing agreement, law or policy.

Seeking consent from individuals for the use of their personal data may be considered *impracticable* when there are difficulties in contacting or notifying individuals for reasons such as:

- the size of the population being researched;
- the proportion of prospective participants likely to have relocated or died since the time the personal information was originally collected; or
- the lack of an existing or continuing relationship between prospective participants and the data holder who would need to contact them (e.g. a patient database that does not have a regular follow-up program to maintain a complete and accurate record of changes in registrants' contact information over time);

such that:

- there is a risk of introducing bias into the research because of the loss of data from segments of the population that cannot be contacted to seek their consent, thereby affecting the validity of results and/or defeating the purpose of the study; or
- the additional financial, material, human, organizational and other resources needed to obtain consent could impose a hardship or burden on the researchers or organization so burdensome that the research could not be done.

ELEMENT # 4: Managing and documenting consent

Consent is an ongoing process that begins upon first contact with prospective participants or authorized third parties, and ends only with the conclusion of their participation in the research or use of their information. Participants should understand that their consent is voluntary, to be obtained without manipulation, undue influence or coercion, and can be withdrawn at any time.

Evidence of initial and ongoing consent and the withdrawal of consent should be *documented* as appropriate for audit and legal purposes.

The majority of research studies use an *opt-in consent*. Opting-in means that prior to the start of the research or data collection, informed individuals give clear indication that they voluntarily agree to participate in the research.

Presumed consent with an opt-out mechanism should be used only when an REB considers prior opt-in consent to be inappropriate or impracticable. A valid opt-out mechanism means that individuals have the opportunity at some time during the research or data collection process to give a clear indication (in writing or orally) that they do not want to be participants in the research or to have their data used in the research. If individuals do not choose to opt-out of the research, their consent is presumed as long as they were given reasonable notice of the research and meaningful opportunity to opt-out.

Collection of data without direct personal identifiers may be necessary or proposed when the research deals with highly sensitive conditions or activities. In such circumstances, consent should be documented but the identity of research participants should not be linkable to their data or to results of analyses.

The researcher may need *information on who does not want to participate in research or who withdraws from research*, for example to document who is not to be included in follow-up research activities; and/or to take into consideration relevant characteristics of the population not included in the study, when reporting possible bias in research results. In these circumstances, researchers may obtain information about non-participants or those withdrawing consent only with individuals' consent or the approval of an REB to waive the consent requirement in the particular circumstances.

Participants in *qualitative studies* are especially vulnerable to unintended identification. For example, in quoting interviewees, biographical details may be revealed that make protecting identities difficult. Therefore, paying attention to the trust relationship between researcher and participant, and obtaining ongoing consent, are very important.

ELEMENT #5: Informing prospective research participants about the research

Researchers should provide to prospective participants or to authorized third parties disclosure of all information relevant to voluntary and informed consent.

Information should be communicated to prospective participants in *plain language*, in oral and/or written form, so that it is easily understood.

The *amount of time* taken to communicate information to prospective participants should be appropriate to the need, not excessive nor too brief. For example, the information could be layered, with a one-page summary of the research, a short consent form, an appendix with more detailed information and instructions on how to obtain more information.

During the consent process, the researcher should determine whether the participant wishes to be *informed of any meaningful research results* that specifically relate to them.

Researchers, particularly those in the areas of health services, population and public health, and genetics/genomic research who study whole populations, should strive to *communicate with the relevant population and governmental authorities regarding results* that are pertinent to the improvement of health and/or the prevention of disease. The population studied should be made aware of possible socio-economic discrimination or group stigmatization as a result of the research results, such as because of perceptions of genetic risks. In the context of genetic research, the population should also be informed of the means taken to minimize the risks.

In the consent process and discussion, researchers using *qualitative methods* may consider involving participants in the writing and reporting process, depending on the circumstances.

For a hybrid project involving the *direct collection of data from individuals and secondary use of data from other sources*, the prospective research participant should also be informed of all expected types and sources of personal data to be used, any expected linkages and the expected purposes for which data will be used.

When personal data are to be entered into a *database for multiple research uses* over an extended period, research participants should also be informed of such things as: expected types of studies, expected data types and purposes, expected commercial uses, data retention period, and the process for

overseeing the use and security of data. Participants may also be given the opportunity to provide *authorization for future uses*, with or without re-contact, including the opportunity to withdraw consent (and any identifying information) in the future. Additional options may include:

- to be re-contacted on a regular (or as needed basis) to seek consent for new research uses of the data, if desired and practicable; and/or
- to not be re-contacted, but to authorize the researchers to use the data only in certain ways in the future (e.g. with or without direct identifiers, coded or in non-identifiable form; or for certain areas of research).

ELEMENT #6: Recruiting prospective research participants

The proposed recruitment procedure and materials should be included in the submission for *REB approval*. The procedure and materials should *foster the conditions for voluntary consent*, and not exert undue influence on prospective participants to agree to take part in research.

Initial contact with individuals about a research project should be made by someone that individuals would expect to have relevant information about them, or in other ways that do not inappropriately intrude on their life or privacy.

Wherever possible, the researcher should *anticipate at the time of the original collection* the future uses of personal information for

further recruitment purposes, and seek consent from individuals for these purposes.

The REB will need to determine if consent is required for the *secondary use of personal information for recruitment purposes*.

Researchers and REBs should be aware of any legal restrictions on contacting individuals in these circumstances.

When a researcher is making a *request for access to data* to recruit participants, the preferred option is for the data holder to determine eligibility of individuals for the research on the basis of criteria provided by the researchers, and to make the initial contact to:

- inform eligible individuals about the research so that they can contact the researcher, if interested, or
- to seek consent from individuals to release their nominal information to the researcher who will contact them to inform them about the research.

When the preferred option is impracticable or inappropriate, an REB may consider whether a researcher should be permitted access to minimal personal data only for the purposes of determining eligibility for the research or contacting individuals to invite them to join the study. If it is legally permissible and the REB considers it appropriate, personal information may be released with appropriate confidentiality protection such as a signed confidentiality agreement with access

restricted to the data holder's site and use limited to the stated purpose.

Researchers should avoid situations where eligible individuals are not aware, prior to being contacted, of information about themselves that makes them eligible for participation in the research, such as a cancer diagnosis.

Typical *scenarios* for recruiting participants, including *community-based research* and *genetics research*, and preferred approaches are briefly described.

ELEMENT #7: Safeguarding personal data

Institutions or organizations where research data are held have a responsibility to establish appropriate institutional security safeguards. Data security safeguards should include organizational, technological and physical measures.

Researchers should take a risk assessment and management approach to protecting research data from loss, corruption, theft or unauthorized disclosure, as appropriate for the sensitivity and identifiability of the data.

REBs should review and approve researchers' proposed measures for safeguarding any personal data to be collected.

ELEMENT #8: Controlling access and disclosure of personal data

Data sharing for research purposes— whether of linked or unlinked data sets— is an important way of enabling socially valuable research. It avoids unnecessary duplication of data collection, which reduces the burden on research participants and permits researchers to use limited or scarce resources more productively.

However, once approved by an REB, there should be strict limits on access to data and secure procedures for data linkage, subject to data-sharing agreements.

When personal data are essential to research objectives and questions, researchers need a plan for making public the results of research in ways that do not permit tracing back to individuals if they do not wish their identities to be known.

The most secure way of conducting *data linkages* requested by external researchers is for the data holder to conduct the linkage and provide linked data sets to the researcher without direct identifiers and at the minimum level of identifiability necessary for the research purpose. If that is not practicable, a trusted third party may conduct the linkage or the researcher may conduct the linkage on the data holder's site. As a last option, a researcher may be permitted to conduct the linkage at a secure site but under strict controls, as specified in a data-sharing agreement.

Following the linkage of datasets, the person doing the data linkage should reduce datasets to the lowest level of identifiability needed to accomplish the research objectives.

Data-sharing agreements bind data providers and researchers to their respective responsibilities and obligations for protecting personal data. Data-sharing agreements should set out the terms and conditions under which data providers will allow researchers to access personal data for research purposes.

In assessing the privacy aspects of research, researchers and REBs should also be aware of the possibility that in some instances *individuals may want their identities to be known*—for example, when individuals want their contribution to research as participants to be recognized, or where they want to help others afflicted with a similar condition. In some *qualitative research*, individual participants may understand and willingly accept the possibility that their identities may be revealed in the public reporting of research results.

ELEMENT #9: Setting reasonable limits on retention of personal data

Personal data should be retained as long as is necessary to fulfill the research purposes. Personal data may then be destroyed or returned to the data provider, if appropriate, as set out in the terms of the original collection, data-sharing agreement, institutional policies, and legal requirements.

Retention periods for personal data should be defined in writing. Researchers should be explicit about what they plan to do with the data they collect and have storage, management and access policies in place.

When personal data are collected in a *database to support general health research purposes* in the future, personal data may be retained for the general purposes originally consented to, subject to security safeguards proportionate to the identifiability and sensitivity of the data.

Administrative databases such as hospital discharge records and vital statistics registries, which may be used to support health research, may retain personal data over the long-term, provided that this is permitted according to legislation or the mandate of a public body such as a government health department.

Any long-term retention of personal data established for general health research purposes should be subject to periodic audits and effective oversight by independent third parties including REBs.

ELEMENT #10: Ensuring accountability and transparency in the management of personal data

Individuals and organizations engaged in health research involving personal data are accountable for the proper conduct of such research in accordance with applicable funding policies, privacy principles and/or

legislation. Processes and practices must be clearly established and implemented in order to give meaningful effect to these policies, principles or laws. Proper accountability and transparency practices require adequate resources for such things as communication, education and training relating to privacy.

Roles and responsibilities of all those involved in the conduct and evaluation of research should be clearly defined and understood, including those of researchers, their employing institutions, REBs, any data stewardship committees, Privacy Commissioners and other legally-designated privacy oversight agencies. Their concerted efforts should aim to provide a coherent governance structure for effective and efficient data stewardship.

Recognizing that transparency may enhance public support for, and interest in, socially valuable research, individuals and organizations engaged in the conduct and evaluation of health research should:

- be open to the public with respect to the objectives of the research;
- be open about the policies and practices relating to the protection of personal data used in the research;
- promote ongoing dialogue between the research community and privacy oversight agencies; and
- promote ongoing dialogue between the research community and the community at large (the public).

When a *database is created for multiple research purposes, or across multiple sites or jurisdictions*, researchers and institutional data holders should promote coordinated and streamlined approaches to the review of privacy and confidentiality concerns, and to data stewardship over the long term.

A *centralized data stewardship committee* could be put in place to authorize future uses of the database in accordance with the research

objectives and, where applicable, within the parameters set by the consent obtained from participants. The responsibilities of this committee could include the review of data access requests; long-term management of the database; coordination of reviews by local REBs (e.g. by means of agreements between REBs, institutions and researchers, as appropriate); and provision of information to the public (e.g. on a web site).

How to navigate the document: Areas of special interest*

Areas of special interest	Element #. section #. subsection #	TCPS excerpts at end of element #
Type of project		
Single research project	1.1, 9.1.1	
Database created for long-term research use	1.2, 5.7, 9.1.2	
Qualitative (e.g. inductive analysis)	1.4, 2.4, 4.3, 5.4, 8.4.1	Element #3
Genetics/Genomics	2.1.2, 3.5, 5.3, 6.3.3	Element #5, 8
Data collection (sources)		
Individuals (legally competent)	2.2, 3.1, 4.1, 5.3.1, 5.5, 6.1.1, 6.2, 6.3	Element #5
Individuals not legally competent		Element #3
Children		Element #3
From individuals & secondary use or disclosure	3.2, 5.6	
Communities	3.3.5, 5.3.2, 6.3.2	
Secondary use or disclosure	2.3, 3.3, 6.1, 8.1	Element #2, 3, 5, 6
Data linkage	2-Summary guide (b), 8.2	Element #8
Real world case studies	Appendix A-3	
Examples of studies recruiting individuals or communities	Appendix A-4 Table 1	
Examples of databases with research potential, in diverse settings	Appendix A-4 Table 2	
Additional stewardship, oversight		
Advisory committee on research priorities	1.3	
Data stewardship committee	10.2.4	
Legal requirements		
Tables of concordance with privacy legislation	Appendix A-7	

* based on feedback during 2004 consultations on draft CIHR privacy best practice guidelines.



Introduction

CIHR'S Mandate

The Canadian Institutes of Health Research (CIHR) is Canada's main federal funding agency for health research. CIHR's mandate is to invest in research that has the potential to lead to improved health³ for Canadians, more effective health services and products, and a strengthened Canadian health care system. CIHR-funded health research must also meet the highest standards of scientific excellence and ethics.

In the area of ethics, one of the key challenges for the health research community is to protect the privacy of individuals and the confidentiality of personal information, at a time of great change in research. For example, technological advances in information technology and the advance of genetic research are challenging existing standards and mechanisms for privacy protection. Also, the sheer number, diversity and complexity of new privacy laws and policies within and beyond Canada's borders are increasing the practical challenges faced by researchers, particularly for those conducting studies across jurisdictions. And, while there are increasing demands for privacy protection in health research, there is also clear recognition that health research plays a critical role in improving the health of Canadians and supporting an evidence-based health care system.

Goals

These Best Practices are intended to be innovative approaches to the challenge of protecting the privacy of individuals and the confidentiality of personal information in the context of health research. These Best Practices are meant to:

- provide guidance for health researchers in the design and conduct of health research involving personal information;
- be a resource for research ethics boards and institutions to consult when reviewing and evaluating health research involving personal information; and
- through the uptake and application of these Best Practices in the development of privacy laws or policies across Canada, contribute toward a more coherent and harmonized framework for addressing privacy and confidentiality issues in health research.

³ The World Health Organization defines "health" as "a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity". From *Preamble to the Constitution of the World Health Organization* as adopted by the International Health Conference, New York, 19-22 June, 1946; signed on 22 July 1946 by the representatives of 61 States (Official Records of the World Health Organization, no. 2, p. 100) and entered into force on 7 April 1948). Online at: <http://www.who.int/about/definition/en/>.

Statement of Values

These Best Practices primarily reflect the values articulated in two foundational documents: the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (TCPS), Canada's national ethics guidelines for research funded by the three main federal funding agencies, and internationally accepted fair information principles codified by the Canadian Standards Association.

Tri-Council Policy Statement (TCPS)

The Best Practices are firmly embedded in CIHR's ongoing commitment to support TCPS.⁴ Compliance with TCPS is mandatory for all research funded through the three main federal research funding agencies: Canadian Institutes of Health Research (formerly Medical Research Council of Canada), Natural Sciences and Engineering Research Council of Canada (NSERC) and Social Sciences and Humanities Research Council of Canada (SSHRC). Research ethics boards (REBs) also use the TCPS as guidance in the review of research funded through other sources.

The broad ethical framework of the TCPS is based on recognition of the need for and social value of research, along with moral imperatives to respect human dignity, ethical guiding principles and the law.⁵ Ethical guiding principles for research include respect for privacy and confidentiality, among the following fundamental and interrelated ethical guiding principles in the TCPS:

Respect for human dignity
Respect for justice and inclusiveness
Respect for free and informed consent
Balancing harms and benefits
Respect for vulnerable persons
Respect for privacy and confidentiality
Minimizing harm
*Maximizing benefit*⁶

The TCPS acknowledges privacy as a fundamental value, and dignity and autonomy of individuals as the ethical basis of respect for the privacy of research subjects. These national research ethics guidelines also recognize that the right to privacy is not absolute and that compelling and specifically identified public interests may justify an infringement of that right, specifically the requirement to obtain consent before collecting, using or disclosing personal information.⁷

⁴ The TCPS can be accessed on the Interagency Advisory Panel for Research Ethics web site at <http://www.pre.ethics.gc.ca/english/policystatement/policystatement.cfm>.

⁵ TCPS, pg. i.4.

⁶ TCPS, *Context of an Ethics Framework*, Section C, pg. i.5.

⁷ TCPS, Section 3- *Privacy and Confidentiality*, pg. 3.1.

Fair information principles

These Best Practices are also grounded in internationally recognized fair information principles, which are at the heart of Canadian privacy legislation and form the basis of the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information*.⁸ These ten core principles are:

- 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.
- 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.
- 3) *Consent* – The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
- 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.
- 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 law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
- 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.
- 7) *Safeguards* – Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- 8) *Openness* – An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- 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.

⁸ The core principles and associated sub-principles of the CSA Model Code were incorporated into the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Schedule 1, accessible on the Department of Justice website at: <http://laws.justice.gc.ca/en/P-8.6/index.html>.

- 10) *Challenging Compliance* – An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

The CSA Code was not designed specifically for the research context. Thus, these Best Practices are intended to provide guidance on the application of these fair information principles to health research.

Scope of Application

Voluntary guidance in the Canadian context

These Best Practices are intended as voluntary guidance for the health research community in Canada. They are based on and are consistent with the TCPS, and they are designed to assist in the interpretation of the TCPS by offering additional detail and practicality. In turn, as these Best Practices evolve in light of practice, they have the potential to inform the ongoing development of the TCPS and relevant laws and policy.

Applicable legislation and policy

These Privacy Best Practices do not replace existing laws, policies and professional codes of conduct that apply to certain types of personal information, designated organizations and/or specific kinds of activity. Researchers, REBs and institutions should be aware of, and continue to comply with, the relevant laws, policies and codes, including the TCPS, that govern research activities in their respective jurisdictions. In the case of multi-centre research crossing provincial, territorial or even national borders, several privacy laws and policies may have to be considered and complied with.

To help health researchers, REBs and others navigate the sea of privacy laws and policies, a series of tables are included in the Appendix highlighting existing requirements relating to privacy in selected legislation.

Health research

Consistent with CIHR's mandate, these Privacy Best Practices are intended to be a resource primarily for the health research community, and are relevant to health research that requires ethics review under the TCPS.⁹

⁹ Research is defined in the TCPS as "a systematic investigation designed to develop or establish principles, facts or generalizable knowledge" (TCPS, pg. 1.1). The range of research requiring ethics review in the TCPS is listed in Appendix 1 (TCPS, pg. A.1).

Health research is interdependent on a range of knowledge-generating activities that are generally perceived to be outside the boundaries of research, but which are related to the improvement of health and health services. These “non-research” activities, such as public health surveillance, health service management, and program quality assurance and improvement, are beyond the manageable scope of the present document. In the future, however, these Best Practices could potentially serve as models for best practices in these related areas, with the necessary adaptations.

Personal information

These Best Practices cover identifiable personal information. Identifiable personal information may contain a direct link to a specific individual (e.g. name and street address, personal health number, etc.) or any element or a combination of elements that allows indirect identification of an individual (e.g. if birth date combined with postal code and other personal information on the record such as ethnicity could lead to the identification of an individual).

The TCPS definition of identifiable personal information covers a wide range of personal information that may be used in the conduct of research.¹⁰ For example, health researchers may need information about such things as a person’s clinical history and use of health care services, but also about broad determinants of health, such as a person’s education, employment, and income level.

The scope of personal information covered in these Privacy Best Practices includes personal information **derived** from blood and other human biological materials (e.g. information such as blood type, DNA code and the presence or absence of disease), but not the materials themselves. The privacy issues related to the banking, storage and use of those biological materials are beyond the scope of this document.

Commitment to Continuous Learning and Review

These Privacy Best Practices are expected to evolve over time in response to changes in the circumstances of research and as new best practices emerge. One of the valuable ways in which researchers, REBs and institutions can assist the evolution of this document is by bringing to the attention of the CIHR Ethics Office lessons learned through the application of these Best Practices and suggesting areas for further development.

Emailed feedback can be sent to the CIHR Ethics Office at ethics-ethique@cihr-irsc.gc.ca.

¹⁰ “Identifiable personal information” is defined in TCPS as: “information relating to a reasonably identifiable person who has a reasonable expectation of privacy. It includes information about personal characteristics such as culture, age, religion and social status, as well as their life experiences and educational, medical or employment histories.” TCPS, Section 3, pg. 3.2.





Privacy Best Practices

Privacy Best Practices: 10 Elements

How to read these elements

These Best Practices are organized into a series of elements that should be considered in the design, conduct and evaluation of health research to address privacy and confidentiality concerns. These elements are not meant to represent a step-by-step process, since many of the elements are interdependent.

As noted in the Introduction, the TCPS and the laws of Canada are the minimum standard for protecting privacy and confidentiality in health research. To indicate the links between these Best Practices and the TCPS, and as another vehicle for promoting wider knowledge of that national Policy Statement, excerpts from TCPS are provided at the end of most Element sections. These are relatively short excerpts and do not include all text related to a particular topic. Readers are encouraged to use these excerpts merely as guides toward a more comprehensive review of the TCPS.¹¹

In addition, concordance tables of selected privacy legislation are presented in the Appendix, organized by the corresponding Best Practice Element and by jurisdiction. These concordance tables are intended to supplement the Best Practices and should only be used as preliminary guidance. The application of the legal provisions in the tables to a particular research project must be determined in consultation with a legal advisor. In addition, any health professional belonging to a regulatory college has the responsibility of complying with that college's code of ethics.

In addition to the TCPS and applicable laws, CIHR-funded researchers conducting clinical trials intended for use in seeking regulatory approval for pharmaceuticals must review and be in compliance with the Food and Drug Regulations – *Division 5 Drugs for clinical trials involving human subjects, the ICH¹² Guidance E6: Good Clinical Practice: Consolidated Guideline* (ICH GCP), and other Health Canada guidance.¹³

Please note the distinction made in these Elements between a “research participant” and “data subject”. In the Best Practices, a **research participant** is an individual who consents to participation in research and who is the subject of personal data or information collected for research. A **data subject** is an individual who is the subject of personal data/information collected for research purposes, but who has not been directly approached to provide consent.

¹¹ The current version of the TCPS and information about its further evolution are accessible on the Interagency Advisory Panel on Research Ethics (PRE) web site at: <http://www.pre.ethics.gc.ca/english/aboutus/aboutus.cfm>.

¹² International Conference on Harmonization of Technical Requirements of the Registration of Pharmaceuticals for Human Use.

¹³ These documents are accessible on the Health Canada Therapeutic Products Directorate website at: http://www.hc-sc.gc.ca/hpfb-dgpsa/inspectorate/drug_gcp_e.html. The Food and Drug Regulations, ICH GCP and further Health Canada guidance documents cover such privacy-related topics as the roles of investigators, industry sponsors and ethics review committees; informed consent of trial subjects; information to be collected from subjects; information to be included in the study protocol; access to trial records and data for quality assurance purposes; and record retention periods. The ICH GCP is also referenced in the TCPS – Section 7 – *Clinical Trials*, pg. 7.3.

ELEMENT #1: Determining the research objectives and justifying the data needed to fulfill these objectives

General statement

At the outset of the research design process, and as thoroughly as possible given the proposed research method, researchers should:

- identify and document research objectives and questions as a basis for determining what data will be needed;
- anticipate and document research questions related to the primary research objective, which might become relevant after the initial data analyses; and
- anticipate and document likely future uses of the data, including possible collaborations with other researchers or possible commercial uses.

1.1 Research study

For each research study, researchers should identify and document the specific research objectives and related research questions.

Researchers should also describe and justify the data needed to fulfill the research objectives and to answer any related research questions.

Example:

Research study: *Impact of ethnic group membership and age on health*

Study objectives: To examine and compare the health status, health care, and social involvement of distinct ethnic groups living in [region X of province Y], to inform policy development by community organizations and governments.

Research questions: (examples) What is the association between health status, experience of health care and ethnicity? What are the impacts of personal support networks and activity level on health status and perceived well-being?

Personal data needed and justification:

Initials: To assist in checking for duplicate records, using a combination of initials and demographic data.

Demographics (date of birth, gender, ethnicity...): Needed to make between-group comparisons on health variables by ethnicity, and between- and within-group comparisons by other demographic variables.

Physical health and sense of well-being/Use of health services: Needed to investigate and compare health status and perceived health status by health care-related knowledge, behaviours, attitudes and use.

Meaning of health and of aging: Needed to explore the meanings of health and illness and the cultural context of aging in the ethnic community.

Family and friends/Social activities: Needed to investigate the impact of family structure and interaction and environmental factors on measures of health and well-being.

1.2 Creation of a database for general research purposes

Define the scope and purpose of the database in a way that will be meaningful for REBs and any prospective research participants, even if the boundaries are at a relatively general level.

Even though all of the research studies that may use data from this database cannot be anticipated or explained in detail at the time the database is being created, try to describe the types of studies that could be undertaken.

In addition to the scope and purpose, describe what the database will not be used for. This is an opportunity to be as open and transparent as possible about the proposed research, and to reassure research participants and REBs that although future research purposes are not specified in detail, data management, storage and use will occur within a defined framework, including review and approval by an REB.

Describe the general types of personal data that are necessary for these general research objectives (e.g. diagnoses, risk factors, outcomes). Include data that are expected to be collected over the lifespan of the database, particularly if there will be multiple data collection periods per participant, or data that will be requested from secondary sources. Be as specific as possible.

Example:

Research database on disease X	
<p>Research objectives:</p> <ol style="list-style-type: none"> 1. Compiling statistics on population trends in disease X and in its risk factors. 2. Conducting health and epidemiological research to improve screening and treatment programs for disease X. <p>Types of research questions (examples):</p> <ol style="list-style-type: none"> 1. What is the association between disease X and risk factors such as diet, tobacco use, physical activity level, education, income or gender? 2. What is the risk of developing disease X after exposure to environmental risk factors, such as pollutants in the area of residence? 3. What is the cost-effectiveness and efficacy of screening programs for disease X? 	
Types of personal data to be collected over multiple collection periods	Research justification
Name, address, telephone number	Contact participants for further data collection
Demographic information	Assess other variables by demographics of the population
Family history	Disease X is known to have an inherited basis
Diet, reproductive factors, physical activity, anthropometric measures, education, income, gender	Assess risk factors for disease X
Medical conditions, medication use	Assess impact of other existing conditions on disease X and effectiveness of medications.
<p>Limits on data uses (examples):</p> <p>Access to data will be restricted to academic and health researchers with a primary purpose of public (non-commercial) benefit, for the purpose of research on disease X or related conditions. The database will be managed by an independent data stewardship committee¹⁴ to ensure that the confidentiality of the information is maintained and access is controlled, consistent with the consents obtained from participants. Any future use of the data for new purposes will require approval by an REB.</p>	

¹⁴ A data stewardship committee could be established to oversee and authorize future uses of the database in accordance with the research objectives. This committee could also assist in coordinating reviews by local REBs, in the case of multi-site studies. See Element #10, 10.2.4.

1.3 Advisory committee for defining the scope and strategic priorities of the research

If appropriate, setting up an advisory committee drawn from the scientific community, other relevant areas (such as ethics, policy, or information technology) and those affected by the condition or health event under study, can assist in defining the scope and strategic priorities for a research project in the context of both short and long-term initiatives.

Data stewardship tasks could be addressed by this advisory committee or by another body, as described in Element #10, 10.4.

Example:

Multi-year family-centered study on childhood condition X

Research objectives

1. Track and assess the factors that facilitate or hinder the development of family-centered provincial services for children with condition X and their family members.
2. Provide guidance to community organizations and provincial governments.
3. Validate questionnaire and interview methods for creating individualized family service plans.
4. Assess long term effectiveness and adverse effects of standard and emerging treatments for Condition X.

Setting the scope of research

- Initial partnership between the research team and Provincial Ministry of Children's Services results in agreement on key objectives.
- A Local Advisory Committee is established to assist in setting out the scope and strategic priorities for the research program, to review research progress, to facilitate the achievement of study objectives, and to assist with the dissemination of results; with representatives from the Ministry, provincial clinic for childhood condition X, two community advocacy groups for persons with condition X, and parent representatives.
- A National Project Advisory Committee with representation from provinces actively interested in this initiative meets annually to advance services to young children with condition X, and to plan and disseminate research findings.

1.4 Qualitative research using inductive data collection and analysis

It is important to recognize that all potential relevant and useful research questions cannot always be foreseen at the outset of a research project. For example, researchers using inductive methods of research may discover an “emergent” research approach through encounters with and in

collaboration with research participants. In such research, the development of research questions and procedures is an ongoing process. For example, open-ended interviewing often goes down avenues not anticipated leading to new questions and new approaches.

The wide range of methods in inductive approaches makes it difficult to document detailed and specific strategies for protection of privacy. Therefore, while planning their research, researchers should attempt to foresee both obvious and emerging issues related to privacy. These should be included in the submission to a research ethics board.

Researchers should also document for a research ethics board any amendments to the protocol and consequent privacy protection strategies emerging over the course of the study. For relatively junior researchers, mentorship can be especially helpful for ensuring adherence to REB requirements.

LINK TO TRI-COUNCIL POLICY STATEMENT:

[Informing prospective participants of purposes]

Article 2.4 "...researchers or their qualified designated representatives shall provide prospective subject with the following: ... (b)..."A comprehensible statement of the research purpose..." (pg. 2.5)

[Informing REBs of purposes]

Article 3.2 "...researchers shall secure REB approval for obtaining identifiable personal information about subjects. Approval for such research shall include such considerations as: (a) The type of data to be collected; (b) The purpose for which the data will be used;..." (pg. 3.3)

ELEMENT #2: Limiting the collection of personal data

General statement

Researchers should plan to collect personal data only as necessary for the research. The amount of personal information collected and the level of identifiability and sensitivity of this information should be restricted to what is necessary to achieve the research objectives.¹⁵

2.1 Personal data: Identifiability and sensitivity

2.1.1 Identifiability

Limiting data identifiability means minimizing as much as possible, the collection of:

- direct identifiers (e.g. name, street address) and
- other data items that could potentially be used to identify an individual.

Data identifiability can be characterized as being on a continuum, in which the division between degrees of “identifiability” are not always clear-cut. Even a dataset without direct identifiers may present a risk of indirectly identifying data subjects if the dataset contains sufficient information about the individuals concerned.

For example, data items that may increase the likelihood of an individual's identity being inadvertently revealed include:

- geographic location (e.g. location of residence, location of health event),
- named facilities and service providers,
- dates (e.g. date of an automobile accident),
- uncommon characteristics of the individual (e.g. a rare health condition or occupation), or
- highly visible characteristics of the individual (e.g. ethnicity in certain locales).

These types of data items, if needed for the research, should be collected at a minimum level of detail consistent with the research objectives.

¹⁵ See the table of concordance for Element #2 in Appendix A-7 referring to the statutory provisions regarding the general requirement to collect a limited amount of personal information.

2.1.2 Sensitivity

The sensitivity of personal data is related to the potential for harm or stigma that might attach to the identification of an individual because of the nature of the information.¹⁶ The type of information that an individual may consider sensitive could relate to:

- sexual attitudes, practices and orientation;
- use of alcohol, drugs, or other addictive substances;
- illegal activities;
- suicide;
- sexual abuse;
- sexual harassment;
- an individual's psychological well-being or mental health;
- some types of genetic information (e.g. information that predicts future illness or disability and raises concerns around future employability or insurability); and
- any other information that, if released, might lead to social stigmatization or discrimination.

Researchers should also be aware of information that communities may consider sensitive because, for example, of its potential to stigmatize a community.

2.2 Collection from individuals

2.2.1 Consider first whether individually identifiable data are needed, or whether non-identifiable data or aggregate data would serve the research objectives (e.g. data on individuals grouped by age or some other meaningful variable).

2.2.2 If identifiable data are needed to meet the research objectives, determine the minimum level of identifiability that will be needed.

Does the researcher need to do any or all of the following:

- Contact the research participant for follow-up data collection?
- Provide data, with consent, to a health care provider to ensure clinical monitoring of the participant?







¹⁶ See TCPS excerpt (Article 3.3, explanatory note) at the end of Element #2.

- Return individual results to the participant?
- Conduct data linkage with a high degree of accuracy?

If yes, the researcher will likely propose the collection of direct identifiers.

If these are not requirements of the research, the researcher should not collect direct identifiers. However, other potentially identifying elements may be needed to answer the research questions and for other data management reasons, such as to check for duplicate records. The lowest level of identifiability of these other data items should be used, consistent with the research objectives.

Examples of reducing personal detail in specific data items collected:

Personal details	 Most identifiable Least identifiable
<p>Subject name</p>  <ul style="list-style-type: none"> • Full name • Partial name • Initials • Code • Blank <p>Age</p>  <ul style="list-style-type: none"> • Birth day/month/year • Birth month/year • Birth year; Age at time of data collection • Age range (e.g. 5 or 10-year age groups) <p>Facilities and service providers</p>  <ul style="list-style-type: none"> • Name of institution/provider • Specific type of facility, provider (university hospital, family physician) • Generic class (hospital, medical doctor) 	<p>Location of residence</p>  <ul style="list-style-type: none"> • Street address • 6-character postal code (e.g. one side of a city street; average of 15 households) • first 3 characters of postal code/Forward Sortation Area (average of 7,000 households) • first character of postal code (province or region: e.g. A= Nfld/Lab.; J = Que. West; K = Eastern Ont.) <p>Census area</p>  <ul style="list-style-type: none"> • Block (an area equivalent to a city block bounded by intersecting streets; the smallest geographic area for which population and dwelling counts are disseminated) • Census enumeration or dissemination area (small area composed of one or more neighbouring blocks, used by Statistics Canada for distributing questionnaires to households and dwellings for the census collection) • Census subdivision (e.g. municipality, village) • Census agglomeration (urban core: min. 10,000 pop.) • Census metropolitan area (urban core: min. 100,000 pop.)

2.3 Secondary use

2.3.1 As in 2.2.1, consider whether aggregate data on groups of individuals would serve the research objective. If not, consider whether non-identifiable data relating to individuals would serve the purpose.

2.3.2 Removal or coding of direct identifiers

If identifiable data are required for the research purpose, direct identifiers should be avoided or concealed to the extent that is reasonably practical (e.g. as soon as a data linkage has been completed). Data without direct identifiers can be:

- coded to allow a trace-back to individuals, by means of:
 - single-coding (the researcher has the key to the code to link the research data back to direct identifiers, which are held separately); or
 - double-coding (an increased level of confidentiality protection over single coding because the data holder does not give the researcher the key to re-identify individuals); or
- without a code, if the capacity to trace the research data or results back to individuals is not required for the research purpose.

Even if the direct identifiers in shared data have been removed or coded, consider how to minimize the collection or sharing of potentially identifying data elements.

2.4 Inductive data collection

For inductive data collection, for example where open-ended interview techniques are used, the extent of personal data to be collected may not always be foreseeable in detail at the outset of the interview. In these cases, the ongoing negotiation of consent with research participants is the best way to ensure that the privacy of individuals and the community is being appropriately protected.

Definition of terms: Individual identifiability of data

Levels of data identifiability by capacity to identify or re-identify individuals

In rank order from most to least identifiable

1) Directly identifiable: The data contains direct identifiers of an individual (e.g. name, address, health number).

2) Coded:

- i) **Single coded:** A participant's data are assigned a random code. Direct identifiers are removed from the dataset and held separately. The key linking the code back to direct identifiers is available only to a limited number (e.g. senior members) of the research team.
- ii) **Double or multiple coded:** Two or more codes are assigned to the same participant's data held in different datasets (e.g. health administrative data, clinical data, genetic samples and data). The key connecting the codes back to participants' direct identifiers is held by a third party (such as the data holder) and is not available to the researchers.

3) Not directly identifiable and not coded: Direct identifiers were never collected or have been deleted, and there is no code linking the data back to the individual's identity.

4) Non-identifiable: Any element or combination of elements that allows direct or indirect identification of an individual was never collected or has been removed, although some elements may indirectly identify a group or region. There is no code linking the data back to the individual's identity.

Summary guide: Levels of data identifiability needed for research-related purposes

Research-related purposes	Specific examples	Data requested for these purposes when:	
		Collecting data directly from individuals:	Requesting data for secondary use:
a) Contact individuals	Recruit individuals for a research project	Direct identifiers	Coded (Single coding is a more efficient mechanism for linking back to individuals than double-coding. Linking back becomes increasingly difficult for investigators who receive double or multiple-coded data, and therefore do not have the key to the code.)
	Contact the participant for follow-up data collection		
	Provide data, with consent, to health care provider for clinical monitoring of the participant		
	Return individual results to the participant		
b) Data linkage¹⁷	Conduct a data linkage with a high degree of accuracy	Preferred: Direct identifiers (e.g. name and street address; or personal health number) ¹⁸	Preferred: Data holder conducts linkage and provides to researcher the linked dataset without direct identifiers. Data to be provided at the lowest level of identifiability needed, consistent with the research objectives.
	Conduct a data linkage with a measurable degree of accuracy sufficient for the particular research	Direct identifiers or potentially identifying data items (e.g. date of birth, initials, 3-character or full postal code, gender, specific health data)	
c) Data accuracy check	Eliminate duplicate records	Direct identifiers or potentially identifying data items	Coded data so that the data holder (preferred) or researcher can use the key to check direct identifiers for duplication
d) No contact with individuals and no data linkage needed		No direct identifiers need to be collected.	No direct identifiers. Data to be provided at the lowest level of identifiability needed, consistent with the research objectives.

¹⁷ See also Element #8, 8.2.

¹⁸ See the legal concordance table for Element #2 in Appendix A-7 regarding the collection of health numbers under Ontario's health privacy legislation.

LINK TO TRI-COUNCIL POLICY STATEMENT:

[REB approval of type of data]

Article 3.2 "...researchers shall secure REB approval for obtaining identifiable personal information about subjects. Approval for such research shall include such considerations as: (a) the type of data to be collected..." (pg. 3.3)

[Secondary use of data]

Article 3.3 "If identifying information is involved, REB approval shall be sought for secondary uses of data. Researchers may gain access to identifying information if they have demonstrated to the satisfaction of the REB that: (a) identifying information is essential to the research..." (pg. 3.5)

Article 3.3 Explanatory text: "Databases can vary greatly in the degree to which personal information is identifiable. A proportionate approach should be applied by the REB to evaluate the sensitivity of the information in the database and to modulate its requirements accordingly. If it is impossible to identify individuals whose records exist within a database, then researchers should be allowed access to that database. The REB must carefully appraise the possibility of identification, in particular with regard to the extent of the harm of stigma that might be attached to identification. The REB and the researcher should also be aware of legal provisions that affect the database(s) to be used in the research.

REBs and researchers should also be sensitive to the context in which the database was created, such as a confidential relationship, as well as to the expectations of the groups or individuals at the time of the collection of the data with regard to its use, retention and disclosure. When it is unclear as to whether information is to be regarded as personal, researchers should consult their REBs. Confidential information collected in this manner should normally not be transmitted to authorities, unless required by law, the courts or similar legally constituted bodies." (pg. 3.5)

ELEMENT #3 : Determining whether consent from individuals is required

General statement

Voluntary and informed consent from legally competent individuals or authorized third parties is a fundamental principle in research involving humans, and specifically for the use of their personal data.¹⁹

Under specified circumstances, given a satisfactory rationale by the researcher, an REB may approve the waiver of a consent requirement, or a partial waiver of some elements of a consent requirement. According to TCPS Article 2.1(c), the REB must find and document that: “(i) The research involves no more than minimal risk²⁰ to the subjects; (ii) The waiver or alteration is unlikely to adversely affect the rights and welfare of the subjects; (iii) The research could not practicably be carried out without the waiver or alteration; (iv) Whenever possible and appropriate, the subjects will be provided with additional pertinent information after participation; and (v) The waived or altered consent does not involve a therapeutic intervention.”

In addition to REB approval, disclosure of personal data for research without consent will be subject to other specific legal requirements in relevant jurisdictions.²¹

3.1 Collection from individuals

The requirement for consent from participants applies to research involving:

- Collection of personal (including genetic) information from persons (e.g. in face-to-face meetings, by mail, telephone or email).
- Procedures to screen for, prevent or treat disease.
- Medical examinations.
- Clinical trials of new drugs or other health care products.²²

¹⁹ See TCPS excerpts at the end of Element #3 regarding the definition of “competence” in the research context. See also the legal concordance table for Element #4-Part 2, Consent by Substitute Decision Makers, in Appendix A-7.

²⁰ For a definition of minimal risk, the TCPS states: “if potential subjects can reasonably be expected to regard the probability and magnitude of possible harms implied by participation in the research to be no greater than those encountered by the subject in those aspects of his or her everyday life that relate to the research then the research can be regarded as within the range of minimal risk” (TCPS Section 1, C1, pg. 1.5). For secondary use of information, the researcher must, among other conditions, have appropriate measures “to minimize harms to subjects” (TCPS Article 3.3 (b)).

²¹ See the legal concordance table for Element #3 in Appendix A-7.

²² As required under the Food and Drug Regulations and ICH GCP.

3.2 Direct collection and secondary use (Hybrid model)

When a research objective requires the collection of personal information directly from individuals to whom the data belong and subsequent linking to other sources to form a combined file, consent should be sought for both types of data collection at the time of direct contact with prospective research participants.

If the secondary use involves identifying individuals eligible to be invited into a study, the procedures under Element #6 are applicable. As described in Element #6, the preferred practice is for a data holder to assess the eligibility of individuals for a particular research project (e.g. on the basis of criteria provided by the researcher). The data holder would then make the initial contact with individuals to seek their permission for disclosure of contact information to a researcher or to inform them as to how to contact a researcher. An REB will need to determine if consent is required for this secondary use of data and for the contacting of individuals.

3.3 Secondary use

When personal data are to be collected from sources other than the individuals to whom the data relate, consent should be obtained from those individuals unless an REB determines that a waiver of consent is appropriate in the specified circumstances. These circumstances should include that a waiver of the consent requirement is permitted by law.²³

For secondary use of data for research, an REB should consider the factors set out in the following table in determining whether a research proposal meets the requirements for waiver of consent. These factors, and their description in the table, expand on TCPS Article 2.1(c)(i)- (iii).

²³ For conditions in privacy legislation under which a waiver of the consent requirement may be permitted see the legal concordance table for Element #3 in Appendix A-7.

Factors to consider in determining whether a research proposal meets the requirement for waiver of consent		
	<i>Factor</i>	<i>Explanation</i>
3.3.1	Necessity of the personal data.	Personal data, in the proposed amount and at the proposed level of identifiability and sensitivity, are necessary to fulfill the research objectives. (See Element #2)
3.3.2	Harm-benefit analysis, where (1) the risk of harm is minimal, and (2) potential benefits of the research to the public and individuals outweigh any potential harm to research participants or data subjects.	<p>1) The research should present minimal risk of harm to individuals and, if appropriate, particular groups or communities. In assessing potential harm, REBs should consider:</p> <ul style="list-style-type: none"> • the probability of harm (related to the identifiability of data²⁴ and the adequacy of security measures)²⁵, and • the magnitude of potential harm (related to the sensitivity of data),²⁶ including potential: <ul style="list-style-type: none"> – physical injury; – emotional or psychological harm; – social harm (e.g. stigmatization); – financial harm (e.g. insurability, employability); – loss of trust; – harm from a perceived invasion of privacy, such as when a researcher has made secondary use of existing records with an REB waiver of the consent requirement, and then proposes to contact individuals for additional data collection; or – negative impact of the findings of the research. <p>2) Potential benefits of the research to individuals, groups, communities or the public outweigh potential harms. Where there is only minimal risk of harm, the REB need only ensure that there is public interest or other merit in the proposed research (e.g. as determined by a peer-review committee).²⁷</p>
3.3.3	A consent requirement being (1) inappropriate or (2) impracticable. ²⁸	<p>1) Seeking consent from individuals may be considered inappropriate because:</p> <p>(a) there is potential harm to individuals from direct contact where there is:</p> <p>(i) a risk of inflicting psychological, social or other harm by contacting individuals or families with particular conditions (e.g. where</p>

²⁴ See Element #2, 2.1.

²⁵ The REB should review and approve the researcher's proposed measures for safeguarding personal data. See also Element #7, Element #8, and Element #10, 10.2.3.

²⁶ See Element #2, 2.2.

²⁷ Note that the TCPS (Article 1.5 and explanatory text) states that REBs are normally to avoid duplicating previous professional peer-review assessments of the scientific merit of a research proposal unless there is a good and specified reason to do so. REBs may have specific criteria, set out in legislation, to take into account in assessing the potential benefits of research proposing to use health sector data without consent (e.g. the requirements set out in Alberta's *Health Information Act*, referenced in the legal concordance table for Element #3, in Appendix A-7.)

²⁸ See real world examples summarized in Appendix A-3, from *CIHR Secondary Use of Personal Information in Health Research: Case Studies* (November 2002), online at <http://www.cihr-irsc.gc.ca/e/1475.html>.

		<p>making contact might reveal an individual's condition to others, against the individual's wishes; or research with minors, which would normally require parental consent, when the minors are street youth who have left home to escape abuse) or in certain circumstances (e.g. during a hospital emergency room visit); or</p> <p>(ii) a risk of creating additional threats to privacy by having to link otherwise usable coded data with identifiers in order to contact individuals to seek their consent; or</p> <p>(b) contact with individuals is not permitted under a previous data-sharing agreement, law or policy.²⁹</p> <p>2) Seeking consent from individuals for the use of their personal data may be considered impracticable³⁰ when there are difficulties in contacting or notifying individuals for reasons such as:</p> <ul style="list-style-type: none"> • the size of the population being researched; • the proportion of prospective participants likely to have relocated or died since the time the personal information was originally collected; or • the lack of an existing or continuing relationship between prospective participants and the data holder who would need to contact them (e.g. a patient database that does not have a regular follow-up program to maintain a complete and accurate record of changes in registrants' contact information over time); <p>such that:</p> <p>(a) there is a risk of introducing bias into the research because of the loss of data from segments of the population that cannot be contacted to seek their consent, thereby affecting the validity of results and/or defeating the purpose of the study; or</p> <p>(b) the additional financial, material, human, organizational and other resources needed to obtain consent could impose a hardship or burden on the researchers or organization so burdensome that the research could not be done.</p>
--	--	---

²⁹ For legal prohibitions against contacting individuals see the legal concordance table for Element #6 in Appendix A-7. For an example of prohibitions against contact in policy, see CIHR *Secondary Use of Personal Information in Health Research: Case studies* (November 2002), Case Study #10, in which researchers investigating cancer screening services were unable to institute a consent process in part because of an existing policy which prevented physicians (who were the data holders) from contacting patients.

³⁰ These conditions are characteristic of much health services and population and public health research where whole populations (not specific individuals) are being studied.

3.3.4	Expectations of individuals.	In general, the expectations of a reasonable person in the circumstances should be taken into account (considering, for example, the nature of the research, the type of data to be collected and the context in which the data were originally collected). If individuals have previously objected to the secondary use of their data for research or to the use of their contact information, their directions should be respected.
3.3.5	Views of relevant groups.	<p>Privacy concerns may extend beyond the individual to include well-defined groups or communities, e.g. remote communities and Aboriginal peoples.³¹ Also, genetic information about individuals is more than personal information—it may also be intimate information about those who share a common genetic lineage—family members, other relatives and, in some cases, well-defined communities.³²</p> <p>The REB may require that efforts be made to consult with family groups, Aboriginal peoples, community representatives, consumer associations, and/or special populations such as the homeless or under-housed, as appropriate, to address possible concerns of affected individuals and communities. These concerns may relate to the design and scope of the research, the recruitment of individuals, and the analysis and disseminations of results of research. This consultation process will be a high priority when dealing with controversial issues and/or individuals, groups or communities in vulnerable circumstances.</p>
3.3.6	Legal requirements.	<p>In addition to REB approval, access to personal data for research without consent will be subject to specific legal requirements in relevant jurisdictions. For example, some jurisdictions require some or all of the following:</p> <ul style="list-style-type: none"> • a data-sharing agreement between the data holder and the researcher;³³ • notification and/or approval by other relevant oversight bodies;³⁴ and/or • agreement that personal data will not be used to contact individuals.³⁵
3.3.7	Openness: Informing the public.	In the spirit of openness, the researcher should have an appropriate strategy for informing the general public about the research. ³⁶

³¹ See TCPS Chapter 6—*Research Involving Aboriginal Peoples* (under review).

³² See TCPS Article 8.1 for more on this topic.

³³ See Element #8; and the legal concordance table for Element #8, Part 2, in Appendix A-7 for legal references to data-sharing agreements for research purposes.

³⁴ As above.

³⁵ See the legal concordance table for Element #6 in Appendix A-7 for statutory prohibitions to contacting individuals.

³⁶ See also Element #10.

LINK TO TRI-COUNCIL POLICY STATEMENT:

[Requirements for consent]

Article 2.1 *“(a) Research governed by this Policy... may begin only if (1) prospective subjects, or authorized third parties, have been given the opportunity to give free and informed consent about participation...*

(c) The REB may approve a consent procedure which does not include, or which alters, some or all of the elements of informed consent... or waive the requirement to obtain informed consent, provided that the REB finds and documents that: (i) The research involves no more than minimal risk to the subjects; (ii) The waiver or alteration is unlikely to adversely affect the rights and welfare of the subjects; (iii) The research could not practicably be carried out without the waiver or alteration; (iv) Whenever possible and appropriate, the subjects will be provided with additional pertinent information after participation; and (v) The waived or altered consent does not involve a therapeutic intervention.” (pg. 2.1)

[Randomized clinical trials]

Article 2.1 *“... (d) In studies including randomization and blinding in clinical trials, neither the research subjects nor those responsible for their care know which treatment the subjects are receiving before the project commences. Such research is not regarded as a waiver or alteration of the requirements for consent if subjects are informed of the probability of being randomly assigned to one arm of the study or another.” (pg. 2.1)*

[Naturalistic observation]

Article 2.3 *“REB review is normally required for research involving naturalistic observation. However, research involving observation of participants in, for example, political rallies, demonstrations or public meetings should not require REB review since it can be expected that the participants are seeking public visibility.” Explanatory text: “Naturalistic observation is used to study behaviour in a natural environment. Because knowledge of the research can be expected to influence behaviour, naturalistic observations generally implies that the subjects do not know that they are being observed, and hence cannot have given their free and informed consent...In considering research involving naturalistic observation, researchers and REBs should pay close attention to the ethical implications of such factors as: the nature of the activities to be observed; the environment in which the activities are to be observed (in particular, whether it is to be staged*

for the purposes of the research); and the means of recording the observations (in particular, if the records will allow subsequent identification of the subjects). Naturalistic observation that does not allow for the identification of the subjects, and that is not staged, should normally be regarded as of minimal risk..." (pg. 2.5)

[Legal competence]

"Competence refers to the ability of prospective subjects to give informed consent in accord with their own fundamental values. It involves the ability to understand the information presented, to appreciate the potential consequences of a decision, and to provide free and informed consent... It does not require prospective subjects to have the capacity to make every kind of decision. It requires that they be competent to make an informed decision about participation in particular research... The law on competence varies between jurisdictions. Researchers must comply with all applicable legislative requirements. Ethical consideration around research involving those who are not competent to give a free and informed consent on their own behalf must seek to balance (1) the vulnerability that arises from their incompetence with (2) the injustice that would arise from their exclusion from the benefits of research..." (pg. 2.9)

Article 2.5 "Subject to applicable legal requirements, individuals who are not legally competent shall be asked to become research subjects only when: (a) The research question can only be addressed using individuals within the identified group(s); and (b) Free and informed consent will be sought from their authorized representative(s); and (c) The research does not expose them to more than minimal risks without the potential for direct benefits for them." (pg 2.9)

Article 2.6 "For research involving incompetent individuals, the REB shall ensure that, as a minimum, the following conditions are met: (a) The researcher shall show that free and informed consent will be sought from the authorized third party, and how the subjects' best interests will be protected. (b) The authorized third party may not be the researcher or any other member of the research team. (c) The continued free and informed consent of an appropriately authorized third party will be required to continue the participation of a legally incompetent subject in research, so long as the subject remains incompetent. (d) When a subject who was entered into a research project through third-party authorization becomes competent during the project, his or her informed consent shall be sought as a condition of continuing participation." (pg. 2.10)

Article 2.7 "Where free and informed consent has been obtained from an authorized third party, and in those circumstances where the legally incompetent individual understands the nature and consequences of the research, the researcher shall seek to ascertain the wishes of the individual

concerning participation. The potential subject's dissent will preclude his or her participation.” (pg. 2.10)

[Research with children]

“..the notion of harm applied to children should be understood differently from harm in adults. Harm induced in children may have longer-term consequences to their growth and development. Furthermore, harms and benefits for children with chronic disabilities and terminal illnesses require special consideration. Every researcher working with child subjects must consider the possibility of the children suffering pain, anxiety or injury, and must develop and implement suitable precautions and ameliorating measures. Cumulative physical, moral, psychological and social consequences (relevant to pain, anxiety and injury) should be reviewed by REBs when assessing the probability, magnitude and character of any harmful impact the research may have on the child.” (pg 2.10)

[Secondary use of data]

Article 3.3 “If identifying information is involved, REB approval shall be sought for secondary uses of data. Researchers may gain access to identifying information if they have demonstrated to the satisfaction of the REB that: (a) identifying information is essential to the research;(b) They will take appropriate measures to protect the privacy of the individuals, to ensure the confidentiality of the data, and to minimize harms to subjects; and (c) Individuals to whom the data refer have not objected to secondary use.” (pg. 3.5)

Article 3.4 “The REB may also require that a researcher's access to secondary use of data involving identifying information be dependent on (a) The informed consent of those who contributed data or of authorized third parties; or (b) An appropriate strategy for informing the subjects; or (c) Consultation with representatives of those who contributed data.” (pg. 3.5)

ELEMENT # 4: Managing and documenting consent

General statement

Consent is an ongoing process that begins upon first contact with prospective participants or authorized third parties, and ends only with the conclusion of their participation in the research or the use of their information. Participants should understand that their consent is voluntary, to be obtained without manipulation, undue influence or coercion, and can be withdrawn at any time.³⁷

Evidence of initial and ongoing consent and the withdrawal of consent should be documented as appropriate for audit and legal purposes.

4.1 Forms of consent

4.1.1 Opt-in consent

The majority of research studies use an opt-in consent. Opting-in means that prior to the start of the research or data collection, informed individuals give clear indication that they voluntarily agree to participate in the research.

Opt-in consent can be indicated in writing (e.g. by signing a consent form), orally (e.g. in a face-to-face or telephone encounter with the researcher) or by conduct (e.g. by filling out and returning a questionnaire received by mail). Consent is only voluntary if it can be withdrawn at any time.³⁸

4.1.2 Presumed consent with opt-out

Presumed consent with an opt-out mechanism should be used only when an REB considers prior opt-in consent to be inappropriate or impracticable.

A valid opt-out mechanism means that individuals have the opportunity at some time during the research or data collection process to give a clear indication (in writing or orally) that they do not want to be participants in the research or to have their data used in the research.

If individuals do not choose to opt-out of the research, their consent is presumed as long as they were given reasonable notice of the research and meaningful opportunity to opt-out.

³⁷ See table of concordance for Element#4, Part 1, in Appendix A-7 for statutory references to the general consent requirement. Part 2 of the concordance table sets out the statutory references to consent by substitute decision-makers.

³⁸ Note that participants should understand what withdrawal of consent will mean to the use of their previously collected information and that non-identifiable data cannot be retrieved and withdrawn from the database.

Ranked forms of consent and associated conditions

Type of consent	Specific forms of consent	Required conditions for REB consideration
(i) Opt-in consent (preferred)	<p>Ways of opting in:</p> <ol style="list-style-type: none"> 1. Written (preferred) 2. Oral 3. Conduct (e.g. returning a questionnaire) 	<p>All of the following:</p> <ul style="list-style-type: none"> • Voluntary. • Informed. • Unambiguous. • Obtained before beginning the research. • Consent can be withdrawn at any time, with a clear understanding of what that means, for example: <ul style="list-style-type: none"> – no further collection of additional data; – no further analyses using the already collected data; or, – removal of data from the database to the extent possible (Note: Non-identifiable data will be impossible to isolate and retrieve). • The process of consent to be documented by the researcher.
(ii) Presumed consent, with opt-out mechanism	<p>Consent is presumed unless the person opts out</p> <p>Ways of opting out:</p> <ol style="list-style-type: none"> 1. Written (preferred) 2. Oral 	<p>All of the following:</p> <ul style="list-style-type: none"> • Voluntary. • Informed (e.g. through notices, brochures, letters, media announcements): <ul style="list-style-type: none"> – of the research – of the opportunity to opt-out – of the means of opting out. • Accessible means for opting out. • Opt-out may be done at any time before or during the research, with a clear understanding of what opting out means, for example: <ul style="list-style-type: none"> – no further collection of additional data; or – no further analyses using the already collected data; or, – removal of data from the database to the extent possible (Note: Non-identifiable data will be impossible to isolate and retrieve). • The process of opting-out to be documented by the researcher.

4.2 Documenting consent

4.2.1 Written documentation signed by the research participant (preferred)

Whenever appropriate and practicable, a written documentation of opting-in or opting-out of research is preferred. This should be documented using a consent form or refusal statement signed by the individual.

4.2.2 Oral consent documented by the researcher

Where oral consent is obtained for telephone interviews, where written documentation is culturally unacceptable, or where there are good reasons for not recording opt-in or opt-out in writing using a form that the participant signs, an oral procedure should be managed and documented, indicating that the opt-in or opt-out was conducted orally.

4.2.3 Documented consent and collection of data without direct personal identifiers

Collection of data without direct personal identifiers may be necessary or proposed when the research deals with highly sensitive conditions or activities. In such circumstances, consent should be documented but the identity of research participants should not be linkable to their data or to results of analyses.

Example: Oral consent and non-identifiable data and results

Disease X prevalence study among women undergoing abortion in City Y. Before undergoing therapeutic abortions, women must necessarily have a blood test.

Women who were scheduled for therapeutic abortions were approached in a hospital clinic about their willingness to participate in the study on Disease X. Those who gave oral consent to participate in this study agreed to fill out questionnaires (without providing their names) about certain risk factors for disease X, and to permit the testing of leftover blood from the blood test for the presence of disease X.

For each participant, the computer generated a specific scrambled code linking the blood sample for the disease test and the answers to the questionnaire. Once the results of the disease tests were linked to the corresponding questionnaire, the computer-generated code was removed. In this way, it was not possible to identify the research participants, even if one had used the same computer program to try to retrace the scrambled codes.

The linked information for each person was thus non-identifiable so that the researchers could look at risk factors and determine the incidence of disease X but could not identify any of the research participants.

Example: Documented consent and non-identifiable data and results

From a study on workplace injuries in nursing and laboratory staff

...The study questionnaire had no name or code number on it and participants were asked not to write their name on it. The cover letter from the researcher asked participants to fill out the questionnaire, put it in the provided envelope and return it through internal [staff] mail. The letter also asked participants to then sign a response card that had their name on it, put it in a separate envelope that was also provided and deposit it into slotted drop boxes located in each work area.

The researcher did not need to know the names of persons who had responded; it was the content of the responses that was of interest. The only identifying information required was on the response card in order to allow the researcher to send targeted reminder letters to those persons who had still not responded. In addition, general reminders to return the questionnaires were also posted in designated work areas in an effort to increase response rates.

To minimize the risk of linking questionnaire responses with the names provided on the response cards, the researcher picked up the cards regularly throughout the week and the questionnaires only once every week or two. Furthermore, no data were entered until the end of data collection to reduce the possibility of identifying late respondents. With this method, the researcher could not identify who had filled out each questionnaire, but she would know from the response cards who on the list had or had not returned a questionnaire.

In this study sensitive information could be revealed about those staff who had suffered an injury at work but who had not reported it, contrary to mandatory hospital reporting policies. Some respondents may not have reported injuries because they did not want to appear careless; others may have wished to avoid the fairly lengthy follow-up procedures required of persons with certain injuries. The researchers had anticipated that this might be the case and understood that this information would be considered quite sensitive. It was for this reason that the survey was conducted with no ability to link the data collected to individuals' identities.

4.3 Qualitative research

Participants in qualitative studies are especially vulnerable to unintended identification. For example, in quoting interviewees, biographical details may be revealed that make protecting identities difficult. Deleting all possible identifiers may rob the quote of its impact and research value. Changing names and places is not a guarantee that individuals' identities will be concealed.

Therefore, paying attention to the trust relationship between researcher and participant, and obtaining ongoing consent, are very important in qualitative research. Constant sensitivity to

participants' behaviour and reactions during data collection is essential. Unsolicited and unanticipated disclosures of information by participants can easily fall outside the original consent agreement.

As the interaction between a researcher and participants progresses, there may be situations where the researcher will need to recognize that participants should be given the opportunity to reiterate their consent, to withdraw from the research, or to withdraw their particular comments.³⁹ Thus, obtaining informed consent should be an ongoing negotiation.

4.4 Documenting non-participation or withdrawal of consent

The researcher may need information on who does not want to participate in research or who withdraws from research, for example to:

- document who is not to be included in follow-up research activities; and/or
- take into consideration relevant characteristics of the population not included in the study, when reporting possible bias in research results.

In these circumstances, researchers may obtain information about non-participants or those withdrawing consent only with:

- individuals' consent or
- the approval of an REB to waive the consent requirement in the particular circumstances.⁴⁰

LINK TO TRI-COUNCIL POLICY STATEMENT:

[Voluntary consent: No manipulation, undue influence or coercion]

Article 2.2 "Free and informed consent must be voluntarily given, without manipulation, undue influence or coercion". Explanatory text: "...Undue influence may take the form of inducement, deprivation or the exercise of control, or authority over prospective subjects. Voluntariness is especially relevant in research involving restricted or dependent subjects, and is absent if consent is secured by the order of authorities or as a result of coercion or manipulation. ...REBS should also pay particular attention to the elements of trust and dependency, for example, within doctor/patient or professor/student relationships, because these can constitute undue influence

³⁹ See Element #5, 5.4.

⁴⁰ See Element #3.

on the patient to participate in research projects, especially those involving residents in long-term care facilities or psychiatric institutions...” (pg. 2.4)

Article 2.4 “... researchers or their qualified designated representatives shall provide prospective subjects with the following:.. (d) An assurance that prospective subjects are free not to participate, have the right to withdraw at any time without prejudice to pre-existing entitlements, and will be given continuing and meaningful opportunities for deciding whether to continue to participate..” Explanatory text: “..Articles 2.2 and 2.4(d) help to ensure that a prospective subject’s choice to participate is voluntary. Pre-existing entitlement to care, education and other services shall not be prejudiced by the decision on whether to participate. Accordingly, a physician should ensure that continued clinical care is not linked to research participation, and teachers should not recruit prospective subjects from their classes, or students under their supervision, without REB approval. Nothing in this Section should be interpreted as meaning that normal classroom assessments of course work require REB approval...” (pg. 2.6)

[Evidence of consent]

Article 2.1 “...(b) Evidence of free and informed consent by the subject or authorized third party should ordinarily be obtained in writing. Where written consent is culturally unacceptable, or where there are good reasons for not recording consent in writing, the procedures used to seek free and informed consent shall be documented...” Explanatory text: “Free and informed consent... encompasses a process that begins with the initial contact and carries through to the end of the involvement of research subjects in the project. As used in this Policy, the process of free and informed consent refers to the dialogue, information sharing and general process through which prospective subjects choose to participate in research that involves themselves. ” (pg. 2.1)

[Written and oral documentation]

Article 2.1 Explanatory text: “Article 2.1 (b) states the preference for written evidence of free and informed consent. The article acknowledges that written consent is not always appropriate. For most people in our society, a signed statement is the normal evidence of consent. However, for some groups or individuals, a verbal agreement, perhaps with a handshake, is evidence of trust, and a request for a signature may imply distrust. Nonetheless, in most cases a written statement of the information conveyed in the consent process, signed or not, should be left with the subject. In some types of research, oral consent may be preferable. In others, written consent is mandatory. Where oral consent is appropriate, the researcher may wish to make a contemporaneous journal entry of the event and circumstances. These and like elements may

sometimes need to be refined in concert with the REB, which plays an essential education and consultative role in the process of seeking free and informed consent. When in doubt about an issue involving free and informed consent, researchers should consult their REB.” (pg. 2.2)

[Witness of signatures]

Article 2.4 Explanatory Text: “In some circumstances, having a witness to the signatures on the consent form may be felt to be appropriate. In law, the role of a witness is only to attest that the person actually signed the form; a witness is not responsible for certifying such factors as the signature being obtained under defined conditions or that the signers were competent. However, a court might subsequently seek the opinions of the witness on such issues”. (pg. 2.8)

[Time allocation]

Article 2.4 Explanatory Text: “Rushing the process of free and informed consent or treating it as a perfunctory routine violates the principles of respect for persons, and may cause difficulty for potential subjects. The time required for the process of free and informed consent can be expected to depend on such factors as the magnitude and probability of harms, the setting where the information is given (e.g. hospital or home) and the subject’s situation (e.g., level of anxiety, maturity or seriousness of disease).” (pg. 2.8)

[Translating materials]

Article 2.1 Explanatory text: “The requirement for free and informed consent should not disqualify research subjects who are not proficient in the language used by the researchers from the opportunity to participate in potential research. Such individuals may give consent provided that one or more of the following are observed to the extent deemed necessary by the REB, in the context of a proportionate approach to the harms envisaged in the research and the consent processes that are to be used: An intermediary not involved in the research study, who is competent in the language used by the researchers as well as that chosen by the research subject, is involved in the consent process; The intermediary has translated the consent document or approved an existing translation of the information relevant to the prospective subject; The intermediary has assisted the research subject in the discussion of the research study; The research subject has acknowledged, in his or her own language, that he or she understands the research study, and the nature and extent of his or her participation, including the risks involved, and freely gives consent. . . .”

ELEMENT #5: Informing prospective research participants about the research

General statement

Researchers should provide to prospective participants or to authorized third parties disclosure of all information relevant to voluntary and informed consent.

As part of the consent process, the researcher or other appropriate person (depending on the approved recruitment procedure) should explain such things as the nature of the research, what information will be collected and how it will be used in this study and possible future studies, as well as the risks and benefits of the research, so that they can make an informed decision about whether they wish to participate.

Researchers must ensure that prospective participants are given adequate opportunities to ask questions, discuss their concerns and consider their participation.⁴¹

5.1 Understandable language

Information should be communicated to prospective participants in plain language, in oral and/or written form, so that it is easily understood.⁴²

5.2 Reasonable time allocation

The amount of time taken to communicate information to prospective participants should be appropriate to the need, and should be neither excessive nor too brief. For example, the information could be layered, so that participants are given a one-page summary, a short consent form with headings corresponding to core elements (e.g. requirements of participation, right to refuse and withdraw), and more detailed information in an appendix. Participants should also be informed about how to obtain more details if desired (e.g. via a web site or a toll-free telephone number).

⁴¹ See table of concordance for Element #5 in Appendix A-7 for cross-reference to statutory provisions regarding notice/information requirements.

⁴² According to the results of the international *Adult Literacy and Life Skills Survey* (2003), a joint project of the Government of Canada, the U.S. National Center for Education Statistics and the Organization for Economic Cooperation and Development, some 15% of Canadians, about one out of every seven, have problems dealing with printed materials and score at the lowest performance level in reading prose. From Statistics Canada, *The Daily*, Wednesday, May 11, 2005, reporting on *Learning a Living: First Results of the Adult Literacy and Life Skills Survey*, 2003 (89-603-XWE, free), available online at: <http://www.statcan.ca/english/freepub/89-603-XIE/89-603-XIE2005001.htm>

5.3 Communicating results back to research participants

5.3.1 Informing research participants about results specifically relating to themselves

During the consent process, the researcher should determine whether the participant wishes to be informed of any meaningful research results that specifically relate to them.⁴³ Also, there should be agreement on how any results relating to the participant will be communicated to the participant (e.g. whether the information will be provided first to a genetic counsellor or a health care provider).

5.3.2 Informing populations of general results and potential negative impacts

The results of research should be made public to contribute towards better understanding of the health issue under investigation. Researchers, particularly those in the areas of health services, population and public health, and genetics or genomic research, who study whole populations, should strive to communicate with the relevant population and governmental authorities regarding results that are pertinent to the improvement of health and/or the prevention of disease. Where appropriate, researchers, in collaboration with the population concerned, should facilitate the development and the implementation of a follow-up plan in response to the research findings.⁴⁴

The population studied should be made aware of possible socio-economic discrimination or group stigmatization as a result of the research results, for example, due to perceptions of genetic risks. In the context of genetic research, the population should also be informed of the means taken to minimize the risks. To avoid misleading or unrealistic expectations, the researchers should make known the limitations of the research results and of their practical or potential application.⁴⁵

5.4 Qualitative research

Researchers using qualitative methods may consider involving participants in the writing and reporting process, depending on the circumstances. For example, during the process of informing prospective research participants about the research, it may be appropriate:

- to provide participants with the opportunity to look at transcripts and to delete or footnote what they consider to be inaccurate or sensitive information (known as member-checking);

⁴³ When results of research tests are determined to be scientifically valid, have significant implications for the health of the participant, and prevention or treatment is available, these results should be communicated to the participant through his or her treating physician, unless the participant has chosen not to receive any results. In communicating results to the participant, particularly with respect to genetic research, the choices of each participant, the extent of available clinical services, the availability of counselling, and the implications for family members, should be taken into account (based on Quebec's Network of Applied Genetic Medicine (RMGA) *Statement of Principles: Human Genome Research* Version 2000, part IV *Professionalism*, part 3 *Communication of Specific Results*, pg. 12).

⁴⁴ Based on Quebec Network of Applied Genetic Medicine (RMGA) *Statement of Principles on the Ethical Conduct of Human Genetic Research Involving Populations* (2002), Section 6, *Communication of Research Results*, pg. 3.

⁴⁵ As above.

- to ask participants if they wish to be publicly acknowledged in articles coming from the research; or
- to invite community leaders or representatives to help interpret the findings to their constituencies.

5.5 Providing information about privacy to prospective research participants

The following categories of information relating to privacy matters should be included in the information provided to prospective research participants:

Basic information	Explanation
1) Research objectives ⁴⁶ and procedure	<ul style="list-style-type: none"> • Specific research objectives and related questions.
2) Data types and uses ⁴⁷	<ul style="list-style-type: none"> • Types of data to be collected and why. • Any planned or foreseeable commercial uses of the data. • If appropriate, a statement indicating whether test results are for research purposes only or if they can serve other non-research purposes (e.g. clinical care).
3) Voluntary basis for to participation ⁴⁸	<ul style="list-style-type: none"> • Voluntary basis for participation, and ongoing meaningful opportunities decide whether to continue. • Withdrawal, without any negative effect on a person's reasonable expectations of rights and benefits, being possible at any time (but be clear that data which have already been made non-identifiable cannot be retrieved and destroyed). • Option of contacting other family members to ask their willingness to be contacted by the researcher (e.g. in genetic research, participants should make first contact with related family members). • Circumstances under which the researcher may terminate the participant's involvement in the research (e.g. in clinical drug trials).
4) Risks, benefits, compensation	<ul style="list-style-type: none"> • Possible risks or discomforts to the research participant (including physical, emotional and psychological impacts, or privacy intrusion).

⁴⁶ See also Element #1.

⁴⁷ See also Element #2. We recognize that certain types of research may not be compatible with full disclosure of data to be collected, for example in some psychology research. This is an area that requires further reflection, and CIHR welcomes suggestions from those for whom these exceptions may apply.

⁴⁸ See also Element #4.

	<ul style="list-style-type: none"> • Benefits of the research in general and, if relevant, the benefits to the individual participant. • Any compensation offered to participants should not constitute an undue influence to agree to participate.⁴⁹
5) Confidentiality and safeguards ⁵⁰	<ul style="list-style-type: none"> • Protection of data confidentiality (e.g. affirmation that genetic data will not be given to third parties) • General description of security measures (e.g. coding of data,⁵¹ locked storage).
6) Data access and legal disclosure requirements ⁵²	<ul style="list-style-type: none"> • Who will have access to the data and for what purposes (include any legal requirements, such as mandatory public health reporting of certain diseases or obligation to produce evidence on court order; access required for scientific integrity such as auditing or verification of data; and any plans to archive or destroy the data).
7) Reporting of results ⁵³	<ul style="list-style-type: none"> • Explanation of the conditions, if any, under which personal results are to be reported back (e.g. results of genetic testing should normally be reported back to the participant through a physician and with provision of genetic counseling; conditions for informing implicated family members of research results should be clearly stated). • A clear statement, if relevant, of conditions under which results will not be given to the participant (e.g. exploratory research for which results are not clinically meaningful or community-based research where results are applicable only to the community). • Explanation of the impossibility for researchers to trace results from non-identifiable data back to individuals.
8) Data retention ⁵⁴	<ul style="list-style-type: none"> • Time period that data will be retained (e.g. provide a specified time period or, if for an extended/indefinite period, provide a specified time for REB review).
9) Inquiries and complaints ⁵⁵	<ul style="list-style-type: none"> • Who is available to answer questions about the research. • Who to contact about the ethics of the research. • Who to complain to about the research. • Who to contact if the participant decides to withdraw consent.

⁴⁹ TCPS states that “ undue influence may take the form of inducement, deprivation or the exercise of control or authority over prospective subjects.” (TCPS Article 2.2, pg. 2.4)

⁵⁰ See also Element #7.

⁵¹ See Element #2, 2.3.2 and Box- Definition of terms.

⁵² See also Element #8.

⁵³ See also Element #8.

⁵⁴ See also Element #9.

⁵⁵ See also Element #10.

5.6 Collection from individuals and secondary use (Hybrid model)

For a hybrid project involving the direct collection of data from individuals and secondary use of data from other sources, the prospective research participant should also be informed of:

- all expected types and sources of personal data to be accessed and used;
- any expected linkages; and
- the expected purposes for which data will be used (e.g. health survey data to be collected and linked, with consent, to health records to investigate health care use in the population).

5.7 Creation of a database for general research purposes

5.7.1 Information to be provided at time of collection

When personal data are to be entered into a database for multiple research uses over an extended period, research participants should also be informed, at the time of collection, of the following:

Basic information	Explanation
1) Expected types of studies	<ul style="list-style-type: none"> • The type of studies that might be conducted, with possible examples (e.g. research on cardio-vascular disease).
2) Expected data types and purposes	<ul style="list-style-type: none"> • The types of data to be collected from all sources including data linkages, and for what research purposes.
3) Expected commercial uses	<ul style="list-style-type: none"> • Any anticipated commercial uses.
4) Data retention period	<ul style="list-style-type: none"> • For how long the data will be retained (if for an extended/indefinite period, provide a specified time for REB review).
5) The process for overseeing the use and security of data	<ul style="list-style-type: none"> • The process being implemented to ensure proper data stewardship and data security, including: <ul style="list-style-type: none"> – the main rules governing future uses of the database; – the process by which requests for data access will be reviewed and monitored; and – the organization or persons to whom the researcher is accountable for the proper management of the data.

<p>6) Authorization for future uses, with or without re-contact</p>	<ul style="list-style-type: none"> • Options for the participant to control future uses of personal data in the database. These options should include the opportunity to withdraw consent (and any identifying information) in the future, and may also include the options: <ul style="list-style-type: none"> – To be re-contacted on a regular (or as needed basis) to seek consent for new research uses of the data, if desired and practicable; and/or – To not be re-contacted, but to authorize the researchers to use the data only in certain ways in the future, for example: <ul style="list-style-type: none"> ◦ only for certain research purposes (to be determined with the participant during the consent process); ◦ only for the original broad purposes for establishing the database; ◦ for any purposes as long as a research ethics board has approved the proposed research; ◦ at what level of identifiability (e.g. with or without direct identifiers, coded, or in non-identifiable form):⁵⁶ and ◦ with or without linkages to other data sources (e.g. with controls over what can be linked, and who can access the linked data).
---	---

Example: Informing participants and presenting options for control of new uses of data

The invitation to participate in the study is made by a dedicated nurse coordinator employed by, and accountable to, the participating hospital. The nurse coordinator arranges, at a convenient time for the patient (and his/her family), to explain the study and seek the patient's consent to participate. Patients can refuse or can agree to any or all of the following:

- Access to their current hospitalization records by the nurse coordinator to collect information relevant to their condition, for future research uses.
- A follow-up telephone call by the nurse coordinator 6 months after the onset of their health event to determine longer-term changes in their functional ability—this survey information is also intended for inclusion in the registry for future research purposes.
- Linkage of their data in the study database, with administrative files from the provincial Ministry of Health, and other sources such as laboratory and physician records, in order to collect information about physician and laboratory services, subsequent hospitalizations,

⁵⁶ See Box – *Definition of terms: Individual Identifiability of Data*, in Element #2.

and causes of death. The linked data will be used for research on the use of health care services and effects on health for patients with condition X; and

- Use of their non-identifiable records in future analyses performed at the independent not-for-profit research organization based in City Y. The results of these analyses are to be released in aggregate form to third-party private companies seeking to improve services and products related to condition X.

5.7.2 Promotion of openness and accountability⁵⁷

Researchers should endeavour to keep participants informed of future data uses through continuing means (e.g. web site information), as part of an ongoing commitment to openness and to the maintenance of informed consent.

LINK TO TRI-COUNCIL POLICY STATEMENT:

[Information to be provided to research participants]

Article 2.4 "Researchers shall provide, to prospective subjects or authorized third parties, full and frank disclosure of all information relevant to free and informed consent. Throughout the process of free and informed consent, the researchers must ensure that prospective subjects are given adequate opportunities to discuss and contemplate their participation. Subject to the exception in Article 2.1 (c), at the commencement of the process of free and informed consent, researchers or their qualified designated representatives shall provide prospective subjects with the following:

(a) Information that the individual is being invited to participate in a research project;

(b) A comprehensible statement of the research purpose, the identity of the researcher, the expected duration and nature of participation, and a description of research procedures;

(c) A comprehensive description of reasonably foreseeable harms and benefits that may arise from research participation, as well as the likely consequences of non-action, particularly in research related to treatment, or where invasive methodologies are involved, or where there is a potential for physical or psychological harm;

⁵⁷ See Element #10, 10.2.1

(d) An assurance that prospective subjects are free not to participate, have the right to withdraw at any time without prejudice to pre-existing entitlements, and will be given continuing and meaningful opportunities for deciding whether to continue to participate; and

(e) The possibility of commercialization of research findings, and the presence of any apparent or actual or potential conflict of interest on the part of researchers, their institutions or sponsors.” (pg. 2.5, 2.6)

“..REBs may require researchers to provide prospective subjects with additional information, such as that detailed in Table 1...” (pg. 2.6)

“Table 1: Additional Information that may be required for some projects

- 1. An assurance that new information will be provided to the subjects in a timely manner whenever such information is relevant to a subject's decision to continue or withdraw from participation;*
- 2. The identity of the qualified designated representative who can explain scientific or scholarly aspects of the research;*
- 3. Information on the appropriate resources outside the research team to contact regarding possible ethical issues in the research;*
- 4. An indication of who will have access to information collected on the identity of subjects, description of how confidentiality will be protected, and anticipated uses of data;*
- 5. An explanation of the subject's responsibilities;*
- 6. Information on the circumstances under which the researcher may terminate the subject's participation in the research;*
- 7. Information on any costs, payments, reimbursement for expenses or compensation for injury;*
- 8. In the case of randomized trials, the probability of assignment to each option;*
- 9. For research on biomedical procedures, including health care interventions: information about (a) forgoing alternative procedures that might be advantageous to the subject; (b) which aspects of the research involve the use of procedures that are not generally recognized or accepted; and (c) particularly in trials of therapeutic interventions, the care provided if the potential subject decides not to consent to participation in the study;*
- 10. The ways in which the research results will be published, and how the subjects will be informed of the results of the research.” (pg. 2.7)*

[Genetic counseling]

Article 8.4 “Genetics researchers and the REB shall ensure that the research protocol makes provision for access to genetic counseling for the subjects, where appropriate.” Explanatory note: “Genetic counselors who are formally trained to impart genetic information have two main roles in dealing with a family: The first is to educate regarding the condition in question, and the second is to counsel by presenting options or possible action scenarios in a non-directive manner. The complexity of genetic information along with its social implications usually requires that free and informed consent be supplemented with genetic counseling.” (pg. 8.4)

[Conditions for less than full disclosure]

Article 2.1 Explanatory text: “... the REB should exercise judgment on whether the needs for research justify limited and/or temporary exception to the general requirements for full disclosure of information relevant for a research subject’s meaningful exercise of free and informed consent. In such cases, subjects may be given only partial information or they may be temporarily led to believe that the research has some other purpose because full disclosure would likely colour the responses of the subjects and thus invalidate the research. For example, social science research that critically probes the inner workings of publicly accountable institutions might never be conducted without limited recourse to partial disclosure. Also some research in psychology seeks to learn about human responses to situations that have been created experimentally. Such research can only be carried out if the subjects do not know in advance about the true purpose of the research...Another scenario, in questionnaire research, embeds questions that are central to the researcher’s hypotheses within distractor questions, decreasing the likelihood that subjects will adapt their responses to their perceptions of the true objective of the research. For such techniques to fall within the exception to the general requirements of full disclosure for free and informed consent, the research must meet the requirements of Article 2.1 (c)...” (pg. 2.2- 2.3)

[Secondary uses]

Article 3.2 Explanatory text: “It is essential that subsequent uses of data be specified in sufficient detail that prospective subjects may give free and informed consent; it is inappropriate to seek blanket permission for “research in general”. (pg. 3.4)

ELEMENT #6: Recruiting prospective research participants

General statement

To recruit research participants, the researcher will typically need to complete the following steps, each of which involves the researcher or another more appropriate person having access to personal information:

Step A: Assess eligibility criteria for the research and assemble a list of eligible individuals.

Step B: Establish initial contact with eligible individuals.

Step C: Inform eligible individuals about the research, as part of the informed consent process.

The proposed recruitment procedure and materials should be included in the submission for REB approval.

The procedure and materials should foster conditions for voluntary consent, and not exert undue influence on prospective participants to agree to take part in the research.⁵⁸

Initial contact with individuals about a research project should be made by someone that individuals would expect to have relevant information about them, or in other ways that do not inappropriately intrude on their life or privacy.

If permitted by law⁵⁹ and subject to REB approval, the data holder who would normally have access to the required personal information is the preferred person to access that information to assess eligibility of individuals for the research (Step A) and to make initial contact with those individuals (Step B), unless the REB considers this approach to be impracticable or inappropriate.

Typical scenarios for recruiting participants and preferred approaches are described under 6.3.

⁵⁸ See also Element #4 regarding managing and documenting the consent process.

⁵⁹ See the legal concordance table for Element #6 in Appendix A-7.

6.1 Consent and secondary use of personal information to assess eligibility and contact individuals

The REB will need to determine if consent from individuals is required for the secondary use of their personal information for assembling a list of eligible individuals for research or contacting these individuals to seek their consent for participation.⁶⁰ Researchers and REBs should be aware of any legal restrictions on contacting individuals in these circumstances.⁶¹

6.1.1 Anticipating future uses of personal information at the time of the original collection

Wherever possible at the time of the original collection of personal information from individuals, the researcher and/or data custodian should anticipate the future uses of this information to assemble eligibility lists for research or to contact eligible individuals, and should seek consent for these future uses at that time.

For example, patients could be asked at the time of the original collection of their personal information whether they consent to the health care provider reviewing their records and contacting them to inform them of research for which they are eligible. If such a prior opt-in consent procedure is not a practicable option, a health care provider could inform patients through notices that their personal information may be reviewed from time to time for recruitment purposes, and that they have the opportunity to opt-out. If patients do not opt-out, their consent for the use of their personal information to assess their eligibility for research or to contact them about the research project would be presumed.

6.2 Initial contacting and informing prospective participants

6.2.1 Trust vs. undue influence

Recruitment raises complex issues around who is the appropriate person to make initial contact and inform eligible individuals about the research. On the one hand, individuals may feel more comfortable if approached by a data holder, such as a clinic physician or nurse, whom they trust and accept as having access to their personal information. On the other hand, individuals may be unduly influenced to agree to participate in research if approached by someone on whom they are dependent, for example, their employer, health provider, community leader or program director.

In some cases, someone who has a relationship of some influence over prospective research participants may be the preferred person to contact individuals and inform them of the research

⁶⁰ See Element #3 regarding determining if consent is required.

⁶¹ See the legal concordance table for Element #6 in Appendix A-7.

where this is considered the best way to ensure that prospective research participants fully understand the risks and the benefits of the research to themselves. For example, a health care provider or professional (who may or may not be involved in the research) may be the preferred person to contact individuals and inform them about the research because of a relationship of medical confidence, special expertise and/or in-depth knowledge of the patients' situations. It is critical in such cases that the participants are reassured that their reasonable expectations of care will be met whether or not they take part in the research.⁶²

6.2.2 Prior communication

Researchers should avoid situations where eligible individuals are not aware, prior to being contacted, of information about themselves that makes them eligible for participation in the research. For example, a health care provider may not yet have informed the patient of a diagnosis (e.g. cancer) that is in the patient health record and that is used to determine eligibility. The researcher should confirm with the data holder that individuals have been informed of relevant health-related information before initiating contact.

6.3 Selected scenarios and preferred recruitment practices

Index to recruitment scenarios

6.3.1 Scenario: ■ Eligible research participants are in a city telephone directory.

6.3.2 Scenario: ■ A research team proposes to recruit research participants from members of an Aboriginal community.

6.3.3 Scenario: ■ A genetics researcher proposes to recruit the family members of research participants.

6.3.4 Scenarios: ■ The researcher has access to personal data from prior research studies. ■ The research unit of a hospital is proposing to conduct research on patients. ■ The researcher is the health care provider of eligible individuals.

6.3.5 Scenario: ■ The researcher is external to the data-holding organization, and is submitting a proposal to conduct research on patients, employees or students of the organization.

6.3.6 Scenario: ■ A clinician-researcher at a health care facility wants to conduct research on patients being treated by another physician in the same facility. ■ An academic wants to conduct research on students in his or her university department or program, but not in a class that he or she is currently teaching.

⁶² See also TCPS Article 4.1 and Section 4-A *Conflicts of Interest Involving Researchers* (pg. 4.1); TCPS Section 7-*Clinical Trials*; and TCPS Articles 7.1, 7.2 and explanatory text regarding recruitment and informed consent (pg. 7.2).

6.3.1 Scenario: ■ Eligible research participants are in a city telephone directory.

When eligibility information and the means of notifying individuals about the research are publicly available, the researcher should normally be able to make the initial contact without needing an intermediary.

6.3.2 Scenario: ■ A research team proposes to recruit research participants from members of an Aboriginal community.

As a general rule, researchers planning to work in a community should make contact with and inform community leaders and groups relevant to their research, prior to initiating the recruitment or informed consent process with members of that community.

For many Aboriginal communities and groups, approval by local authorities may be required prior to beginning the recruitment of research participants.⁶³

6.3.3 Scenario: ■ A genetics researcher proposes to recruit the family members of research participants.

For the purpose of recruiting relatives for genetic or genomic research, there should be no direct contact between the researcher and the family members of the initial research participant. In order to respect the privacy of the participant and his family, only the participant or his/her spouse or a designated family member should contact other family members to ask their willingness to be approached by the researcher. The principal researcher (or a member of the research team) should not directly contact the family.⁶⁴

6.3.4 Scenarios: ■ The researcher has access to personal data from prior research studies. ■ The research unit of a hospital is proposing to conduct research on patients. ■ The researcher is the health care provider of eligible individuals.

In these scenarios, the researcher is the data holder or is employed by the data holder. If permitted by law⁶⁵ and subject to REB approval, the data holder may assess the eligibility of individuals for the research.

⁶³ TCPS Section 6 (*Research Involving Aboriginal Peoples*) is currently under review, coordinated by the Interagency Advisory Panel on Research Ethics and including CIHR Aboriginal health research guidelines (in development). See also the articulation of First Nations' principles: *Ownership, Control, Access and Possession (OCAP) or Self-determination Applied to Research*, online at: <http://www.research.utoronto.ca/OCAP%20principles.pdf>.

⁶⁴ Based on Quebec Network of Applied Genetic Medicine (RMGA) *Statement of Principles: Human Genome Research* Version 2000-Section 3 (pg. 7).

⁶⁵ Where this access would be a secondary use of data, see 6.1. The data holder's access to data for recruitment purposes must be in accordance with applicable legislation. See the legal concordance table for Element #6, Appendix A-7.

The data holder should have rules nevertheless to limit the number of people permitted access to data for this purpose.⁶⁶

Preferred options for **contacting** individuals will depend on whether the REB considers that the researcher/data holder has undue influence over prospective research participants (see the Options table).

Options for contacting individuals according to whether the researcher/data holder has influence over prospective research participants

Option	Contacting prospective research participants
A) If the researcher/data holder is not in a position of undue influence.	If the researcher/data holder is not in a position of undue influence over prospective participants with regard to the research, the researcher should make the initial contact and inform prospective participants about the research, if permitted by law and subject to REB approval.
B) If the researcher/data holder is in a position of undue influence.	<p>In some cases, the researcher/data holder is considered to potentially be in a position of undue influence over eligible individuals with regard to the research or there is a potential conflict of interest. For example, an REB may decide that patients who will be recruited for a clinical trial being conducted by their health care provider may not understand the difference between the research treatment and the standard treatment provided at the health centre.</p> <p>In such cases, initial contact with prospective research participants should be made by neutral means, so that there is no undue influence exerted on individuals to participate. For example, a neutral person on the research team or in the data holder's agency who is not in a position of authority over prospective research participants, could contact eligible individuals. Alternatively, it may be possible to make initial contact with eligible individuals by advertising in newspapers or in public locations, and then having a neutral member of the research team or staff provide further information to interested individuals.</p>

⁶⁶ See also Element #8.

6.3.5 Scenario: ■ The researcher is external to the data-holding organization, and is submitting a proposal to conduct research on patients, employees or students of the organization.

In this scenario, the researcher is not the data holder, and does not have undue influence over prospective research participants. If permitted by law,⁶⁷ the preferred recruitment approach is for the data holder to assess eligibility for research and to make initial contact with eligible individuals, unless the REB considers that the preferred approach is impracticable or inappropriate (see the ranked Options table).

Ranked options for assessing eligibility and contacting prospective participants, when the researcher is not the data holder and does not have undue influence

Option	Assessing eligibility and contacting prospective research participants
<p>A) The data holder assesses eligibility and makes initial contact. (Preferred)</p>	<p>If permitted by law and subject to REB approval, the data holder should determine eligibility of individuals for the research on the basis of criteria provided by the researcher. The data holder should make the initial contact to: (i) inform eligible individuals about the research so that they can contact the researcher, if interested, or (ii) to seek consent from individuals to release their nominal information to the researcher who will contact them to inform them about the research.</p>
<p>B) If the REB considers option A impracticable or inappropriate, the REB may permit the researcher to access minimal personal information for assessing eligibility and/or making contact with eligible individuals, if permitted by law and under strict controls (e.g.</p>	<p>In some cases, the preferred option above may be considered impracticable or inappropriate. For example, the preferred option may be impracticable if:</p> <ul style="list-style-type: none"> • the data holder does not, despite funding from the researcher, have the resources to assess eligibility and make initial contact, and therefore the research could not proceed unless an alternative recruitment procedure is used; or • the data holder does not have an ongoing relationship with eligible individuals to make contact (e.g. as may the case for a registrar of a population records database, or a government agency holding health insurance registration and billing information). <p>The preferred option may be considered inappropriate where the data holder has undue influence over eligible individuals; professional or</p>

⁶⁷ See the legal concordance table for Element #6, Appendix A-7.

<p>access restricted to data holder's site).</p>	<p>other legal requirements makes the data custodian's involvement in the recruitment process inappropriate; or the data holder's contacting of eligible individuals would defeat the purpose of the research.⁶⁸</p> <p>When the preferred option is impracticable or inappropriate, an REB may consider whether a researcher should be permitted access to minimal personal data only for the purposes of determining eligibility for the research or contacting individuals to invite them to join the study⁶⁹. If it is legally permissible and the REB gives approval, the researcher may be given access to personal information with appropriate confidentiality protections such as a signed confidentiality agreement with access restricted to the data holder's site, and use limited to the stated purpose.</p> <p>Minimal personal data provided to the researcher should normally contain only contact information and no other personal information related to health status. However, if health-related data are inherent in the eligibility criteria used to assemble the list of individuals to be contacted, an REB may determine that camouflage sampling or other masking techniques should be used to enable researchers to contact individuals while preventing researchers from viewing any identifiable health-related information of eligible individuals prior to gaining consent.⁷⁰</p>
--	---

Option A: Examples of recruitment methods:

Health professional society makes contact with members

Prospective research participants are members of a health professional society. The Society mails out a letter (drafted by the researcher) to its members, which explains how to contact the researcher to learn more about the research.

Health professionals assess eligibility and make contact

Given the criteria provided by the researchers, pharmacists are automatically notified by a computer flag in a centralized database, at the time of filling a prescription, of any patient eligible

⁶⁸ For example, see Case Study #10 in CIHR's *Secondary Use of Personal Information in Health Research: Case Studies*, November 2002 in which initial contact by physicians of "hard-to-reach" patients would have confounded the results of the study which was investigating effective strategies for contacting patients. Also, because this study involved contacting patients about visiting their physicians for cancer screening services, physicians' involvement in the research was limited by a policy that existed at that time which prevented them from soliciting patients to come in for services.

⁶⁹ The REB should weigh the benefits of the research and the potential for a perceived invasion of privacy and any legal prohibitions against researchers' contacting individuals. See Element #3, 3.3.2 (b). See also the legal concordance table for Element #6, in Appendix A-7.

⁷⁰ See references to *Camouflage* techniques in the following: Element #7, 7.2.2 4th bullet; and the Glossary, Appendix A-6.

for the research study (e.g. receiving a certain number of concurrent medications). This automatic flag of eligible individuals for the study is visible only to pharmacists in participating pharmacies. Once the eligible persons are identified, the pharmacists seek consent from these individuals to release their contact information to the researcher.

Option B: Examples of recruitment methods

Researcher assesses eligibility and makes initial contact for data holder

Hospital administrators do not have the personnel necessary to search through files in order to identify potentially eligible research participants according to selection criteria provided by the researcher, or to establish prior contact with these individuals on behalf of the researcher. Therefore, with the approval of the REB and a signed undertaking of confidentiality by the researcher, hospital administrators provide the researcher with the names of staff, their work location and full or part-time status, in the form of a computer file. The researcher then uses the computer file to exclude staff that do not fit the eligibility criteria and to select a random sample of eligible staff. Senior hospital staff explain the study in general terms to their staff members and inform them that the researcher will be writing in the near future to individuals eligible to be included in the study. Senior staff emphasize that participation is on a purely voluntary basis. Accordingly, the researcher sends letters of invitation to participate in the research only to eligible staff members.

Data holder assesses eligibility and provides camouflaged list to researcher to make initial contact

The study is approved by the REB and the privacy branch of the Ministry of Health. Ministry of Health staff produces a “camouflaged” list of patient names for the researchers, containing scrambled personal health numbers of patients potentially affected by a new health care policy with scrambled numbers of a random sample of patients who are not affected by the policy. When the scrambled numbers are unscrambled and converted to names, addresses and telephone numbers by the Ministry of Health’s Client Registry, the health status of each patient remains unknown to the researchers and to the Ministry of Health staff. The addition of persons not affected by the health condition prevents the researchers from knowing who is affected and who is not; only those who respond are identified. In order to be most effective, camouflaging should aim to protect the privacy of targeted patients, while limiting the total number of patients who need to be contacted.

6.3.6 Scenario: ■ A clinician/researcher at a health care facility wants to conduct research on patients being treated by another physician in the same facility. ■ An academic wants to conduct research on students in his or her university department or program, but not in a class that he or she is currently teaching.

In these scenarios, the researcher is not the data holder, but does potentially have undue influence over prospective participants with regard to the research.

Preferred approaches to assessing eligibility for research and contacting eligible individuals will depend on whether the REB considers the data holder to have undue influence over prospective research participants (see the Options table).

Options for assessing eligibility and making contact with individuals when the researcher has undue influence over prospective individuals

Option	Assessing eligibility and contacting individuals
A) If the data holder is not in a position of undue influence.	If the data holder is not in a position of undue influence over prospective research participants, the REB may permit the data holder to assess eligibility and make the initial contact with these individuals, if the data holder is permitted to do so by law (see scenario 6.3.5, option A).
B) If the data holder is in a position of undue influence.	If the data holder is considered by an REB to have undue influence on prospective participants, the researcher could make initial contact with eligible individuals by neutral means such as by putting up notices in public areas of the facility or institution with information on how to contact the research team, and a neutral member of the research team or staff could inform interested individuals about the research (see scenario 6.3.4, option B).

LINK TO TRI-COUNCIL POLICY STATEMENT:

[Secondary use of data for prospective collection]

Article 3.5 “Researchers who wish to contact individuals to whom data refer shall seek the authorization of the REB prior to contact.” Explanatory text: “In certain cases, the research goal may only be achieved by follow-up contact and interviews with persons. It is evident that individuals or groups might be sensitive if they discover that research was conducted on their data without their knowledge; others may not want any further contact. This potential harm underlines the importance for researchers to make all efforts to allow subjects the right to consent that their data and private information be part of a study.” (pg. 3.6)

ELEMENT #7: Safeguarding personal data

General statement

Institutions or organizations where research data are held have a responsibility to establish appropriate institutional security safeguards. Data security safeguards should include organizational, technological and physical measures.⁷¹

Researchers should take a risk assessment and management approach to protecting research data from loss, corruption, theft or unauthorized disclosure, as appropriate for the sensitivity and identifiability of the data. Formal privacy impact assessments (PIAs) are required in some institutions and under legislation or policy in some jurisdictions.⁷²

REBs should review and approve researchers' proposed measures for safeguarding any personal data to be collected.

The safeguards described in this Element are particularly relevant to research conducted within large institutions or other organizations. However, smaller scale projects should also demonstrate acceptable ways of protecting the confidentiality of data.

7.1 Threat-risk vulnerability assessment⁷³

A vulnerability assessment assists researchers and institutions in determining an appropriate level of security for research data and the means by which the data should be received, used, stored, and managed. The following are the main steps in a vulnerability assessment:

Assessment	Examples
a) Determine what assets need to be protected	<ul style="list-style-type: none">• Databases and files of personal and other confidential data• Database management software• Computer hardware, fax machines
b) Determine what to protect against	<ul style="list-style-type: none">• Five main classes of threats are: disclosure, interruption, modification, destruction and removal or loss

⁷¹ See the table of concordance for Element #7, Part 1, in Appendix A-7, for statutory references to general safeguarding obligations.

⁷² See the legal concordance table for Element #7, Part 2, in Appendix A-7.

⁷³ Adapted from RCMP *Security Information Publication 5, Guide to Threat and Risk Assessment for Information Technology*, November 1994. Online at: http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/g2-001_e.pdf.

Assessment	Examples
c) Assess the probability of the threat occurring	<ul style="list-style-type: none"> • Low, medium or high
d) Assess the magnitude of the impact and consequences of the threat if it occurs	<ul style="list-style-type: none"> • Loss of public trust • Harms to individuals (loss of privacy or trust; social stigmatization; social discrimination affecting financial, employment, insurance, or other status; loss of benefits) • Loss of data or equipment.
e) Assess existing safeguards and need for additional safeguards	<ul style="list-style-type: none"> • Direct identifiers are separated from personal records as soon as reasonably practicable • Highly identifiable and sensitive data are stored at the highest level of security, e.g. on stand-alone servers. • Pledge of confidentiality signed by all research staff.
f) Recommend the appropriate security safeguards to protect the assets from threats	<ul style="list-style-type: none"> • See security measures proposed in 7.2 below
g) Update and regularly review these safeguards (at least annually)	<ul style="list-style-type: none"> • Respond to changes in: <ul style="list-style-type: none"> – the internal technological environment (including improvements in security strategies), – the research project and the institution, – technologies available to threat agents and – the profile of potential threats.

7.2 Security measures

7.2.1 Organizational safeguards

- There should be ongoing commitment to privacy and continued emphasis of its importance by all involved in the research and the institutional/organizational management.
- All involved in the research project should be subject to a pledge of confidentiality.
- Access to personal information should be strictly limited in terms of numbers of persons, for legitimate purposes, and strictly on a realistic need-to-know basis.

- Data-sharing agreements between the researcher/institution and all involved should be signed prior to providing any access to data.
- Consequences for breach of confidentiality, including dismissal and/or loss of institutional privileges, should be clearly stipulated.
- Institutions and organizations housing research projects and archived data should, with ongoing commitment of adequate resources:
 - develop, monitor and enforce privacy and security policies and procedures;
 - appoint privacy officers and create data stewardship committees as needed; and
 - implement internal and external privacy reviews and audits.

7.2.2 Technological measures

- Encryption, scrambling of data and other methods of reducing the identifiability of data should be used to eliminate unique profiles of potentially identifying information.
- Direct identifiers should be removed or destroyed at the earliest possible opportunity.
- If direct identifiers must be retained, they should be isolated on a separate dedicated server/network without external access.
- Camouflage sampling⁷⁴ or other techniques should be used, when appropriate, to prevent researchers from viewing health-related information of eligible individuals prior to gaining their consent.
- Authentication measures (such as computer password protection, unique log-on identification, etc.) should be implemented to ensure only authorized personnel can access data.
- Special protection for remote electronic access to data should be installed.
- Virus-checking programs and disaster recovery safeguards such as regular back-ups should be implemented.
- Where possible, a detailed audit trail monitoring system should be instituted to document the person, time, and nature of data access, with flags for aberrant use and “abort” algorithms to end questionable or inappropriate access.

⁷⁴ See the Glossary in Appendix A-6 for the definition of *Camouflaged Contacting*.

7.2.3 Physical security

- Computers and files that hold personal information should be housed in secure settings in rooms protected by such methods as combination lock doors or smart card door entry, with paper files stored in locked storage cabinets.
- The number of locations in which personal information is stored should be minimized.
- Architectural space should be designed to preclude public access to areas where sensitive data are held.
- Routine surveillance should be conducted.
- Physical security measures should be in place to protect data from hazards such as floods or fire.

LINK TO TRI-COUNCIL POLICY STATEMENT:

Article 3.2 Explanatory Text: "Researchers should ensure that the data obtained are stored with all the precautions appropriate to the sensitivity of the data...Accordingly, information that identifies individuals or groups should be kept in different databases with unique identifiers. Researchers should take reasonable measures to ensure against inadvertent identification of individuals or groups, and must address this issue to the satisfaction of the REB." (pg. 3.4)

ELEMENT #8: Controlling access and disclosure of personal data

General statement

Data sharing for research purposes- whether of linked or unlinked data sets- is an important way of enabling socially valuable research. It avoids unnecessary duplication of data collection, which reduces the burden on research participants and permits researchers to use limited or scarce resources more productively.

However, there should be strict limits on access to data and secure procedures for data linkage, subject to REB approval and data-sharing agreements.

When personal data are essential to research objectives and questions, researchers need a plan for making public the results of research in ways that do not permit tracing back to individuals if they do not wish their identities to be known.

8.1 Controlled levels of data access within research team and for secondary use

Researchers and institutions should protect against unauthorized disclosure and use of sensitive data or data subjects' identities, by controlling access to personal data.

Controlling access to data for research purposes means, under most circumstances, that:

- sensitive and/or highly identifiable data are accessible to the minimum number of persons necessary on the research team on a need-to-know basis (e.g. for cleaning data, conducting data linkages, and verifying the accuracy of data matches);
- team members have appropriate training in, and comply with, security safeguards;
- access to coded data, or to data where the direct identifiers are removed but potentially identifying elements remain in the dataset, may be permitted for researchers outside the research team only under strictly controlled conditions described in a written agreement and following REB approval; and
- non-identifiable data about individuals and aggregated data are made available to the general scientific community and for public use after appropriate scrutiny to minimize or avoid risks of inadvertent disclosure of individuals' identities.

Controlled access to personal data for research purposes

Access to:	Who should be permitted access: (examples)	Required safeguards to include:
Direct identifiers	<ul style="list-style-type: none"> • Selected members of the research team • Selected institution employees • “Deemed employees” or trusted third parties, subject to the same undertaking of confidentiality as the data holder (e.g. institution employees) 	<ul style="list-style-type: none"> • REB review and approval • Review by institution data privacy committees where relevant • Access on need-to-know basis • Appropriate training • Undertaking of confidentiality by employees or research team • No direct access for researchers external to the research team, except for linkage purposes in exceptional circumstances (see 8.2) • Audit trails on access (where possible)
Not directly identifiable data (single or double coded; or without codes)	<ul style="list-style-type: none"> • Research team • Collaborators at local sites of a multi-site study • External researchers, with limitations (see required safeguards). 	<ul style="list-style-type: none"> • REB-approved projects • Review by institution data privacy committees where relevant • Data-sharing agreement, including undertaking of confidentiality (see 8.3) • Disclosure of only enough data to answer the intended research question
Non-identifiable data in public use files (where data have been scrutinized and altered to protect against risks of inadvertent disclosure of individuals’ identities). ⁷⁵	<ul style="list-style-type: none"> • Scientific community • General public • Universities 	<ul style="list-style-type: none"> • There may be no restrictions on use, or there may be a basic form of data sharing agreement, requiring an undertaking, for example, to not attempt to re-identify the records so as to relate the information on the file to a particular person.⁷⁶

⁷⁵ For more information on disclosure control, refer to Statistics Canada Research Data Centres (RDCs) *Guide for Researchers Under Agreement with Statistics Canada*, July 2004, online at: http://www.statcan.ca/english/rdc/rdc_guides.htm.

⁷⁶ See, for example, the data acquisition and use agreement for Statistics Canada public use microdata files under the Data Liberation Initiative, online at: <http://www.statcan.ca/english/DLI/reports.htm>.

8.2 Conducting data linkages

The most secure way of conducting data linkages requested by external researchers is for the data holder to conduct the linkage and provide linked datasets to the researcher without identifiers, and at the minimum level of identifiability required for the research purpose.⁷⁷ If that is not practicable, a trusted third party may conduct the linkage or the researcher may conduct the linkage on the data holder's site. As a last option, a researcher may be permitted to conduct the linkage at a secure site but under strict controls, as specified in a data-sharing agreement.⁷⁸

Ranked options for conducting data linkages

Who should conduct the linkage	Conditions for REB consideration
A) Data holder (Preferred)	The data holder performs the linkage(s) and subsequently removes all direct identifiers, or replaces direct identifiers with a code, prior to releasing the linked data set to the external researcher.
B) A trusted third party (e.g. a statistical agency) or C) The researcher conducts the linkage on the data holder's site	When the original data holder does not have the technical capacity or resources to perform linkages in-house: <ul style="list-style-type: none"> • a trusted third party acting as an information manager may conduct the linkage off site; or • the researcher as a "deemed employee" (e.g. the Statistics Canada model) may conduct the linkage on the data holder's site. The third party and the researchers should be bound by equivalent conditions of confidentiality and security as apply to the data holder and the data holder's employees.
D) The researcher conducts the linkage off site	If Options A, B or C are demonstrably impracticable, the researcher may conduct the linkage in compliance with a data-sharing/confidentiality agreement with the data holder, setting out their respective and shared obligations, including restrictions on use and disclosure and appropriate security requirements (see 8.3 below). In this situation, any direct identifiers or other personal data not required to answer the research question should be destroyed or returned to the original data holder as soon as is practicable, and in compliance with the terms of the data-sharing agreement.

⁷⁷ The linked dataset may have direct identifiers removed or coded, or be made non-identifiable, depending on the needs of the research. See Element #2, 2.2.2, 2.3, and Summary Guide in that section.

⁷⁸ Refer to table of concordance for Element #8, Part 1, in Appendix A-7, for statutory cross-references to data matching/linking provisions.

Following the linkage of datasets, the person doing the data linkage should reduce datasets to the lowest level of identifiability needed to accomplish the research objectives.

For example, direct identifiers (e.g. name or personal health number) or potentially identifying elements when combined (e.g. a full date of birth or full postal code) may be needed for data linkage but may not be needed to answer the research questions. In such cases, these identifiers should be destroyed as soon as is reasonably practicable or returned to the data holder, as per the terms of the data-sharing agreement.

Universities may have specified retention periods for research data. Researchers should either destroy the new linked dataset at the end of the specified period, or use enhanced security measures to store it as per the terms of the data-sharing agreement. Within some research or statistical agencies it may not be practicable to unlink datasets after each use. However these institutions should document a process to ensure that the linked datasets are used only for authorized purposes (e.g. for REB-approved projects).

8.3 Data-sharing agreements

Data-sharing agreements bind data providers and researchers to their respective responsibilities and obligations for protecting personal data.

Data-sharing agreements should set out the terms and conditions under which data providers will allow researchers to access personal data for research purposes.⁷⁹

Data-sharing agreements typically include the following information related to privacy concerns:

Basic information	Explanation
1) Research purposes ⁸⁰	<ul style="list-style-type: none"> • A meaningful description of the research objectives and methods.
2) Data elements and uses ⁸¹	<ul style="list-style-type: none"> • A meaningful explanation of why the research objectives cannot reasonably be accomplished without access to these personal data. • Identification of data sources for the project and any linkages to be conducted. • A statement that the researcher will not use the data for any other purpose without prior authorization by the data provider.

⁷⁹ Refer to the table of concordance for Element #8, Part 2, in Appendix A-7, for statutory provisions for research data-sharing agreements.

⁸⁰ See also Element #1.

⁸¹ See also Element #2.

Basic information	Explanation
3) Informed consent materials and form ⁸²	<ul style="list-style-type: none"> • Copies of the explanatory material and consent form to be provided to prospective participants, if appropriate (see #4 below).
4) Contact ⁸³	<ul style="list-style-type: none"> • Statement that the researcher will not attempt to contact data subjects without prior authorization by the data provider, if appropriate.
5) Data access and disclosure	<ul style="list-style-type: none"> • A listing of who will have access to personal data within the research team or the institution, and a requirement that each of these individuals have signed an undertaking of confidentiality. • A statement that the researcher will not disclose the data to other parties without prior authorization by the data provider.
6) Reporting results	<ul style="list-style-type: none"> • A requirement that results and data not be released in a form that identifies individuals to whom the information relates.
7) Security ⁸⁴	<ul style="list-style-type: none"> • A description of the physical, organizational and technological security measures in place to safeguard against risks of unauthorized use, disclosure, corruption or destruction.
8) Retention/ destruction of data ⁸⁵	<ul style="list-style-type: none"> • The time period for data retention and conditions for the return or the destruction of direct identifiers at the earliest reasonable time consistent with the research objectives. • The possibility for the data provider to authorize an extended retention period. • Statement that the researcher will not attempt to re-identify the data subjects without prior authorization by the data provider, if appropriate.
9) Required approvals/ authorizations ⁸⁶	<ul style="list-style-type: none"> • The requirement to have obtained REB approval and other relevant authorizations. • The duration of the agreement or a date designated for the parties to review the agreement.
10) Compliance with laws and policies ⁸⁷	<ul style="list-style-type: none"> • Obligation of recipients to comply with applicable laws and any of the data holder's policies and procedures relating to the confidentiality of personal information.

⁸⁰ See also Element #1.

⁸¹ See also Element #2.

⁸² See also Element #4 and #5.

⁸³ See also Element #3 (3.3) and #6; and the legal concordance table for Element #6 in Appendix A-7 for restrictions on contact.

⁸⁴ See also Element #7

⁸⁵ See also Element #9.

⁸⁶ See also Element #10.

⁸⁷ See also Element #10.

Basic information	Explanation
11) Accountability ⁸⁸	<ul style="list-style-type: none"> • The data provider reserves the right to conduct on-site visits, to monitor or audit data use or to respond to allegations of breach. • If the conditions of the data-sharing agreement are breached, penalties should be imposed, such as no further data to be provided by the data holder to the researcher(s) in question; legal recourse against the researcher for breach of contract; referral of matters to federal or provincial oversight or regulatory bodies for investigation and possible sanctions, and/or a report of the researcher's conduct to the relevant REB and/or federal research sponsor, where relevant and applicable (for example, where a breach of the data-sharing agreement also amounts to a breach of the TCPS).⁸⁹

8.4 Controls over disclosure in public reports of research findings

Appropriate measures should be taken to avoid or minimize the identifiability of data in publications or public databases. Statistics Canada guidance in this area is available online.⁹⁰

8.4.1 Reporting qualitative research results when concealing individuals' identities is not desired

In assessing the privacy aspects of research, researchers and REBs should also be aware of the possibility that in some instances individuals may want their identities to be known—for example, when individuals want their contribution to research as participants to be recognized, or where they want to help others afflicted with a similar condition. In some qualitative research, individual participants may understand and willingly accept the possibility that their identities may be revealed in the public reporting of research results.

⁸⁸ See also Element #10.

⁸⁹ For example, see CIHR's *Procedure for Addressing Allegations of Non-compliance with Research Policies*, online at <http://www.cihr-irsc.gc.ca/e/25178.html>.

⁹⁰ See Statistics Canada *Quality Guidelines* (4th Edition- Oct 2003), pg. 61-66, on line at <http://www.statcan.ca/english/freepub/12-539-XIE/index.htm>. Also, see Statistics Canada's *Guide for Researchers under Agreement with Statistics Canada* (July 2004), Appendix 2- *More on Disclosure and Disclosure Risk*, online at: http://www.statcan.ca/english/rdc/rdc_guides.htm.

LINK TO TRI-COUNCIL POLICY STATEMENT:

[Disclosure controls]

"Data released should not contain names, initials or other identifying information. While it may be important to preserve certain types of identifiers (e.g., region of residence), these should be masked as much as possible using a standardized protocol before the data are released for research purposes. However, legitimate circumstances may exist where such information is critical for the research project..." (pg. 3.4)

[Human genetic research]

Article 8.2 "The researchers and the REB shall ensure that the results of genetic testing and genetic counseling records are protected from access by third parties, unless free and informed consent is given by the subject. Family information in databanks shall be coded so as to remove the possibility of identification of subjects within the bank itself." (pg. 8.2)

[Secondary uses]

Article 3.3, 3.4 – See Element #3

[Data linkage]

Article 3.6 "The implications of approved data linkage in which research subjects may be identifiable shall be approved by the REB." Explanatory note: "...Only a restricted number of individuals should perform the function of merging databases; researchers should either destroy the merged file immediately after use, or use enhanced security measures to store it. Whether the data are to be used statistically or otherwise, confidentiality of the information must be maintained by all members of the research team." (pg. 3.6)

ELEMENT #9: Setting reasonable limits on retention of personal data

General statement

Personal data should be retained as long as is necessary to fulfill the research purposes.⁹¹ Personal data may then be destroyed or returned to the data provider, if appropriate, as set out in the terms of the original collection, data-sharing agreement, institutional policies and legal requirements.

There is a tension between the privacy principle of limiting the retention of data and the scientific principle of preserving research data so that published research results can be replicated and verified, and opportunities for further investigation of valuable data are maximized. While this is a very complex area in need of further reflection and development, the default principle is to define retention periods for personal data, in writing. Researchers should be explicit about what they plan to do with the data they collect and have storage, management and access policies in place.

9.1 Retention of personal data

9.1.1 Specific research project

Where personal data are collected and used in the context of a specific research project, identifying personal data should be retained by the researcher as long as necessary to fulfill the original research objectives,⁹² including related purposes such as tracing, validating or auditing research results as may be required by regulators, study sponsors and/or publishers.⁹³

9.1.2 Database for general health research purposes

When personal data are collected in a database to support general health research purposes in the future, personal data may be retained for the general purposes originally consented to, subject to security safeguards proportionate to the identifiability, sensitivity and amount of the data, as well as its format and method of storage.

⁹¹ Note that under the Food and Drug Regulations- Division 5- C.05.012 (4) records for clinical trials must be retained for 25 years. Universities may have specified retention periods for research data.

⁹² See Element #1.

⁹³ See the legal concordance table for Element #9 in Appendix A-7 for general obligations in privacy legislation with respect to retention of personal information.

Administrative databases such as hospital discharge records and vital statistics registries, which may be used to support health research, may retain personal data over the long term, provided that this is permitted according to legislation or the mandate of a public body such as a government health department.

Any long-term retention of personal data established for general health research purposes should be subject to periodic audits and effective oversight by independent third parties including REBs.

ELEMENT #10: Ensuring accountability and transparency in the management of personal data

General statement

Individuals and organizations engaged in health research involving personal data are accountable for the proper conduct of such research in accordance with applicable funding policies, privacy principles and/or legislation. Processes and practices must be clearly established and implemented in order to give meaningful effect to these policies, principles or laws. Proper accountability and transparency practices require adequate resources for such things as communication, education and training relating to privacy.

Roles and responsibilities of all those involved in the conduct and evaluation of research should be clearly defined and understood, including those of researchers, their employing institutions, REBs, any data stewardship committees, Privacy Commissioners and other legally-designated privacy oversight agencies. Their concerted efforts should aim to provide a coherent governance structure for effective and efficient data stewardship.⁹⁴

10.1 Transparency

Recognizing that transparency may enhance public support for, and interest in, socially valuable research, individuals and organizations engaged in the conduct and evaluation of health research should:

- be open to the public with respect to the objectives of the research;
- be open about the policies and practices relating to the protection of personal data used in the research;
- promote ongoing dialogue between the research community and privacy oversight agencies; and
- promote ongoing dialogue between the research community and the community at large (the public).

⁹⁴ See the table of concordance for Element #10, Part 1, in Appendix A-7, for general statutory accountability and transparency obligations as well as Part 2 for statutory references to research ethics boards.

10.2 Accountability

Key roles and responsibilities with respect to privacy concerns of those involved in designing, conducting and approving publicly-funded health research are outlined below.

10.2.1 Researchers (Principal investigator, researchers)

Privacy-related responsibilities include:

- being aware of all applicable policies and laws in the jurisdictions in which the research is conducted and conducting their research in accordance with such requirements;
- seeking REB and institutional approval and, where required or considered appropriate, the review or approval of other relevant legal privacy oversight bodies;
- providing a mechanism to handle queries and complaints from participants about the privacy aspects of the research (e.g. REB contact information in the consent form); and
- promoting openness and accountability through publicly available information which describes the purpose and conduct of the research project(s) and how privacy concerns are being managed.

10.2.2 Academic and other affiliated or hosting institutions

Privacy-related responsibilities include:

- developing and applying institutional privacy policies and procedures for the conduct and review of research that meet, as a minimum, the requirements set out in the TCPS and other applicable funding policies and laws;
- designating an individual who is accountable for the institution's compliance with those policies and procedures;
- providing for the education and training of researchers and REB members on how to manage personal data in health research;
- providing a mechanism for handling queries and complaints about the privacy and confidentiality aspects of research;
- demonstrating impartial and accountable procedures to investigate allegations of individual non-compliance, with appropriate sanctions for non-compliance;

- being open with the public about research supported by the institution; processes and practices for managing personal information; and procedures for receiving and handling complaints; and
- fostering coordinated data stewardship and institutional review processes within and between institutions.

10.2.3 REBs

Privacy-related responsibilities include:

- reviewing any proposed and ongoing research involving humans in accordance with the TCPS and its principles,⁹⁵ as well as other applicable laws and policies, including:
 - the institution's own policies;
 - federal, provincial and territorial legislation; and
 - relevant laws, regulations, policies and/or research contexts of other countries, when research is to be conducted in those countries;
- serving as a consultative body to the research community and thus contributing to education in research ethics;
- fostering coordinated and consistent REB review processes, particularly with respect to multi-jurisdictional and multi-site research; and
- undertaking regular monitoring of research and coordinating reviews of multi-centre research to ensure equivalencies in standards across jurisdictions, by conducting:
 - an annual review of the research (required under TCPS);
 - an audit of critical aspects of the research protocol including the consent process, safeguards and, where relevant, methods of reducing the identifiability of data prior to disclosure; and
 - other effective monitoring mechanisms, as appropriate.

10.2.4 Independent data stewardship committees

When a database is created for multiple research purposes, or across multiple sites or jurisdictions, researchers and institutional data holders should promote coordinated and streamlined approaches

⁹⁵ The TCPS ethical framework includes a general principle that the more potentially invasive or harmful the research, particularly from the individual participants' perspective, the greater should be the REB's care in assessing the research. This is the concept of proportionate review.

to data stewardship over the long term. A centralized data stewardship committee could be put in place to authorize future uses of the database in accordance with the research objectives, REB approval and, where applicable, within the parameters set by the consent obtained from participants.

The responsibilities of this advisory committee could include:

- the review of data access requests;
- long-term management of the database;
- coordination of reviews by local REBs, for example, by means of agreements between REBs, institutions and researchers, as appropriate; and
- provision of information to the public (e.g. on a web site).

The composition of the committee should include scientific experts in the field and representatives from the population being studied.

10.3 Legally-designated privacy oversight agencies

As specified in legislation, the responsibilities of privacy oversight agencies, such as the Office of the Privacy Commissioner or Ombudsman in each jurisdiction, may include all or any of the following:

- monitoring and investigating compliance with legal requirements;
- issuing findings and recommendations and/or adjudicating complaints from the public with regard to non-compliance;
- initiating and/or participating in court action for breach of legal requirements for privacy protection;
- conducting audits of organizations' information management practices;
- reviewing privacy impact assessments for proposed research;
- reviewing and/or approving the collection of personal information without consent;⁹⁶
- reporting publicly on matters of privacy compliance;
- reviewing and providing comments or approvals on proposed laws or policies; and
- promoting public education with respect to privacy issues.

⁹⁶ See the legal concordance table for Element #3 in Appendix A-7, in particular Quebec privacy laws.

LINK TO TRI-COUNCIL POLICY STATEMENT:

[Mandate of the three federal research granting agencies: CIHR, SSHRC and NSERC]

“The...Agencies have adopted this Policy as their standard of ethical conduct for research involving human subjects. As a condition of funding, the Agencies require, as a minimum, that researchers and their institutions apply the ethical principles and the articles of this policy.” (pg. i.2)

Article 1.1 “(a) All research that involves living human subjects requires review and approval by an REB in accordance with their Policy Statement, before the research is started, except as stipulated..” (pg. 1.1)

[Review procedures for ongoing research]

Article 1.13 “(a) Ongoing research shall be subject to continuing ethics review. The rigour of the review should be in accordance with a proportionate approach to ethics assessment. (b) As part of each research proposal submitted for REB review, the researcher shall propose to the REB the continuing review process deemed appropriate for that project.(c) Normally, continuing review should consist of at least the submission of a succinct annual status report to the REB. The REB shall be promptly notified when the project concludes.” (pg. 1.10)

“In accordance with the principle of proportionate review, research that exposes subjects to minimal risk or less requires only a minimal review process. The continuing review of research exceeding the threshold of minimal risk that is referred to in Article 1.13(b), in addition to annual review (Article 1.13 (c)) might include:

- formal review of the process of free and informed consent*
- establishment of a safety monitoring committee*
- periodic review by a third party of the documents generated by the study*
- review of reports of adverse events*
- review of patients’ charts or*
- a random audit of the process of free and informed consent.*

Other models of a continuing ethics review may be designed by researchers and REBs to fit particular circumstances.

The process of a continuing ethics review should be understood as a collective responsibility, to be carried out with a common interest in maintaining the highest ethical and scientific standards. Research institutions should strive to educate researchers on the process of a continuing ethics review through workshops, seminars and other educational opportunities.” (pg. 1.10- 1.11)

[Review of multi-centered research]

“Principles of institutional accountability require each local REB to be responsible for the ethical acceptability of research undertaken within its institution. However, in multi-centred research, when several REBs consider the same proposal from the perspectives of their respective institutions, they may reach different conclusions on one or more aspects of the proposed research. To facilitate coordination of ethics review, when submitting a proposal for multi-centered research, the researcher may wish to distinguish between core elements of the research—which cannot be altered without invalidating the pooling of data from the participating institutions—and those elements that can be altered to comply with local requirements without invalidating the research project. REBs may also wish to coordinate their review of multi-centred projects, and to communicate any concerns that they may have with other REBs reviewing the same project. The needed communication would be facilitated if the researcher provides information on the institutional REBs that will consider the project.” (pg. 1.11)

[Equivalence level of protection in multi-jurisdictional research]

Article 1.14 “Research to be performed outside the jurisdiction or country of the institution that employs the researcher shall undergo prospective ethics review both (a) by the REB within the researcher’s institution; and (b) by the REB, where such exists, with the legal responsibility and equivalent ethical and procedural safeguards in the country or jurisdiction where the research is to be done.” (pg. 1.12)

LINK TO: Memorandum of Understanding on the Roles and Responsibilities in the Management of Federal Grants and Awards (MOU). Schedule 2- Ethics Review of Research Involving Humans.

1.0 Policy “The Agencies developed, approved and implemented a joint policy statement to promote the ethical conduct of research involving human subjects – the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS). The Agencies will only fund researchers, Institutions or partnering organizations that comply with the ethical principles and articles of the TCPS. In addition CIHR will only fund human pluripotent stem cells research that adheres to its recently published guidelines.

In addition to the TCPS, the ethics review of research involving humans may, where appropriate, be subject to other legislation and policies, such as:

- *the Institution's own policy on research involving human subjects;*
- *the Québec Civil Code;*
- *provincial and federal legislation on privacy, confidentiality, intellectual property, competence and other areas;*
- *Canada Food and Drug Act and Regulations;*
- *guidelines and policies of the Therapeutic Products Directorate of Health Canada;*
- *relevant laws, regulations and/or policies of other countries, when research is to be conducted in those countries;*
- *Good Clinical Practices: Consolidated Guidelines for clinical trials sponsored by industry, published by the International Conference on Harmonization.*

Researchers, Institutions and research ethics boards (REBs) should be aware of all applicable policies, regulations and guidelines. In some cases, it may be necessary for Institutions to have recourse to specific expertise to identify legal and other issues in the ethics review process..."

See web link for updates – http://www.nserc.gc.ca/institution/mou_sch2_e.htm

Appendices

A-1 CIHR Privacy Advisory Committee: Members	96
A-2 Drafting process and consultations 2004	98
A-3 Real world case studies and links to the elements	100
A-4 Diversity of health research and future considerations.....	103
A-5 Selected documents and web links.....	108
A-6 Glossary.....	110
A-7 Tables of concordance with privacy legislation	113
<i>Explanatory Note</i>	114
<i>Application of Canadian Privacy Legislation</i>	115
<i>For Element #1</i>	118
<i>For Element #2</i>	119
<i>For Element #3</i>	121
• Conditions for use and disclosure for research purposes without consent	
<i>For Element #4</i>	129
• Part 1- Consent requirement and elements of consent	
• Part 2- Consent by substitute decision makers	
<i>For Element #5</i>	135
• Provision of all information relevant to voluntary and informed consent	
<i>For Element #6</i>	138
• Statutory prohibitions to secondary use/disclosure of personal information to contact individuals to participate in research	
<i>For Element #7</i>	140
• Part 1- General safeguarding requirements	
• Part 2- Requirement for a privacy impact assessment	
<i>For Element #8</i>	147
• Part 1- Data matching/linkage provisions	
• Part 2- Data-sharing agreements for research purposes	
<i>For Element #9</i>	153
• Retention and destruction of personal information	
<i>For Element #10</i>	157
• Part 1- Accountability and transparency	
• Part 2- Statutory references to research ethics boards	

A-1 CIHR Privacy Advisory Committee

MEMBERS

Privacy Commissioners

David Loukidelis
Information and Privacy Commissioner of British Columbia

(Privacy-enhancing Technologies)

Debra Grant
Senior Health Privacy Specialist
Information and Privacy Commissioner/Ontario

Research ethics boards (REBs)

Sharon Buehler
Co-Chair, Research Ethics Board, Memorial University

Don Willison
(CIHR-funded research on REBs)
Scientist, Centre for Evaluation of Medicines,
McMaster University

Health researchers

Charlyn Black (Health Services Research)
Director, BC Centre for Health Services and Policy Research

Colin L. Soskolne (Epidemiology)
Professor, Department of Public Health Sciences,
University of Alberta

Voluntary health organizations

Roy West
Co-Chair, Science and Research Committee, Health Charities Council of Canada

Patients/consumers

Mary Vachon
Psychotherapist and Consultant in Private Practice
Professor, Depts. of Psychiatry and Public Health Science, University of Toronto
Clinical Consultant, Wellspring

Phil Upshall
Chair, Canadian Alliance on Mental Illness and Mental Health
President- The Mood Disorders Society of Canada

Policy-makers

Heather McLaren
Director, Legislative Unit
Manitoba Health

Data producers/custodians

Joan Roch
Former Chief Privacy Officer, CIHI
Privacy Consultant

Michael Wolfson
Assistant Chief Statistician
Statistics Canada

Aboriginal interests

Bronwyn Shoush
CIHR Institute Advisory Board Member- Institute of Aboriginal People's Health,
Director, Aboriginal Justice Initiatives Unit, Alberta Solicitor General

Health service providers

Denis Cournoyer
Associate Physician, McGill University Health Centre;
Associate Professor, Dept. of Medicine and Oncology, McGill University

Ethics/law

Brent Windwick
Partner, Field LLP
Former Executive Director, Health Law Institute

Bartha Maria Knoppers
Canada Research Chair in Law and Medicine;
Professor, Public Law Research Centre, Faculty of Law, University of Montreal

Ex officio membersInteragency Advisory Panel on Research Ethics (PRE):

Pierre Deschamps, PRE member
Member of the Canadian Human Rights Tribunal

Social Sciences and Humanities Research Council of Canada (SSHRC)

Christian Sylvain (alternate : Jocelyn Girard)
Director, SSHRC Corporate Policy and Planning

National Council on Ethics in Human Research (NCEHR)

Fern Brunger, NCEHR Member
Assistant Professor, Health Care Ethics, Faculty of Medicine
Memorial University

Health Canada

Ross Hodgins/John Horvath
Privacy Division
Information, Analysis & Connectivity Branch, Health Canada

International advisor

William W Lowrance
International Consultant in Health Policy and Ethics,
Geneva, Switzerland

Canadian Institutes of Health Research

Patricia Kosseim - Chair
Former A/Director, Ethics Office
General Counsel, Office of the Privacy Commissioner of Canada

Sheila Chapman
Senior Ethics Policy Advisor

Mylène Deschênes
Former Senior Ethics Policy Advisor

Sylvie Burion
Project Officer

A-2 Drafting process and consultations in 2004

The Canadian Institutes of Health Research (CIHR) is Canada's main federal funding agency for health research. CIHR's mandate is to invest in research that has the potential to lead to improved health for Canadians, more effective health services and products, and a strengthened Canadian health care system. CIHR-funded health research must also meet the highest standards of scientific excellence and ethics.

Recognizing that one of the key ethical challenges for the health research community is to appropriately protect the privacy of those individuals whose information is used for research purposes, CIHR has initiated and promoted dialogue with the broad health research community on a range of privacy-related matters for many years. In particular, a multi-stakeholder workshop in November 2002 entitled *Privacy in Health Research: Sharing Perspectives and Paving the Way Forward* resulted in a number of recommendations including that CIHR initiate the development of privacy best practices and promote the harmonization of privacy laws and policies that impact on health research.

Following on these recommendations, CIHR established a Privacy Advisory Committee (PAC) in 2003 to advise CIHR on the development of privacy best practices for health research, and on strategies for consultation, communication and knowledge translation. CIHR, with the advice of PAC, developed *Guidelines for protecting privacy and confidentiality in the design, conduct and evaluation of health research- Best Practices, Consultation Draft*, April 2004.⁹⁷ A wide range of stakeholders was consulted on this draft from March through September, 2004. The current version of the Privacy Best Practices was revised to reflect the feedback received.

Response to consultations in 2004

We thank the many organizations and individuals who provided feedback on the 2004 draft Guidelines.⁹⁸ The consultation period extended from March through September, 2004, with some written comments being received through mid-October. There were three streams for providing feedback: (1) written comments received in response to invitations sent to key stakeholders, and through an on-line feedback questionnaire; (2) three multi-stakeholder workshops on specific themes aimed at addressing potential gaps in coverage; and (3) two small group dialogue sessions with citizens.

We heard that the broad health research community, including review and oversight bodies, were generally supportive of this initiative, while also making a number of suggestions for improvements of the draft Best Practices. We also were reminded that there is a diversity of points of view within and between stakeholder groups on privacy and confidentiality issues. Some respondents commented that the draft privacy best practices were too restrictive and could impede research, and others thought they were not restrictive enough. We heard from discussions with citizens that there appears to be generally strong support for health research, but also concern about potential unauthorized uses of personal information.

In response to feedback received, we have made the following main changes for this 2005 release:

- A change in the title to: "*Best Practices for Protecting Privacy in Health Research*". Respondents noted that the previous title was too long, and combined both "guidelines" and "best practices" concepts. Also, it was noted that the document is meant to be recommended practices, which aspire in the future to the status of mandatory policy; thus there was general agreement that the term "best practices" was most appropriate at this stage.
- A revision of the Executive Summary to better reflect the main text.
- A clearer explanation of CIHR's mandate – to promote health research that meets the highest standards of excellence and ethics.
- Addition of accompanying tables on relevant legal requirements, as guideposts for health researchers, research ethics boards and others, but not intended to serve as formal legal advice.

⁹⁷ The *Guidelines for protecting privacy and confidentiality in the design, conduct and evaluation of health research- Best Practices, Consultation Draft*, April 2004 are accessible on CIHR's web site at: <http://www.cihr-irsc.gc.ca/e/22085.html>

⁹⁸ Summary reports of feedback received, and an evaluation of the 2004 consultation process, are accessible on CIHR's web site at: <http://www.cihr-irsc.gc.ca/e/28350.html>.

- Addition of an accompanying table on different research areas, user groups, data collection methods, and activities, to demonstrate the applicability of this document to a wide range of target users.
- Addition of an index to research methods covered in the Privacy Best Practices, to help researchers navigate the document to find relevant sections.
- A more explicit acknowledgement of the different fundamental values in play, such as the rights and responsibilities of individuals, and the ethical framework articulated in the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (TCPS).
- A clear recognition that the default position in health research should be the requirement for consent from individual participants.
- Acknowledgement that the reality of researchers in such fields as health services and population health differs significantly from that of clinical researchers, with reference to CIHR *Secondary Use of Personal Information in Health Research: Case Studies* document.
- Strengthened recognition of the privacy concerns of communities and groups.
- Strengthened coverage of privacy issues for qualitative methods and inductive data collection and analysis.
- Strengthened coverage of genetic data, and confirmation that the scope of the Privacy Best Practices does not extend to the management and governance of human biological materials.
- Recognition of the tension between the principles of limiting access and retention of personal data, and the growing importance of making research data (particularly from publicly-funded research) available for broad research use and social benefit, with encouragement for researchers to think about these issues and to be explicit about what they plan to do with the data they collect.

Not surprisingly, given the extent of feedback received, the diversity in points of view, and the need to limit the scope and size of the document, not all requests for changes could be met. For example, these Best Practices do not specifically address privacy issues associated with health surveillance, program quality assurance studies, or private industry-funded research. Nevertheless, these Best Practices could serve as models for best practices developed in these other areas. And in response to requests for more focus on Aboriginal research and qualitative research methods, we provide some additional coverage in this 2005 document. However, we look forward to the more detailed work in these areas being coordinated through the Interagency Advisory Panel on Research Ethics.

As we note throughout this document, these Best Practices will need to continually evolve to reflect new best practices, refinements of existing practices, the findings of research on privacy, and changes in the legal and policy framework for health research in Canada.

A-3 Real world case studies and links to the elements

In 2002, CIHR published *Secondary Use of Personal Information in Health Research: Case Studies* (November 2002).⁹⁹ Nineteen case studies were developed to describe real-life examples of actual research involving secondary use of data in Canada. These case studies highlighted the practical challenges that arise when applying various legal and ethical norms in the specific context of population health and health services research. The case studies identified a number of ethical and legal issues that warranted further consideration and discussion.

The summary table of issues from the *Case Studies* is reprinted below, with an additional column on the far right providing a link to relevant sections of the Best Practices.¹⁰⁰

Case study #	Title of case study	Collection / use / linkage of data	Issues raised	Relevant to Privacy Best Practices Element #:
1	<i>The computerization of medical practices for the enhancement of therapeutic effectiveness</i>	Collection and use of coded data from patient medical records contained in doctors' offices; no direct patient contact involved; implied consent with possibility of opting out.	Prior contact by original data custodian. Form of consent required	3, 4, 6, 7
2	<i>Seasonal patterns of Winnipeg hospital use</i>	Linkage and analyses of coded data contained in provincial databases routinely collected for other purposes (i.e. hospital discharge data and population registry file); no direct contact involved; no consent obtained.	Impracticability of obtaining consent. Long-term retention of data for future research purposes.	3, 7, 8, 9
3	<i>Assessing the accuracy of the Nova Scotia health survey</i>	Linkage and analyses of coded data contained in provincial databases routinely collected for other purposes (i.e. hospital discharge data and physician claims database); no direct contact involved; no consent obtained.	Impracticability of obtaining consent.	3, 4, 7, 8
4	<i>National diabetes surveillance system</i>	Creation of a national diabetes database of aggregate data by linking and assembling coded data contained in provincial databases routinely collected for other purposes (i.e. hospital files, physician billing records and drug claims data); no direct contact involved; no consent obtained.	Impracticability of obtaining consent. Need for harmonization of laws and policies across jurisdictions. Long-term retention of data for future research purposes.	3, 7, 8, 9, 10
5	<i>Use of RFLP molecular epidemiology to find out how tuberculosis is spread among people infected with HIV</i>	Linkage and analyses of TB bacteria grown from individual sputum samples in a public health laboratory, with non-identifying demographic data held by the province's health ministry; no direct contact involved; no consent obtained.	What constitutes personal information. Form of consent required.	2, 3, 4, 7, 8

⁹⁹ See CIHR's web site, online at: <http://www.cihr-irsc.gc.ca/e/1475.html>.

¹⁰⁰ The table is reprinted verbatim from pg. 39 of the *Case Studies* document except for changes to terms referring to the level of identifiability of data, to be consistent with terms defined in Element #2, *Box-Definition of terms: Individual identifiability of data*, and in the Glossary, in Appendix A-6.

Case study #	Title of case study	Collection / use / linkage of data	Issues raised	Relevant to Privacy Best Practices Element #:
6	<i>HIV seroprevalence among women undergoing abortion</i>	Linkage of non-identifying questionnaires with non-identifying test results of blood samples obtained for therapeutic abortion purposes; direct patient contact; written consent obtained.	Form of consent required. Need for harmonization of laws and policies across jurisdictions.	3, 4, 6, 10
7	<i>New use of anti-arrhythmia drugs in Saskatchewan</i>	Linkage and analyses of coded data contained in provincial databases routinely collected for other purposes (i.e. drug claims database, hospital discharge data and physician billing records); no direct contact involved; no consent obtained.	Impracticability of obtaining consent.	3, 7, 8
8	<i>Barriers to accessing health care in Canada: is the System Fair?</i>	Linkage and analyses of personal information contained in Statistics Canada's National Population Health Survey, with provincial databases routinely collected for other purposes (i.e. hospital discharge data and physician billing data); direct contact involved; express consent obtained.	Validity of informed consent. Need for harmonization of laws and policies across jurisdictions.	5, 7, 8, 10
9	<i>Needle stick injuries in nursing and laboratory staff</i>	Collection and use of non-identifying questionnaires, combined with general statistics at each participating hospital; direct contact involved; express consent obtained.	Prior contact by original data custodian. Mandatory reporting and the researchers' duty of confidentiality.	4, 6, 7, 9
10	<i>A randomized controlled trial of call/recall of 'hard-to-reach' women for Pap tests</i>	Linkage of personal information from electronic medical records, with provincial cancer and cytology registries for purpose of assembling study population; direct contact involved; no individual consent obtained but physician authorization granted.	Prior contact by original data custodian. Impracticability of obtaining consent. Long-term retention of data for consistent research purposes.	6, 7, 8, 9
11	<i>The impact of having elderly and welfare patients in Quebec pay a greater share in the costs of their prescription drugs</i>	Linkage and analyses of coded data routinely collected in provincial databases for other purposes (i.e. prescriptions claims data, hospital discharge data, physician billing data and mortality data); no direct contact involved; no consent obtained.	Distinction between policy evaluation and research. Impracticability of obtaining consent.	2, 3, 8
12	<i>A randomized drug policy trial with camouflaged contacting of patients</i>	Linkage of coded data routinely collected in provincial databases for other purposes (i.e. prescriptions claims data, hospital discharge data, physician billing data and mortality data) for the purpose of assembling a study population; quality of life questionnaires then sent to potentially eligible research subjects through camouflaged contacting method; consent obtained for linking questionnaires with administrative data.	Distinction between policy evaluation and research. Prior contact by original data custodian.	5, 6, 8
13	<i>Cancer and other health problems associated with breast implants</i>	Linkage and analysis of personal information obtained from hospital records and clinical records, with data obtained from provincial cancer registries and registrars of vital statistics; no direct contact involved; no individual consent obtained, but nation-wide publicity program conducted.	Unique legal status of cancer registries. Prior contact by original data custodian. Impracticability of obtaining consent.	2, 3, 4, 7

Case study #	Title of case study	Collection / use / linkage of data	Issues raised	Relevant to Privacy Best Practices Element #:
14	<i>Second cancers following treatment for non-Hodgkin lymphoma</i>	Linkage and analysis of personal information obtained from a provincial cancer registry with personal information contained in hospital and radiotherapy center records; no direct contact involved; no individual consent obtained as 75% of the study cohort had died.	Unique legal status of cancer registries. Prior contact by original data custodian. Impracticability of obtaining consent.	3, 5, 6
15	<i>Ontario familial colon cancer registry</i>	Reviewing tumour pathology report forwarded to a provincial cancer registry, as validated by attending surgeons, in order to first identify and invite eligible patients and families for inclusion in the registry; survey data and tissue samples then collected; direct contact involved; consent obtained.	Unique legal status of cancer registries. Prior contact by original data custodian. Implications of assembling genetic information as a particularly sensitive category of personal information.	2, 5, 6, 7
16	<i>Rapid surveillance of cancer in neighbourhoods and near point sources of pollution</i>	Linkage and analysis of personal information contained in a provincial cancer registry with a provincial property assessment file and mortality database; no direct contact involved; no consent obtained; community-wide publicity and consultation process are planned.	Unique legal status of cancer registries. Impracticability of obtaining consent. Community interests.	2, 3, 7, 8
17	<i>Patient outreach via PharmaNet</i>	Automatic flagging of eligible research subjects in the province's drug claims database through the use of a computerized algorithm in order to assemble a study population without any human intervention; direct patient contact involved; consent obtained.	Prior contact by original data custodian.	3, 6
18	<i>The registry of the Canadian Stroke Network</i>	Creation of a national stroke registry by collecting, linking and assembling patients' survey data, health care utilization data and mortality data; direct patient contact involved; consent obtained.	Prior contact by original data custodian. Validity of informed consent. Long-term retention of data for future research purposes. Need for harmonization of laws and policies across jurisdictions.	3, 4, 5, 7, 10
19	<i>Studying the health of health care workers</i>	Linkage and analyses of coded health data contained in provincial databases routinely collected for other purposes (i.e. hospital records, physician billing data, and drug claims data); no direct contact involved; no consent obtained.	Impracticability of obtaining consent. Long-term retention of data for future research purposes.	3, 7, 8, 9

A-4 Diversity of health research and future considerations

To understand the scope of these Best Practices, it is helpful to consider the multi-faceted landscape of CIHR-funded health research in this country.

Health research projects span a spectrum of disciplines and methods.

These Best Practices are intended to address the full spectrum of CIHR-funded research.¹⁰¹ CIHR categorizes health research in four broad themes, as defined in its Grants and Awards Guide:¹⁰²

- **Bio-medical research**
Research with the goal of understanding normal and abnormal human functioning, at the molecular, cellular, organ system and whole body levels, including development of tools and techniques to be applied for this purpose; developing new therapies or devices that improve health or the quality of life of individuals, up to the point where they are tested on human subjects. Studies on human subjects that do not have a diagnostic or therapeutic orientation.
- **Clinical research**
Research with the goal of improving the diagnosis, and treatment (including rehabilitation and palliation), of disease and injury; improving the health and quality of life of individuals as they pass through normal life stages. Research on, or for the treatment of, patients.
- **Health services research**
Research with the goal of improving the efficiency and effectiveness of health professionals and the health care system, through changes to practice and policy. Health services research is a multidisciplinary field of scientific investigation that studies how social factors, financing systems, organizational structures and processes, health technologies, and personal behaviours affect access to health care, the quality and cost of health care, and, ultimately, Canadians' health and well-being.
- **Social, cultural, environmental and population health**
Research with the goal of improving the health of the Canadian population, or of defined sub-populations, through a better understanding of the ways in which social, cultural, environmental, occupational and economic factors determine health status.

CIHR encourages multi-disciplinary research that cuts across these broad thematic areas.

CIHR-funded health research also spans a range of research methods, including quantitative methods (typically based on large numbers of participants, involving hypothesis generation and testing, and statistical analyses of data) and qualitative methods (typically not involving the testing of hypotheses, but rather more open-ended and inductive analysis and collaborative observation techniques, often with smaller numbers of individuals).¹⁰³

Health research projects may cross community, provincial, territorial or national boundaries.

Health research may involve particular cultural groups or communities, such as Aboriginal groups or remote communities.

¹⁰¹ Note that the scope of these Privacy Best Practices does not necessarily extend to particular issues of privacy and confidentiality, and related legal requirements, in research that is entirely funded by private industry.

¹⁰² CIHR's Grants and Awards Guide, 2005-2006.

¹⁰³ A search of the CIHR funding database on the search term "qualitative methods" elicited over a hundred CIHR-funded research projects using qualitative methods as of 2004-2005. These CIHR-funded projects were investigations into such areas as public, community and family values, and in some cases involved the community in the development and conduct of the research.

A single health research study may have multiple sites in more than one province or territory. Research teams may be composed of a network of investigators drawn from across the country and across disciplines. CIHR's 13 "virtual" institutes are founded on this model, promoting collaboration among investigators in various jurisdictions, working on similar questions from different perspectives.

And, because health is a global issue, health research can have an international dimension. Researchers collaborate with colleagues in other countries as they have in the multi-year international Human Genome Project and in CIHR's Global Health initiative.

Health research is conducted in various settings, often supported by a mix of public and private funds.

A great deal of research is based at universities where investigators may have both public and private funding sources. Governments and affiliated research or statistical agencies conduct research on such things as emerging public health issues and the effectiveness of the health care system. They increasingly look for private-public partnerships in sponsorship. Statistical and research agencies with a public mandate conduct research within their agencies and frequently also serve as data stewards permitting, under strict controls, access to their data by external researchers such as those with CIHR funding.

Potential data sources for health research are also diverse.

Individuals are one essential source of health-related data. Individuals are recruited, for example, for clinical trials of new treatments and therapies; and for surveys (conducted by telephone, by mail or in person) on personal lifestyles and attitudes and on the health status of the population. Sometimes the interactions of individuals or groups are simply observed and documented.

Existing databases that were not originally created for research purposes are also important sources of data for health research. These databases have the potential to provide data that are difficult to obtain or cannot be obtained directly from individuals, such as physician diagnoses and records of hospital treatment (in health administrative databases), official registration of births, deaths and cause of death (in population registries), and disease trends and geographic "hot spots" in the population over time (in health surveillance databases).

Thus, these Best Practices have a broad scope, encompassing the wide spectrum of CIHR-funded health research intended to contribute generalizable knowledge to protect and improve human health.

For a more detailed description of the diversity of health research methods, the tables in this section provide examples of studies recruiting individuals or communities, and the wide range of important sources of research data.

Table 1: Examples of studies recruiting individuals or communities

Examples of participants	Examples of data items collected	Examples of research potential	Examples of data collection methods
Residents of a rural community	<ul style="list-style-type: none"> • Age, sex and other demographic information • Length of residence • Attitudes toward a new teen drop-in health service • Use of new service • Health history 	<ul style="list-style-type: none"> • To identify factors that influence community acceptance and use of teen drop-in health services • To assess the impact over time of the new clinic on reducing health problems and teen pregnancies among teens in rural communities 	<ul style="list-style-type: none"> • Observation of teen activities or review of service records in a number of rural communities, some with new teen health services and some without • Interviews with health care providers and patients • Interviews or surveys of teens and adults in the community
Individuals with asthma	<ul style="list-style-type: none"> • Age, sex and other demographic information • History of asthma and other medical conditions 	<ul style="list-style-type: none"> • To assess the impact on health of a new asthma drug • To identify barriers to proper use of a drug 	<ul style="list-style-type: none"> • Clinical trials (see TCPS, Section 7 for more information about clinical trials) • Interviews with asthma patients

Examples of participants	Examples of data items collected	Examples of research potential	Examples of data collection methods
	<ul style="list-style-type: none"> Medication history Meaning of illness 	<ul style="list-style-type: none"> To identify the impact of asthma on quality of life To explore the meaning of illness in asthma patients 	and parents <ul style="list-style-type: none"> Survey of asthma patients Focus groups of clinic personnel
Individuals with colon cancer	<ul style="list-style-type: none"> Age, sex and other demographic information Family history Health and treatment history Dietary habits Exposures to cancer risks in the environment Blood sample Meaning of “hereditary” and “risk”, in relation to genetic screening 	<ul style="list-style-type: none"> To examine interactions of genes and the environment in causing cancer To determine the need for education materials (for physicians and patients) about the risk of inheriting cancer To assess the impact on family members of screening for disease 	<ul style="list-style-type: none"> Telephone or mailed surveys In-depth interviews Laboratory analyses of blood samples collected at the time of the interview Long-term follow up by telephone or mail
Tamil refugees in the Greater Toronto area	<ul style="list-style-type: none"> Age, sex and other demographic information Length of residence Refugee status Health history Use of health resources 	<ul style="list-style-type: none"> To identify barriers to accessing health care To identify psychosocial and health issues associated with resettlement To assess use of complementary and alternative medicines 	<ul style="list-style-type: none"> Participant observation research In-depth interviews Analysis of patient files Analysis of personal letters and journals

Table 2: Examples of databases with research potential, held in diverse settings

Databases	Examples of data ¹⁰⁴	Examples of research potential	Examples of data holders
Health administrative databases	<ul style="list-style-type: none"> Health insurance registration Physician diagnoses in billing records for provincial health insurance plans Hospital records 	<ul style="list-style-type: none"> To examine interactions between the environment and health To describe trends in disease and wellness over time To evaluate the impact of changes in the health care system 	<ul style="list-style-type: none"> Government Ministries of Health Hospitals Statistical agencies
Population registries	<ul style="list-style-type: none"> Records of all births, deaths, cause of death in a geographically defined population (e.g. a province) 	<ul style="list-style-type: none"> To assess the burden of disease in a geographic area Linked with health records, to assess prenatal and post-natal care and health outcomes, and long-term outcomes of health conditions (e.g. length of survival and cause of death) 	<ul style="list-style-type: none"> Provincial and Territorial registrars Statistical agencies

¹⁰⁴ Differing amounts of data elements (e.g. age, sex, residence, occupation) will be found in each of these datasets.

Databases	Examples of data ¹⁰⁴	Examples of research potential	Examples of data holders
Disease registries	<ul style="list-style-type: none"> • A database that holds permanent, ongoing personal data about a population group affected by a particular disease (e.g. cancer) or condition, for statistical, surveillance and/or research purposes. 	<ul style="list-style-type: none"> • To identify potential research participants • To look at trends in new cases of disease • To look for associations of disease and risk factors • To assess the effectiveness of treatment • Linked with death records, to assess survival and ultimate cause of death 	<ul style="list-style-type: none"> • Government agencies • Disease agencies • Hospitals • Statistical agencies
Clinical research databases	<ul style="list-style-type: none"> • Detailed data on medical history, psychosocial factors, patient status, care and associated health outcomes 	<ul style="list-style-type: none"> • To identify potential research participants • To evaluate the efficacy of treatment • To look at continuity of care 	<ul style="list-style-type: none"> • Physicians • Disease clinics and institutes (e.g. diabetes, heart disease) • Industry sponsors
Human genetic material banks	<ul style="list-style-type: none"> • Primary materials (blood, bone and cultured tissue) • Secondary materials (copies of primary samples such as cellular protein) • Tertiary materials (electronically stored information such as DNA sequences) • Linked clinical information 	<ul style="list-style-type: none"> • To develop diagnostic methods • To assess the genetic basis of variability in drug efficacy and safety (pharmacogenetics) • To discover the genetic and biochemical causes of disease (often linked to hospital data and/or genealogy information) 	<ul style="list-style-type: none"> • Government public health and research laboratories • Private companies • Universities • Hospitals • Clinical genetics clinics
Health surveillance databases	<ul style="list-style-type: none"> • Public health data on chronic and communicable disease • Reports of adverse health effects from marketed products 	<ul style="list-style-type: none"> • To search for causes of disease outbreaks or increasing numbers of new cases • To document the burden of disease in populations • To describe long-term trends in health status at the community or population level. 	<ul style="list-style-type: none"> • Government Ministries of Health • World Health Organization • Statistical agencies
Survey databases	<ul style="list-style-type: none"> • Demographic information, workplace conditions, health services availability • Self-reported personal behaviours, health status, medical conditions, lifestyle, attitudes, values, and experiences 	<ul style="list-style-type: none"> • To describe and assess the broad determinants of health (individual, biological, social, cultural, and environmental) and their impact on populations and individuals • To describe and assess psychosocial factors in illness and disease and their individual, biological, social, cultural and environmental determinants 	<ul style="list-style-type: none"> • Government departments • Statistical agencies • Researchers • Universities • Research centres

Future considerations: The changing landscape of health research

The research landscape is an evolving one, as our knowledge and technological capacities continue to advance. In particular, the impact of new developments on research is still to be determined in areas such as:

- the projected implementation of electronic health records across Canada over the next decade;
- discoveries in genomics and research on genetic-environmental interactions;
- emerging standards for Aboriginal research;¹⁰⁵
- increasing use of health-related databases, such as hospital and vital statistics records, for multiple purposes including patient care and management, program management, public health functions and services (e.g. cancer screening, vaccinations, chronic disease risk factor surveillance, obesity interventions) and research; and
- government-led initiatives toward a harmonized legal framework for protecting the privacy and confidentiality of health information across all jurisdictions in Canada.

¹⁰⁵ Developments relevant to research in Aboriginal settings include the current review of TCPS Section 6 (*Research Involving Aboriginal Peoples*), coordinated by the Interagency Advisory Panel on Research Ethics and including CIHR-led development of guidance on Aboriginal health research.

A-5 Selected documents and web links

Selected international and national guidelines

• Council for International Organization of Medical Societies (CIOMS):

- *International Ethical Guidelines for Biomedical Research Involving Human Subjects* (2002)
Online: http://www.cioms.ch/frame_guidelines_nov_2002.htm
- *International Ethical Guidelines for the Ethical Review of Epidemiological Studies* (1991)
Online: http://www.cioms.ch/frame_1991_texts_of_guidelines.htm (Currently under revision. See <http://www.cioms.ch/index.htm>)

• European Commission- Data protection:

Online: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

• Interagency Advisory Panel on Research Ethics:

- Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada: *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (TCPS), 1998 (with 2000, 2002, 2005 amendments)
Online: <http://www.pre.ethics.gc.ca/english/policystatement/policystatement.cfm>
- TCPS tutorial
On-line: <http://www.pre.ethics.gc.ca/english/tutorial/>

• Medical Research Council (United Kingdom):

- *Ethics Series- Personal Information in Medical Research* (2000)
Online: <http://www.mrc.ac.uk/pdf-pimr.pdf>

• Quebec Network of Applied Genetic Medicine (RMGA):

All policies online: <http://www.rmgq.qc.ca/en/index.htm>

- *Statement of Principles on the Ethical Conduct of Research Involving Populations*
- *Statement of Principles: Human Genome Research, Version 2000*
- *Research in Human Genetics and Consent* (French only)

• UK Biobank Project:

- *Ethics and Governance Framework*
Online: <http://www.ukbiobank.ac.uk/ethics/egf.php>

For other key guidance documents see the Interagency Advisory Panel for Research Ethics web site at: <http://www.pre.ethics.gc.ca/english/links/links.cfm>.

Privacy legislation

- **CIHR A Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research** (April 2000, to be updated 2005)

Online: <http://www.cihr-irsc.gc.ca/e/6824.html>

- **Federal/Provincial/Territorial Oversight Offices-web links:**

- Canada (Federal)- http://www.privcom.gc.ca/index_e.asp
- British Columbia- <http://www.oipc.bc.ca/>
- Alberta- <http://www.oipc.ab.ca/home/>
- Saskatchewan- <http://www.oipc.sk.ca>
- Manitoba- <http://www.ombudsman.mb.ca/>
- Ontario- <http://www.ipc.on.ca/>
- Quebec- <http://www.cai.gouv.qc.ca/index-en.html>
- Prince Edward Island- <http://www.assembly.pe.ca/foipp/index.php>
- Nova Scotia- <http://www.foipop.ns.ca>
- New Brunswick- <http://www.gnb.ca/0073/index-e.asp>
- Newfoundland and Labrador- <http://www.oipc.gov.nl.ca/default.htm>
- Yukon- <http://www.ombudsman.yk.ca/>
- Northwest Territories- Email : atippcomm@theedge.ca
- Nunavut- Email : atippcomm@theedge.ca

Disclosure controls

- **Statistics Canada:**

- *Quality Guidelines* (4th Edition- Oct 2003), pg. 61-66,
Online: <http://www.statcan.ca/english/freepub/12-539-XIE/index.htm>
- *Guide for Researchers under Agreement with Statistics Canada* (July 2004), Appendix 2- *More on Disclosure and Disclosure Risk*
Online: http://www.statcan.ca/english/rdc/rdc_guides.htm

Related documents

- **CIHR Procedure for Addressing Allegations of Non-compliance with Research Policies.**
Online: <http://www.cihr-irsc.gc.ca/e/25178.html>
- **CIHR Secondary Use of Personal Information in Health Research: Case Studies** (November, 2002).
Online: <http://www.cihr-irsc.gc.ca/e/1475.htm>
- **CIHR Selected International Legal Norms on the Protection of Personal Information in Health Research** (December, 2001).
Online: http://www.cihr-irsc.gc.ca/e/pdf_24017.htm
- **W. Lowrance, Learning from Experience: Privacy and the Secondary use of Data in Health Research,** November 28, 2002.
Online: <http://www.nuffieldtrust.org.uk/publications/detail.asp?id=O&Prid=45>

A-6 Glossary

The following terms are defined here as used in this document. Readers should be aware, however, that these terms are not yet standardized and may be used somewhat differently in other contexts.

Aggregate data. The data have been averaged or grouped into ranges (e.g. 5 or 10-year age groupings).

Camouflaged contacting. This is an approach to sampling and contacting patients with particular medical conditions in such a way that the individual making the contacting is not aware of the health status of that individual at the time of contacting. Records of individuals with and without the condition of interest are sampled in some pre-determined proportion from the original source (e.g. administrative or clinical records). Contact information about the combined-sample group is then released without any information about the health status of the individual being disclosed to the person making contact (by telephone or mail). The health status of the individual remains concealed until such time as the individual agrees to participate in the research and to disclose whether or not he or she has the condition of interest.

Coded data. Single code: A participant's data are assigned a random code. Direct identifiers are removed from the dataset and held separately. The key linking the code back to direct identifiers is available only to a limited number (e.g. senior members) of the research team. Double or multiple codes. Two or more codes are assigned to the same participant's data held in different datasets (e.g. health administrative data, clinical data, genetic samples and data). The key connecting the codes back to participants' direct identifiers is held by a third party (such as the data holder) and is not available to the researchers. Coded data refers to data that are at least single coded. (See Element #2, Section 2.2.2, *Box-Definition of terms*).

Consent. Agreement to participate in research (which may include the collection, use or disclosure of personal data) by a legally competent person, or by authorized third parties on behalf of those who lack legal competence. Consent, to be valid, must be voluntary and informed. For consent to be voluntary, the consent must be given without the exertion of undue influence on the person, and with the option of withdrawing from the research at any time without penalty. For consent to be informed, the person must be given information about the research, and must understand this information. (See TCPS, Section 3)

Confidentiality. Confidentiality is the obligation of an organization or custodian to protect the information entrusted to it and not misuse or wrongfully disclose it. (From *The Pan-Canadian Health Information Privacy and Confidentiality Framework*, January 27, 2005. Accessible on the Health Canada- Health and the Information Highway Division- Ehealth Resource Centre web page, under Reports 2005, at: http://www.hc-sc.gc.ca/ohih-bis/about_apropos/hcpubssc_e.html).

Data. Facts or figures from which conclusions can be drawn. Data can take various forms, but are often numerical, such as daily weight measurements of each person in a group (ref. Statistics: *Power from data!* - Statistics Canada On-line: <http://www.statcan.ca/english/edu/power/toc/contents.htm>). See also definitions for *Information*.

Data custodian. See *Data holder*.

Data holder. The Data holder may have custodianship and/or stewardship functions. These functions may be executed within the same institution/body or may be delegated to distinct but coordinated institutions/bodies. Data custodianship relates primarily to responsibility for data storage and integrity. Data stewardship relates primarily to responsibility for data definition and access authorization, particularly data access and disclosure to third parties.

Data steward. See *Data holder*.

Data subject. The individual who is the subject of personal data/information collected for research purposes. Distinguished from Research Participant.

Direct collection. Collection of data directly from individuals.

Direct identifiers. These are variables such as name and address, health insurance number, etc., that provide an explicit link to a respondent. (Statistics Canada)

Indirect identifiers. These are variables such as date of birth, sex, marital status, area of residence, occupation, type of business, etc. that, in combination, could be used to identify an individual. (Adapted from Statistics Canada)

Impracticable. For the purposes of this document, "impracticable" means a degree of difficulty in doing something under present conditions, where the degree of difficulty is greater than would arise if something is merely inconvenient to do but may be less than if something is impossible. The conditions for assessing "impracticability" of consent are described in Element #3.

Information. Data that have been recorded, classified, organized, related, or interpreted within a framework so that meaning emerges. Information, like data, can take various forms. An example of the type of information that can be derived from data is the number of persons in a group in each weight category or changes in weight over time. (ref. Statistics: *Power from data!* - Statistics Canada On-line: <http://www.statcan.ca/english/edu/power/toc/contents.htm>). See also definitions for *Data* and *Statistics*.

Member-checking. This is when a researcher provides participants with the opportunity to look at transcripts of what they have said or done, and to delete or footnote what they consider to be inaccurate or sensitive information.

Non-identifiable data. Any element or combination of elements that allows direct or indirect identification of an individual was never collected or has been removed, although some elements may indirectly identify a group or region. There is no code linking the data back to the individual's identity. (See Element #2, Section 2.2.2, *Box-Definition of terms*)

Personal data/information. Personal data or information may contain a direct link to a specific individual (e.g. name and street address, personal health number, etc.) or any element or a combination of elements that allows indirect identification of an individual (e.g. if birth date combined with postal code and other personal information on the record such as ethnicity could lead to the identification of an individual). The scope of personal information covered in these Privacy Best Practices includes personal information derived from blood and other human biological materials (e.g. information such as blood type, DNA code and the presence or absence of disease), but not the materials themselves.

Privacy. Privacy includes a right to be free from intrusion and interruption. It is linked with other fundamental rights such as freedom and personal autonomy. In relation to information, privacy involves the right of individuals to determine when, how and to what extent they share information about themselves with others. (From *The Pan-Canadian Health Information Privacy and Confidentiality Framework*, January 27, 2005. Accessible on the Health Canada- Health and the Information Highway Division- Ehealth Resource Centre web page, under Reports 2005, at: http://www.hc-sc.gc.ca/ohih-bis/about_apropos/hcpubssc_e.html).

Research. Research is defined in the TCPS as "a systematic investigation designed to develop or establish principles, facts or generalizable knowledge" (TCPS, pg. 1.1). The range of research requiring ethics review in the TCPS is listed in Appendix 1 (TCPS, pg. A.1).

Research participant. The individual who consents to participation in research and who is the subject of personal data or information collected for research. See *Data Subject*.

Secondary use of data for research. The data may have been collected originally for (i) a non-research purpose (e.g. for health care administrative purposes or for health care insurance billing purposes), or (ii) a different research purpose (e.g. for a study on a different but related disease).

Sensitivity. The sensitivity of personal data is related to the potential for harm or stigma that might attach to the identification of an individual because of the nature of the information. The type of information that an individual may consider sensitive could relate to: sexual attitudes, practices and orientation; use of alcohol, drugs, or other addictive substances; illegal activities; suicide; sexual abuse; sexual harassment; an individual's psychological well-being or mental health; some types of genetic information (e.g. information that predicts future illness or disability

and raises concerns around future employability or insurability); and any other information that, if released, might lead to social stigmatization or discrimination. Researchers should also be aware of information that communities may consider sensitive because, for example, of its potential to stigmatize a community.

Tables of Concordance with Privacy Legislation

A-7 Tables of concordance with privacy legislation

Explanatory note¹⁰⁶

- The Tables of Concordance supplement key provisions of the Privacy Best Practices with cross-references to related requirements under Canadian privacy legislation. The Tables also briefly summarize requirements under Canadian privacy legislation which are supplemental to the Privacy Best Practices. A full text of the provisions referred to in the Tables of Concordance can be found in the CIHR's "Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research".¹⁰⁷
- The Tables are for reference purposes only and are intended to be read in conjunction with the Privacy Best Practices. References to specific Tables are found throughout the Privacy Best Practices.
- The requirements under privacy legislation will vary depending on the factual circumstances. As such, the Tables should not be relied upon as legal advice. Readers should consult the relevant privacy statute(s) and, depending on the circumstances, other applicable legal requirements as well as professional codes of ethics.
- The Tables only refer to Canadian federal, provincial and territorial privacy legislation. Municipal and local public sector privacy statutes have also been included.
- The legislation included in the Tables is current through to June 2005.

¹⁰⁶ These Tables of Concordance were prepared by Adam Kardash and Antonella Penta at Heenan Blaikie LLP in consultation with the Ethics Office, privacy regulatory authorities and Ministries of Health.

¹⁰⁷ The Compendium is accessible on CIHR's web site at: <http://www.cihr-irsc.gc.ca/e/6824.html>

APPLICATION OF CANADIAN PRIVACY LEGISLATION

Jurisdiction	Legislation	Entities covered by Legislation
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	<ul style="list-style-type: none"> ▪ 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.)¹⁰⁸ 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.¹⁰⁹ ▪ Federal works, undertakings and businesses that collect, use or disclose personal information, including personal information about employees in any province or territory. ▪ All personal information collected, used or disclosed in cross-border commercial transactions. ▪ Does not apply to government institutions subject to the <i>Privacy Act</i>.
	<i>Privacy Act</i>	<ul style="list-style-type: none"> ▪ 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).
British Columbia	<i>Personal Information Protection Act</i>	<ul style="list-style-type: none"> ▪ All organizations (e.g., health care providers in private practice, pharmacies, pharmaceutical companies, not-for-profit organizations). ▪ Does not apply to personal information if Freedom of Information and Protection of Privacy Act applies.
	<i>Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., governmental bodies, health authorities, hospitals, mental health facilities and universities).
Alberta	<i>Health Information Act</i>	<ul style="list-style-type: none"> ▪ Applies to custodians with respect to health information (e.g., health professionals, health care facilities, regional health authorities, provincial health boards). ▪ Legislation also impacts ethics committees and researchers.
	<i>Personal Information Protection Act</i>	<ul style="list-style-type: none"> ▪ All organizations, including not-for-profit, corporations, professional regulatory associations. ▪ 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.
	<i>Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., government departments, educational bodies, health care bodies and designated agencies, boards and commissions). ▪ Does not apply to health information in records of a public body that is a custodian as defined in the <i>Health Information Act</i>.
	<i>Municipal Government Act</i>	<ul style="list-style-type: none"> ▪ Municipalities.

¹⁰⁸ The precise application of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") to the health care sector has not yet been considered by a court of law. See Industry Canada's "PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector" at: [http://ecom.ic.gc.ca/epic/internet/inccic-ceac.nsf/vwapj/PARTS_QandA-e.pdf/\\$FILE/PARTS_QandA-e.pdf](http://ecom.ic.gc.ca/epic/internet/inccic-ceac.nsf/vwapj/PARTS_QandA-e.pdf/$FILE/PARTS_QandA-e.pdf).

¹⁰⁹ Note that the *Personal Information Protection Act* (Alberta), the *Personal Information Protection Act* (British Columbia) and *An act respecting the protection of personal information in the private sector* (Quebec) have each been deemed substantially similar. The provincial health privacy legislation in each of Alberta, Saskatchewan, Manitoba and Ontario have not been deemed substantially similar, although the Governor in Council has proposed to exempt health information custodians subject to the *Personal Health Information Protection Act* (Ontario) from the application of PIPEDA. Note also that PIPEDA will always apply to federal undertakings (e.g., broadcasting or telecommunications, banks, etc.) and to an organization's transfer of personal information outside the province.

Jurisdiction	Legislation	Entities covered by Legislation
Saskatchewan	<i>The Health Information Protection Act</i>	<ul style="list-style-type: none"> ▪ Trustees with respect to personal health information (e.g., government institutions, regional health authorities, health professionals, health care organizations, professional regulatory bodies). ▪ Legislation also impacts researchers.
	<i>Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Government institutions (e.g., government departments, Crown Corporations, designated provincial boards, bodies and agencies). ▪ Does not apply to information that constitutes personal health information as defined in <i>The Health Information Protection Act</i>.
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Local authorities (e.g., municipalities, universities, regional health authorities, special care homes, designated boards, commissions and bodies). ▪ Does not apply to information that constitutes personal health information as defined in <i>The Health Information Protection Act</i>.
Manitoba	<i>The Personal Health Information Act</i>	<ul style="list-style-type: none"> ▪ Trustees with respect to personal health information (e.g., health professionals, health care facilities, public bodies (including government departments and universities), health services agencies). ▪ Legislation also impacts health information privacy committees, the institutional research review committees and researchers.
	<i>The Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g. universities, certain hospitals, regional health authorities, municipalities, government departments and agencies). ▪ Does not apply to personal health information to which <i>The Personal Health Information Act</i> applies.
Ontario	<i>Personal Health Information Protection Act</i>	<ul style="list-style-type: none"> ▪ 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). ▪ 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. researchers, employers and insurers). ▪ The legislation also applies to all persons with respect to the collection, use and disclosure of the health number.
	<i>Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Institutions (e.g., ministries, agencies, boards and most commissions of the government of Ontario, community colleges). ▪ 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. ▪ Where a FIPPA institution is not a health information custodian, only FIPPA applies, even where information at issue is health information.
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Institutions (e.g. municipalities, boards of health, designated agencies, boards, commissions, corporations or other bodies)

Jurisdiction	Legislation	Entities covered by Legislation
Quebec	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., universities, cegeps, health care facilities, government departments and agencies).
	<i>An act respecting the protection of personal information in the private sector</i>	<ul style="list-style-type: none"> ▪ Persons carrying on an enterprise (e.g., health care providers in private practice, pharmacies and private research companies).
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., government departments, agencies, boards, designated education and health bodies).
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., universities, hospitals, government departments and agencies).
	<i>Municipal Government Act</i>	<ul style="list-style-type: none"> ▪ Municipalities.
New Brunswick	<i>Protection of Personal Information Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., government departments, school boards, regional health authorities).
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹¹⁰</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., universities, health boards, municipalities, government departments).
Yukon	<i>Access to Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., government departments, agencies, boards, commissions and corporations).
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., government departments, agencies, boards).
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	<ul style="list-style-type: none"> ▪ Public bodies (e.g., government departments, agencies, boards).

¹¹⁰ Part IV to be proclaimed.

ELEMENT #1 – DETERMINING THE RESEARCH OBJECTIVES AND JUSTIFYING THE DATA NEEDED TO FULFILL THESE OBJECTIVES

Element #1 provides that researchers should, at the outset of the research design process, identify and document research objectives as a basis for determining what data will be needed for the research. The precise identification and documentation of the purposes for collection, use and disclosure of personal (health) information is critical for the purpose of complying with various requirements under privacy legislation, including requirements relating to the principles of limiting collection of personal information, obtaining consent for collection, use and disclosure of personal (health) information, and accountability and transparency. Statutory references to each of these requirements under Canadian privacy legislation can be found in the following concordance tables in this section:

- Element #2 - Limiting the Collection of Personal Data
- Element #4 - Managing and Documenting Consent
- Element #5 - Informing Prospective Research Participants about the Research
- Element #10 - Ensuring Accountability and Transparency in the Management of Personal Data

ELEMENT #2 – LIMITING THE COLLECTION OF PERSONAL DATA^{111,112}		
Jurisdiction	Legislation	Privacy Legislation Concordance
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	Schedule 1, 4.4 (Limiting Collection)
	<i>Privacy Act</i>	Section 4 (Collection of personal information) Section 5 (Personal information to be collected directly from individual)
British Columbia	<i>Personal Information Protection Act</i>	Section 11 (Limitations on collection of personal information) Section 12 (Collection from source other than the individual)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 26 (Purposes for which information may be collected) Section 27(1) (How personal information is to be collected)
Alberta	<i>Health Information Act</i>	Sections 18 to 21 (Collection of health information) Section 22 (Duty to collect health information from individual directly) Section 24 (Collection of health information by affiliate) Section 57 (Duty to collect, use or disclose health information with highest degree of anonymity possible) Section 58 (Duty to collect, use or disclose health information in a limited manner) Section 68(a) (Health information to be used in data matching to be collected in accordance with the Act)
	<i>Health Information Regulation</i>	Section 5(2) (Persons authorized to collect personal health number)
	<i>Personal Information Protection Act</i>	Section 7(1)(b) (Direct collection) Section 11 (Limitations on collection)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 33 (Purposes for which information may be collected) Section 34(1) (Direct collection)
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	Section 11 (Collection of health numbers) Section 23 (Collection on a need to know basis) Section 24 (Restrictions on collection) Section 25(1) (Direct collection)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 25 (Purpose of information) Section 26 (Manner of collection)
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
Manitoba	<i>The Personal Health Information Act</i>	Section 13(1) (Restrictions on collection) Section 13(2) (Limit on amount of information collected) Section 14 (Source of information) Section 26 (Collection of health numbers)

¹¹¹ This table cross references the statutory provisions for collecting only the personal information needed to fulfill the purpose of the collection. As a general rule, consent is required for collection of personal information, which consent must be voluntary and informed. For statutory provisions relating to the elements and form of consent, please refer to the table for Element #4. For the statutory provisions relating to the notice required for voluntary and informed consent, please refer to the table for Element #5.

¹¹² This table also includes provisions dealing with the requirement to collect personal information directly from the person the information is about. Note that there are various exceptions to this requirement which have not been included in this table.

ELEMENT #2 – LIMITING THE COLLECTION OF PERSONAL DATA^{111,112}		
Jurisdiction	Legislation	Privacy Legislation Concordance
Manitoba	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 36 (1) (Purpose of collection) Section 36(2) (Limit on amount of information collected) Section 37(1) (Manner of collection)
Ontario	<i>Personal Health Information Protection Act</i>	Section 30 (Extent of information) Section 34 (2) (Limits on collecting health numbers) Section 36(1) (Indirect collection)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 38(2) (Collection of personal information) Section 39(1) (Direct collection)
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	Section 5 (Necessary information) Section 6 (Collection from the person concerned)
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 64 (Unnecessary information)
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 31 (Purpose of Collection of Information) Section 32 (Direct collection)
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	Section 24(1) (Treatment of Personal Information)
	<i>Municipal Government Act</i>	—
New Brunswick	<i>Protection of Personal Information Act</i>	Schedule A, Principle 4 (Limiting Collection) Schedule B, Principle 4 (Individuals from whom personal information may be collected)
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹¹³</i>	Section 32 (Purpose for which personal information may be collected) Section 33 (How personal information is to be collected)
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Section 29 (Purpose for which personal information may be collected) Section 30 (How personal information is to be collected)
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Section 40 (Purpose of collection of information) Section 41 (Collection of information from individual concerned)
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Section 40 (Purpose of collection of information) Section 41 (Collection of information from individual concerned)

¹¹³ Part IV to be proclaimed.

ELEMENT #3 – DETERMINING IF CONSENT FROM INDIVIDUALS IS REQUIRED		
Conditions For Use And Disclosure For Research Purposes Without Consent¹¹⁴		
Jurisdiction	Legislation	Privacy Legislation Concordance
Federal	<i>Personal Information Protection and Electronic Documents Act¹¹⁵</i>	<p>Sections 7(2)(c): Conditions for use by an organization for statistical, or scholarly study or research purposes:</p> <ul style="list-style-type: none"> ▪ purpose cannot be achieved without using the information; ▪ information is used in a manner that ensures confidentiality; ▪ impracticable to obtain consent; and ▪ organization informs the Commissioner of the use before information is used. <p>Section 7(3)(f): Conditions for disclosure by an organization for statistical, or scholarly study or research purposes:</p> <ul style="list-style-type: none"> ▪ purpose cannot be achieved without disclosing the information; ▪ impracticable to obtain consent; and ▪ organization informs the Commissioner of the disclosure before information is disclosed.
	<i>Privacy Act</i>	<p>Section 8(2)(j): Conditions for use and disclosure by a government institution for research or statistical purposes:</p> <p>Head of the government institution:</p> <ul style="list-style-type: none"> ▪ is satisfied that the purpose for disclosure cannot reasonably be accomplished unless the information is provided in identifiable form; and ▪ obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in identifiable form.
British Columbia	<i>Personal Information Protection Act</i>	<p>Section 21: Conditions for disclosure by organizations:</p> <ul style="list-style-type: none"> ▪ Research purpose cannot be accomplished unless the personal information is provided in an identifiable form; ▪ information will not be used to contact persons to ask them to participate in the research; ▪ linkage of the personal information to other information is not harmful to the individuals and the benefits to be derived from the linkage are clearly in the public interest; ▪ the organization to which the personal information is to be disclosed has signed a data sharing agreement; and ▪ it is impracticable for the organization to seek the consent of the individual.

¹¹⁴ Consent is generally required under privacy legislation for the use and disclosure of personal information for any purpose, including research purposes, subject to limited exceptions. This chart sets out the conditions upon which personal information may be used or disclosed for research purposes without consent. Reference should also be made to the statutory requirements for data sharing agreements and data matching/linking detailed in the concordance table for Element #8.

¹¹⁵ Note that the consent exemptions noted only apply for the use and disclosure of personal information for statistical, scholarly study or research purposes. There is no equivalent consent exemption in the statute for collecting personal information for such purposes.

ELEMENT #3 – DETERMINING IF CONSENT FROM INDIVIDUALS IS REQUIRED

Conditions For Use And Disclosure For Research Purposes Without Consent¹¹⁴

Jurisdiction	Legislation	Privacy Legislation Concordance
British Columbia	<i>Freedom of Information and Protection of Privacy Act</i>	<p>Section 35: Conditions for disclosure by public bodies:</p> <ul style="list-style-type: none"> ▪ Research purpose cannot reasonably be accomplished unless information is provided in identifiable form or research purpose is approved by Commissioner; ▪ information is disclosed on condition that it not be used to contact a person to participate in the research; ▪ any record linkage is not harmful to the individuals and the benefits to be derived from the record linkage are clearly in the public interest; ▪ head of the public body concerned has approved conditions relating to (i) security and confidentiality; (ii) removal or destruction of individual identifiers at the earliest reasonable time; (iii) prohibition of any subsequent use or disclosure of the information in individually identifiable form without express authorization of the public body; and ▪ recipient has signed an agreement to comply with the approved conditions, the Act and any of the public body's policies and procedures relating to the confidentiality of personal information.
Alberta	<i>Health Information Act</i>	<p>Sections 27(1)(d) and 35(1)(a): Conditions for use and disclosure by a custodian:</p> <ul style="list-style-type: none"> ▪ Custodian submits a proposal to an ethics committee; ▪ ethics committee is satisfied with respect to importance of research, qualifications of researcher, safeguards and that it is not reasonable or practical to obtain consent; and ▪ custodian has complied with/agreed to conditions suggested by the ethics committee. <p>See also section 49 (Research proposal), section 50 (Role of ethics committee), section 51 (Bar to research), section 52 (Application for disclosure of health information), section 53 (Conditions and consents), section 54 (Agreement between custodian and researcher) and section 55 (Consent of the individual is required if additional information is needed).</p>
	<i>Personal Information Protection Act Regulation</i>	<p>Section 12(2): Conditions for disclosure by an archival institution:</p> <ul style="list-style-type: none"> ▪ Disclosure is necessary for the research purpose; ▪ disclosure is not harmful to the individual concerned; ▪ research purpose is not contrary to the purposes and intent of the Act; and ▪ either (i) a reasonable person, taking into consideration all relevant circumstances, would find that disclosure of the personal information was appropriate at the time, or (ii) the information is disclosed under a research agreement. <p>Section 14(3): Conditions for disclosure by an organization that is not an archival institution:</p> <ul style="list-style-type: none"> ▪ Research agreement required; ▪ recipient agrees to comply with the same requirements as those established in respect of archival institutions; ▪ research has been approved by a research ethics review committee; and ▪ researcher has agreed to any additional conditions imposed by the ethics review committee.

ELEMENT #3 – DETERMINING IF CONSENT FROM INDIVIDUALS IS REQUIRED

Conditions For Use And Disclosure For Research Purposes Without Consent¹¹⁴

Jurisdiction	Legislation	Privacy Legislation Concordance
Alberta	<i>Freedom of Information and Protection of Privacy Act</i>	<p>Section 42: Conditions for disclosure by public bodies:</p> <ul style="list-style-type: none"> ▪ Research purpose cannot reasonably be accomplished unless that information is provided in identifiable form or research purpose has been approved by Commissioner, ▪ record linkage is not harmful to individuals and benefits to be derived from record linkage are clearly in public interest, ▪ head of public body has approved conditions relating to (i) security and confidentiality, (ii) removal or destruction of identifiers at the earliest reasonable time, and (iii) prohibition of subsequent use or disclosure without express authorization of that public body, and ▪ recipient signed an agreement to comply with approved conditions, Act and public body's policies and procedures relating to confidentiality of personal information.
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	<p>Section 29(2): Conditions for disclosure by a trustee or designated archive:</p> <ul style="list-style-type: none"> ▪ Only where not reasonably practicable for consent to be obtained and if: <ul style="list-style-type: none"> a) research purposes cannot reasonably be accomplished using de-identified personal health information or other information; b) reasonable steps are taken to protect privacy of individual by removing all personal health information that is not required for the purposes of the research; c) in the opinion of research ethics committee, the potential benefits of the research project clearly outweigh the potential risk to the privacy of the individual; and d) (i) in the opinion of the trustee or designated archive, the research project is not contrary to public interest; (ii) research project is approved by a research ethics committee approved by minister; and (iii) recipient enters into an agreement with trustee or designated archive.
	<i>The Freedom of Information and Protection of Privacy Act</i>	<p>Section 29(2)(k): Conditions for disclosure by public body:</p> <ul style="list-style-type: none"> ▪ Head of public body must be satisfied that purpose for disclosure is not contrary to public interest and cannot reasonably be accomplished unless information is provided in identifiable form; and ▪ agreement must be signed by recipient not to make a subsequent disclosure of the information in identifiable form.
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	<p>Section 28(2)(k): Conditions for disclosure by local body:</p> <ul style="list-style-type: none"> ▪ Head of local body must be satisfied that purpose for disclosure is not contrary to public interest and purpose cannot reasonably be accomplished unless information is provided in identifiable form; and ▪ recipient provides written agreement not to make subsequent disclosure of the information in identifiable form.

ELEMENT #3 – DETERMINING IF CONSENT FROM INDIVIDUALS IS REQUIRED

Conditions For Use And Disclosure For Research Purposes Without Consent¹⁴

Jurisdiction	Legislation	Privacy Legislation Concordance
Manitoba	<i>The Personal Health Information Act</i>	<p>Section 24: Conditions for disclosure by trustees:</p> <ul style="list-style-type: none"> ▪ Research project must be approved by: <ul style="list-style-type: none"> (a) health information privacy committee if personal health information is maintained by government or a government agency; and (b) institutional research review committee, if personal health information is maintained by a trustee other than the government or a government agency. ▪ Approval may be given only if applicable committee has determined that: <ul style="list-style-type: none"> (a) research is of sufficient importance to outweigh the intrusion into privacy; (b) research purpose cannot reasonably be accomplished unless personal health information is provided in identifiable form; (c) unreasonable or impractical for researcher to obtain consent; and (d) research project contains (i) reasonable safeguards to protect confidentiality and security of the personal health information, and (ii) procedures to destroy the information or remove all identifying information at earliest opportunity consistent with the purposes of the project. ▪ Agreement required between trustee and recipient. ▪ Consent required for direct contact with individuals except where information consists only of individuals' names and addresses.
	<i>The Freedom of Information and Protection of Privacy Act</i>	<p>Section 47(4): Conditions for disclosure by public body:</p> <ul style="list-style-type: none"> ▪ Advice requested from review committee has been received and considered; ▪ head is satisfied that (i) the information is requested for bona fide research purpose, (ii) research cannot reasonably be accomplished unless information is provided in identifiable form, (iii) unreasonable or impractical for recipient to obtain consent, and (iv) disclosure of information, and any information linkage, is not likely to harm individuals and benefits to be derived from research and any information linkage are clearly in the public interest; ▪ head of public body has approved conditions relating to (i) protection of personal information, including use, security and confidentiality, (ii) removal or destruction of identifiers at earliest reasonable time, and (iii) prohibition of subsequent use or disclosure of personal information in identifiable form without written authorization of the public body; and ▪ recipient has entered into a written agreement to comply with approved conditions.

ELEMENT #3 – DETERMINING IF CONSENT FROM INDIVIDUALS IS REQUIRED

Conditions For Use And Disclosure For Research Purposes Without Consent¹¹⁴

Jurisdiction	Legislation	Privacy Legislation Concordance
Ontario	<i>Personal Health Information Protection Act</i>	<p>Section 44(1): Conditions for use by health information custodians and disclosure by health information custodians to researchers:</p> <ul style="list-style-type: none"> ▪ Researcher must submit to custodian (i) an application in writing, (ii) a research plan, and (iii) a copy of the decision of a research ethics board that approves research plan; and ▪ researcher must enter into an agreement with custodian agreeing to comply with conditions and restrictions that custodian may impose relating to use, disclosure, return or disposal of information. <p>See also sections 34(2) and (3) (Use and disclosure of health numbers) 37(1)(j) and (3) (Permitted use for research), section 44(2) (Elements of Research plan), section 44(3) and (4) (Consideration and decision of board), section 44(5) (Content of research agreement), section 44(6) (Compliance by researcher), sections 44(10) and (11) (Research approved outside Ontario) and section 50(1)(b) (Disclosure outside Ontario).</p> <p>See also section 39(1)(c) (Disclosure to prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances), section 45 (Disclosure to prescribed entities for planning and management of health systems) and section 47 (Disclosure for analysis of health system).</p>
	<i>Personal Health Information Protection Act, General Regulation</i>	<p>Section 12 (Disclosure of health number):</p> <ul style="list-style-type: none"> ▪ Researchers with custody or control of health numbers, by reason of a use or disclosure authorized under the Act for research purposes, may disclose the health number to a registry prescribed under the Act, an entity prescribed for the purposes of planning and management of health systems or another researcher if, <ul style="list-style-type: none"> o the disclosure is part of a research plan approved under the Act, or o the disclosure is necessary for the purpose of verifying or validating the information or the research. <p>Section 15 (Requirement for research ethics board)</p> <p>Section 16 (Requirement for a research plan)</p> <p>Section 17 (Disclosure by researcher)</p> <p>Section 18(3) and (4) (Rules applicable to section 45 prescribed entities for use and disclosure of personal health information for research purposes)¹¹⁶</p> <p>Section 13(4) and (5) (Rules applicable to registries of personal health information for use and disclosure of personal health information for research purposes)¹¹⁷</p>

¹¹⁶ The following are prescribed for the purposes of section 45:

1. Cancer Care Ontario.
2. Canadian Institute for Health Information.
3. Institute for Clinical Evaluative Sciences.
4. Pediatric Oncology Group of Ontario.

¹¹⁷ The following are prescribed registries:

1. Cardiac Care Network of Ontario in respect of its registry of cardiac services.
2. INSCYTE (Information System for Cytology etc.) Corporation in respect of CytoBase.
3. London Health Sciences Centre in respect of the Ontario Joint Replacement Registry.
4. Canadian Stroke Network in respect of the Canadian Stroke Registry.

ELEMENT #3 – DETERMINING IF CONSENT FROM INDIVIDUALS IS REQUIRED

Conditions For Use And Disclosure For Research Purposes Without Consent¹¹⁴

Jurisdiction	Legislation	Privacy Legislation Concordance
Ontario	<i>Freedom of Information and Protection of Privacy Act</i>	<p>Section 21(1)(e): Conditions for disclosure by public body:</p> <ul style="list-style-type: none"> ▪ Disclosure is consistent with conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained; ▪ research cannot be reasonably accomplished unless information is provided in identifiable form; and ▪ recipient has agreed to comply with the conditions relating to security and confidentiality prescribed by the regulations.¹¹⁸
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—
	<i>Municipal Freedom of Information and Protection of Privacy Act, General Regulation</i>	<p>Section 10(1): Terms and conditions a person must agree to before a head may disclose personal information to that person for a research purpose:</p> <ul style="list-style-type: none"> ▪ Person shall use the information only for a research purpose set out in the agreement or for which the person has written authorization from the institution; ▪ the person shall name in the agreement any other persons who will be given access to personal information in a form in which the individual to whom it relates can be identified; ▪ before disclosing personal information to other persons, the person shall enter into an agreement with those persons to ensure that they will not disclose it to any other person; ▪ the person shall keep the information in a physically secure location to which access is given only to the person and to the persons given access; ▪ the person shall destroy all individual identifiers in the information by the date specified in the agreement; ▪ the person shall not contact any individual to whom personal information relates directly or indirectly without the prior written authority of the institution; ▪ the person shall ensure that no personal information will be used or disclosed in a form in which the individual to whom it relates can be identified without the written authority of the institution; and ▪ the person shall notify the institution in writing immediately if the person becomes aware that any of the conditions set out in this section have been breached.
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	<p>Section 21: Conditions for disclosure:</p> <ul style="list-style-type: none"> ▪ Written request must be made to the commission. ▪ Commission must be satisfied that (i) intended use is not frivolous and the ends contemplated cannot be achieved unless the information is communicated in identifiable form and (ii) information will be used in manner that ensures its confidentiality. ▪ Authorization is granted for such period and on such conditions as may be fixed by the Commission. It may be revoked before the expiry of the period granted if Commission has reason to believe that the authorized person or body does not respect the confidentiality of the information disclosed or the other conditions.

¹¹⁸ Conditions relating to security and confidentiality are prescribed by section 10 of Regulation 460.

ELEMENT #3 – DETERMINING IF CONSENT FROM INDIVIDUALS IS REQUIRED

Conditions For Use And Disclosure For Research Purposes Without Consent¹¹⁴

Jurisdiction	Legislation	Privacy Legislation Concordance
Quebec	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 125: Conditions for disclosure: <ul style="list-style-type: none"> ▪ Same conditions as above.
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 39: Conditions for disclosure by public body: <ul style="list-style-type: none"> ▪ Research purpose cannot reasonably be accomplished unless information is provided in identifiable form or research purpose has been approved by Commissioner; ▪ any record linkage is not harmful to individuals and benefits to be derived from record linkage are clearly in public interest; ▪ head of a public body has approved conditions relating to (i) security and confidentiality, (ii) removal or destruction of individual identifiers at earliest reasonable time, and (iii) prohibition of subsequent use or disclosure of information in identifiable form without express authorization of that public body; and ▪ recipient signs agreement to comply with approved conditions, Act and public body's policies and procedures relating to confidentiality of personal information.
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	Section 29: Conditions for disclosure by public body: <ul style="list-style-type: none"> ▪ Research purpose cannot reasonably be accomplished unless information is provided in identifiable form; ▪ any record linkage is not harmful to individuals and benefits to be derived from record linkage are clearly in public interest; ▪ head of a public body has approved conditions relating to (i) security and confidentiality, (ii) removal or destruction of individual identifiers at earliest reasonable time, and (iii) prohibition of subsequent use or disclosure of information in identifiable form without express authorization of that public body; and ▪ recipient signs agreement to comply with approved conditions, Act and public body's policies and procedures relating to confidentiality of personal information.
	<i>Municipal Government Act</i>	Section 485(4): Conditions for disclosure by municipality: <ul style="list-style-type: none"> ▪ Research purpose cannot reasonably be accomplished unless information is provided in individually identifiable form; ▪ any record linkage is not harmful to individuals the information is about and the benefits to be derived from record linkage are clearly in the public interest; ▪ the responsible officer has approved conditions relating to (i) security and confidentiality, (ii) the removal or destruction of individual identifiers at the earliest reasonable time, and (iii) the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authority of the municipality; and ▪ the person to whom the information is disclosed has signed an agreement to comply with the approved conditions, this Part of the Act, and any of the municipality's policies and procedures relating to the confidentiality of personal information.
New Brunswick	<i>Protection of Personal Information Act</i>	Schedule B, section 3.4: Consent not required when public body collects, uses or discloses personal information for purposes of legitimate research in the interest of science, of learning or of public policy, or for archival purposes.

ELEMENT #3 – DETERMINING IF CONSENT FROM INDIVIDUALS IS REQUIRED**Conditions For Use And Disclosure For Research Purposes Without Consent¹¹⁴**

Jurisdiction	Legislation	Privacy Legislation Concordance
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act</i>	Section 41: Conditions for disclosure by public body: <ul style="list-style-type: none">▪ Same conditions as for Nova Scotia
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Section 38: Conditions for disclosure by public body: <ul style="list-style-type: none">▪ Same conditions as for Nova Scotia
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Section 49: Conditions for disclosure by public body: <ul style="list-style-type: none">▪ Same conditions as for Nova Scotia
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Section 49: Conditions for disclosure by public body: <ul style="list-style-type: none">▪ Same conditions as for Nova Scotia

ELEMENT #4 – MANAGING AND DOCUMENTING CONSENT¹¹⁹

Part 1 - Consent Requirement and Elements of Consent		
Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	Schedule 1, 4.3 and 4.3.1 (Consent Requirement) Schedule 1, 4.3.4, 4.3.6 and 4.3.7 (Form of Consent) Schedule 1, 4.3.2, 4.3.5, 4.3.8 (Elements of Consent)
	<i>Privacy Act</i>	Sections 7 and 8 (Consent Requirement)
British Columbia	<i>Personal Information Protection Act</i>	Sections 6 and 7 (Consent Requirement) Section 8 (Form of Consent) Section 9 (Elements of Consent)
	<i>Freedom of Information and Protection of Privacy Act</i>	Sections 32(b) and 33.1(1)(b) (Consent Requirement)
	<i>Freedom of Information and Protection of Privacy Regulation</i>	Section 6 (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent to disclosure of personal information must be in writing and specify to whom the personal information may be disclosed and how the personal information may be used.
Alberta	<i>Health Information Act</i>	Section 34(1) and (3) (Consent Requirement) Section 34(2), (4), (5) and (6) (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent to disclosure of personal health information must be in writing or be provided electronically and must include: (a) authorization for custodian to disclose the health information specified in the consent; (b) purpose for which the health information may be disclosed; (c) identity of person to whom health information may be disclosed; (d) acknowledgment that individual providing consent has been made aware of reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent; (e) date consent is effective and date, if any, on which consent expires; and (f) statement that consent may be revoked at any time by the individual providing it. ¹²⁰ • Revocation of consent must be provided in writing or electronically.
	<i>Health Information Regulation</i>	Section 6(2) (Electronic Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> An electronic consent or a revocation of an electronic consent is valid only if the level of authentication is sufficient to identify the individual who is granting the consent or revoking the consent, as the case may be.

¹¹⁹ Canadian privacy statutes generally require consent for collection, use and disclosure of personal information for research purposes, subject to exceptions set out in the legislation. This table sets out the form and elements of consent where consent is required for the protection of privacy. See the exceptions to consent requirement for research purposes in table of concordance for Element #3. See also the statutory notice requirements for informed consent in the table of concordance for Element #5. See also the table following this chart for statutory references to consent by substitute decision makers.

¹²⁰ Section 23 of the *Health Information Act* (Alberta) states that if a custodian collects health information from an individual using a recording device or camera or any other device that may not be obvious to the individual, the custodian must, before collecting the information, obtain the written consent of the individual to the use of the device or camera.

ELEMENT #4 – MANAGING AND DOCUMENTING CONSENT¹¹⁹

Part 1 - Consent Requirement and Elements of Consent

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Alberta	<i>Personal Information Protection Act</i>	Section 7 (Consent Requirement) Section 8 (Form of Consent) Section 9 (Withdrawal or variation of consent) Section 10 (Consent obtained by deception)
	<i>Freedom of Information and Protection of Privacy Act</i>	Sections 39(1)(b) and 40(1)(d) (Consent Requirement)
	<i>Freedom of Information and Protection of Privacy Regulation</i>	Section 6(1) (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent to use or disclosure of personal information must be in writing and must specify to whom the personal information may be disclosed.
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	Sections 5, 26 and 27 (Consent Requirement) Sections 6(1) and (2), and 7 (Elements of Consent) Sections 6(3),(4) and (5) (Form of Consent)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Sections 28 and 29 (Consent Requirement)
	<i>The Freedom of Information and Protection of Privacy Regulations</i>	Section 18 (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent to be in writing unless the head of the public body determines that it is not reasonably practicable.
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
	<i>The Local Authority Freedom of Information and Protection of Privacy Regulations</i>	Section 11 (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent to be in writing unless the head of the local body determines that it is not reasonably practicable.
Manitoba	<i>The Personal Health Information Act</i>	Sections 21(b) and 22(1)(b) (Consent Requirement)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Sections 43(b) and 44(1)(b) (Consent Requirement)
Ontario	<i>Personal Health Information Protection Act</i>	Section 29 (Consent Requirement) Sections 18(1), 18(5), 18(6) and 19 (Elements of Consent) Section 18(2), (3) and (4) (Form of Consent)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 41(a) and 42(b) (Consent Requirement)
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—

ELEMENT #4 – MANAGING AND DOCUMENTING CONSENT¹¹⁹

Part 1 - Consent Requirement and Elements of Consent

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	Sections 12 and 13 (Consent Requirement) Section 14 (Elements and Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent must be manifest, free and enlightened ¹²¹
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 53(1) and 59 (Consent Requirement)
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 36(1)(b) and 37(1)(c) (Consent Requirement)
	<i>Freedom of Information and Protection of Privacy Act, General Regulations</i>	Section 6 (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent to use or disclose personal information must (a) be in writing and (b) specify to whom the personal information may be disclosed and how the personal information may be used.
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	Sections 26(b) and 27(b) (Consent Requirement)
	<i>Freedom of Information and Protection of Privacy Regulations</i>	Sections 7(2) and 8 (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent to use of personal information must (i) be in writing, (ii) identify the information, and (iii) specify to whom the information may be disclosed and how the information may be used. ¹²²
	<i>Municipal Government Act</i>	—
New Brunswick	<i>Protection of Personal Information Act</i>	Schedule A, Principle 3 (Consent Requirement) Schedule B, 3.1 and 3.2 (Form of Consent)
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹²³</i>	Sections 38(1)(b) and 39(1)(b) (Consent Requirement)
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Sections 35 (b) and 36 (b) (Consent Requirement)
	<i>Access to Information Regulation</i>	Section 2 (Consent to disclosure of personal information) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Consent to disclosure to be in writing and specify to whom the personal information may be disclosed and how it may be used.
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Sections 43 (b) and 48 (b) (Consent Requirement)
Northwest Territories	<i>Access to Information and Protection of Privacy Regulations</i>	Section 5 (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> The consent of an individual to a public body's use or disclosure of his or her personal information must be in writing and specify to whom the personal information may be disclosed and how it may be used.

¹²¹ This is often interpreted as requiring express consent.

¹²² Consent to disclosure of personal information may be in prescribed form 3 and consent to use of personal information may be in prescribed form 4, each of which are set out in the Regulations to the Act.

¹²³ Part IV to be proclaimed.

ELEMENT #4 – MANAGING AND DOCUMENTING CONSENT¹¹⁹

Part 1 - Consent Requirement and Elements of Consent

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Sections 43 (b) and 48 (b) (Consent Requirement)
	<i>Access to Information and Protection of Privacy Regulations</i>	Section 5 (Form of Consent) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> The consent of an individual to a public body's use or disclosure of his or her personal information must be in writing and specify to whom the personal information may be disclosed and how it may be used.

ELEMENT #4 – MANAGING AND DOCUMENTING CONSENT

Part 2 - Consent by Substitute Decision Makers¹²⁴

Jurisdiction	Legislation	Privacy Legislation Concordance
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	Schedule 1, 4.3.6 – (Consent by authorized representatives)
	<i>Privacy Act Privacy Regulations</i>	Section 10 (Exercise of rights on behalf of minors, persons deemed incompetent, or deceased persons)
British Columbia	<i>Personal Information Protection Act Regulations</i>	Section 2 (Who may act for minors and others) Section 3 (Who may act for deceased persons) Section 4 (Determination of nearest relative)
	<i>Freedom of Information and Protection of Privacy Regulation</i>	Section 3 (Who can act for young people and others)
Alberta	<i>Health Information Act</i>	Section 104(1) (Exercise of rights by other persons)
	<i>Personal Information Protection Act</i>	Section 61(1) (Exercise of rights by other persons)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 84 (Exercise of rights by other persons)
Saskatchewan	<i>The Health Information Protection Act</i>	Section 56 (Exercise of rights by other persons)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 59 (Exercise of rights by other persons)
Manitoba	<i>The Personal Health Information Act</i>	Section 60 (Exercising rights of another person)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 79 (Exercising rights of another person)
Ontario	<i>Personal Health Information Protection Act</i>	Section 5 (Substitute decision-maker) Sections 23 and 26 (Persons who are entitled to consent to the collection, use, or disclosure of personal health information) Section 25 (Authority of substitute decision-maker) Section 27 (Appointment of representative)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 66 (Exercise of rights of deceased, etc., persons)
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	—
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 53 (Person with parental authority may authorize disclosure for a minor)
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 71 (Exercise of rights by other persons)
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	Section 43 (Exercise of right or power by other persons)
New Brunswick	<i>Protection of Personal Information Act</i>	Schedule B, section 3.3 (Consent can be given by a parent, guardian or other representative of the individual in appropriate circumstances)

¹²⁴ This chart cross references the statutory provisions for substitute consent.

ELEMENT #4 – MANAGING AND DOCUMENTING CONSENT**Part 2 - Consent by Substitute Decision Makers¹²⁴**

Jurisdiction	Legislation	Privacy Legislation Concordance
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹²⁵</i>	Section 65 (Exercising rights of another person)
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Section 62 (Personal Representation)
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Section 52 (Exercise of Rights by other persons)
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Section 52 (Exercise of Rights by other persons)

¹²⁵ Part IV to be proclaimed.

ELEMENT #5 – INFORMING PROSPECTIVE RESEARCH PARTICIPANTS ABOUT THE RESEARCH¹²⁶		
Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	Schedule 1, 4.2 (Purpose for collection must be identified at the time of collection and must be documented) Schedule 1, 4.3.2 (Knowledge and consent)
	<i>Privacy Act</i>	Section 5(2) (Individual to be informed of purpose of collection)
British Columbia	<i>Personal Information Protection Act</i>	Section 8(3) 10(1), 14 and 17 (Notice requirements for collection, use and disclosure)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 27(2) (Information to be given regarding purposes for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information.
Alberta	<i>Health Information Act</i>	Sections 21(2) and 22(3) (Information to be given regarding purposes for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the specific legal authority for the collection.
	<i>Personal Information Protection Act</i>	Section 8(3) and 13 (Notification requirements for collection, use and disclosure)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 34(2) (Information to be given regarding purpose for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information.
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	Sections 6 and 9 (Individual must be informed of purposes for collection use, and disclosure of the individual's personal health information)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 26(2) (Individual must be informed of the purposes for the collection)
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	Section 25(2) (Individual to be informed of purposes of collection) Section 57(l) (Lieutenant Governor in Council may make regulations prescribing any matter to be included in notice)
Manitoba	<i>The Personal Health Information Act</i>	Section 15 (Notice of collection practices)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 37(2) (Individual must be informed of the purposes for the collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information
Ontario	<i>Personal Health Information Protection Act</i>	Section 18(5) and (6) (Knowledge of purposes of collection)

¹²⁶ This chart sets out the notice/information provision requirements under applicable privacy statutes. For statutory cross reference to other elements of consent, refer to the table of concordance for Element #4. For general notice obligations, refer to the accountability and transparency provisions set out in the table of concordance for Element #10.

ELEMENT #5 – INFORMING PROSPECTIVE RESEARCH PARTICIPANTS ABOUT THE RESEARCH¹²⁶		
Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Ontario	<i>Freedom of Information and Protection of Privacy Act</i>	Section 39(2) (Information to be given regarding purpose for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information.
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	Section 29(2) (Individual must be informed of primary purposes of collection) <u>Supplemental Requirement to CIHR Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information
	<i>Municipal Freedom of Information and Protection of Privacy Act, General Regulation</i>	Section 4(1) (When notice not required) <ul style="list-style-type: none"> ▪ Institutions not required to give notice of collection if providing notice would frustrate purpose of the collection or might result in an unjustifiable invasion of another individual's privacy. Head of institution must make available a statement describing purpose of collection and reason why notice not given.
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	Section 8 (Information to be given regarding purpose for collection)
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 65 (Information to be given regarding purpose for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Every person who, on behalf of a public body, collects nominative information from the person concerned or from a third person must first identify himself and inform the person concerned that the collection is either mandatory or optional and of the consequences of failing to provide the information.
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 32(2) (Right to be informed regarding purpose for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information.
Nova Scotia	<i>Freedom of Information and Protection of Privacy Regulations</i>	Section 8 (Requirement before use) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Before information about an individual may be used, the individual must identify the information and give consent in writing specifying to whom the information may be disclosed and how the information may be used
	<i>Municipal Government Act</i>	—
New Brunswick	<i>Protection of Personal Information Act</i>	Schedule A, Principle 2 and Schedule B, section 2.1 (Purposes for collection must be identified)
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹²⁷</i>	Section 33(2) (Information regarding purpose for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information.

¹²⁷ Part IV to be proclaimed.

ELEMENT #5 – INFORMING PROSPECTIVE RESEARCH PARTICIPANTS ABOUT THE RESEARCH¹²⁶		
Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Section 30(2) (Information regarding purpose for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information.
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Section 41(2) (Information regarding purpose for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information.
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Section 41(2) (Information regarding purpose for collection) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual must be told of the legal authority for collecting the information.

ELEMENT #6 – RECRUITING PROSPECTIVE RESEARCH PARTICIPANTS

Statutory Prohibitions to Secondary Use/Disclosure of Personal Information to Contact Individuals to Participate in Research¹²⁸

Jurisdiction	Legislation	Privacy Legislation Concordance
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	—
	<i>Privacy Act</i>	—
British Columbia	<i>Personal Information Protection Act</i>	Section 21(b): An organization may disclose, without the consent of the individual, personal information for a research purpose if the disclosure is on condition that it will not be used to contact persons to ask them to participate in the research.
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 35 (a.1): A public body may disclose personal information for a research purpose without the consent of the individual only if the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in the research.
Alberta	<i>Health Information Act</i>	Section 55: If the researcher wishes to contact the individuals who are the subjects of the information disclosed for research purposes to obtain additional health information, the custodian or an affiliate of the custodian must first obtain consents from those individuals to their being contacted for that purpose.
	<i>Personal Information Protection Act Regulation</i>	Section 12(3)(d): If personal information is to be disclosed by an organization under a research agreement, the person to whom the information is to be disclosed must agree to not contact any individual to whom the information relates.
	<i>Freedom of Information and Protection of Privacy Regulation</i>	Section 8(f): The agreement required by the Act for disclosure of personal information without consent of the individual for research purposes must include provision that recipient will not contact any individual to whom the personal information relates, directly or indirectly, without the prior written authority of the public body.
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	—
	<i>The Freedom of Information and Protection of Privacy Act</i>	—
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
Manitoba	<i>The Personal Health Information Act</i>	Section 24(5): If a research project will require direct contact with individuals, a trustee must not disclose personal health information about those individuals without first obtaining their consent. Trustee need not obtain their consent if the information consists only of the individuals' names and addresses.
	<i>The Freedom of Information and Protection of Privacy Act</i>	—

¹²⁸ Consent is generally required under privacy legislation for secondary uses and disclosures of personal information for any purpose, including for contacting a prospective research participant, subject to limited statutory exceptions. Reference should accordingly be made to the concordance table for Element #3 for the conditions where personal information may be disclosed for research purposes without consent. The above chart sets out the specific statutory prohibitions on the use or disclosure of personal information to contact individuals in circumstances where the statute otherwise permits/authorizes the use and disclosure of personal information for research purposes without consent.

ELEMENT #6 – RECRUITING PROSPECTIVE RESEARCH PARTICIPANTS

Statutory Prohibitions to Secondary Use/Disclosure of Personal Information to Contact Individuals to Participate in Research ¹²⁸		
Jurisdiction	Legislation	Privacy Legislation Concordance
Ontario	<i>Personal Health Information Protection Act</i>	Section 44(6)(e): Researcher shall not make contact or attempt to make contact with the individual, directly or indirectly, unless the custodian obtains the individual's consent to being contacted. ¹²⁹
	<i>Freedom of Information and Protection of Privacy Act, General Regulation</i>	Section 10(1)6: Before a head may disclose personal information for a research purpose to a person, that person must agree not to contact any individual to whom personal information relates, directly or indirectly, without the prior written authority of the institution.
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	—
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	—
PEI	<i>Freedom of Information and Protection of Privacy Act</i>	—
Nova Scotia	<i>Freedom of Information and Protection of Privacy Regulations</i>	Section 9: Research agreement must contain condition that recipient not contact any individual to whom personal information relates, directly or indirectly, without the prior written authority of the public body.
	<i>Municipal Government Act</i>	—
New Brunswick	<i>Protection of Personal Information Act</i>	—
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act</i>	—
Yukon	<i>Access to Information and Protection of Privacy Act</i>	—
Northwest Territories	<i>Access to Information and Protection of Privacy Regulations</i>	Section 8: Research agreement must contain condition that the recipient must not contact any individual to whom the personal information relates, directly or indirectly, without the prior written authority of the public body.
Nunavut	<i>Access to Information and Protection of Privacy Regulations</i>	Section 8: Research agreement must contain condition that the recipient must not contact any individual to whom the personal information relates, directly or indirectly, without the prior written authority of the public body.

¹²⁹ Note that section 37(1)(g) allows a health information custodian to use the name and contact information of an individual for the purpose of seeking the individual's consent.

ELEMENT #7 – SAFEGUARDING PERSONAL DATA^{130,131}

Part 1 – General Safeguarding Requirements

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	Schedule 1, 4.7 (Safeguards for protecting personal information) Schedule 1, 4.1.4 (Policies and practices to be implemented to protect personal information)
	<i>Privacy Act</i>	Section 62 (Security Requirements)
British Columbia	<i>Personal Information Protection Act</i>	Section 5 (Policies and practices) Section 34 (Protection of personal information)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 30 (Protection of personal information) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Information must be stored in Canada and accessed only in Canada unless the individual the information is about has identified the information and has consented, in the prescribed manner¹³², to it being stored in or accessed from, as applicable, another jurisdiction or if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under the Act (section 30.1). ▪ Where a public body receives a foreign demand for disclosure, the head of the public body must inform the Minister responsible for the Act (section 30.2(2)).
Alberta	<i>Health Information Act</i>	Section 60 (Duty to protect health information) Section 63 (Duty to establish or adopt policies and procedures)
	<i>Health Information Regulation</i>	Section 8 (Record of safeguards to be maintained) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Written agreement required with respect to safeguards for health information that is to be stored, used or disclosed outside Alberta unless used for continuing treatment and care (section 8(4) and (5)).
	<i>Personal Information Protection Act</i>	Section 6 (Policies and practice) Section 34 (Protection of information)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 38 (Protection of personal information) Sections 40(1)(h)and(i) and 40(4) (Authorization to disclose personal information to officers and employees for purposes of carrying out their functions)
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	Section 16 (Duty to protect) Section 23 (Collection, use and disclosure on a need-to-know basis) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Individual to be informed about disclosures of personal health information made without consent (section 10(1)).
	<i>The Freedom of Information and Protection of Privacy Act</i>	—

¹³⁰ This table sets out the statutory references to general safeguarding obligations. See also the statutory requirements for data-sharing agreements in table of concordance for Element #8, statutory requirements for disposal and destruction in table of concordance for Element #9, and table of concordance for Element #10 regarding the obligation to develop and implement policies and procedures regarding safeguarding of personal information. In addition, see the following table for Element #7 which sets out the statutory requirement to conduct a privacy impact assessment.

¹³¹ Note that public bodies/institutions governed by such legislation may be obligated to comply with governmental security policies or guidelines as a matter of administrative practice.

¹³² No requirements have been prescribed by regulations as at the date of this publication.

ELEMENT #7 – SAFEGUARDING PERSONAL DATA^{130,131}

Part 1 – General Safeguarding Requirements

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Saskatchewan	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
Manitoba	<i>The Personal Health Information Act</i>	Section 18 and 19 (Security Safeguards) Section 20(3) (Limitation on trustee's employees)
	<i>Personal Health Information Regulation</i>	Section 2 (Written security policy and procedure) Section 3 (Access restrictions and other precautions) Section 4 (Additional safeguards for electronic health information systems) Section 5 (Authorized access for employees and agents) Section 6 (Orientation and training for employees) Section 7 (Pledge of confidentiality for employees) Section 8 (Audit) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Audit of security safeguards to be conducted every 2 years (sections 2 and 8). ▪ Each employee and agent must sign a pledge of confidentiality that includes an acknowledgement that he or she is bound by the policy and procedures and is aware of the consequences of breaching them (section 7).
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 41 (Protection of personal information)
Ontario	<i>Personal Health Information Protection Act</i>	Section 10 (Information Practices) Section 12 (Security) Section 13 (Handling of Records) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ An individual shall be notified at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons. However, a researcher shall not notify the individual unless the health information custodian obtains the individual's consent to having the researcher contact the individual and informs the researcher that the individual has given consent (section 12(2) and(3)). ▪ A health information custodian may disclose personal health information to an entity prescribed pursuant to section 45 of the Act¹³³, if the Commissioner has approved the practices and procedures of the entity (sections 45(3)). ▪ The Commissioner must approve the practices and procedures of a health data institute (sections 47(9) and (10)).

¹³³ The following entities are prescribed for the purposes of section 45 of the Act:

1. Cancer Care Ontario
2. Canadian Institute of Health Information
3. Institute for Clinical Evaluation Sciences
4. Pediatric Oncology Group of Ontario

ELEMENT #7 – SAFEGUARDING PERSONAL DATA^{130,131}

Part 1 – General Safeguarding Requirements

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Ontario	<i>Personal Health Information Protection Act, General Regulation</i>	Section 6(3) (Prescribed requirements for health information network provider.) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Health information custodian may transfer records of personal health information for archive purposes to a person who, (a) has put in place reasonable measures to ensure that personal health information in the person's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal (section 14(1)). ▪ Prescribed registries¹³⁴ must put in place practices and procedures approved by the Commissioner and summary of the practices and procedures must be made available to the public (sections 13(2) and 13(3)).
	<i>Freedom of Information and Protection of Privacy Act, General Regulation</i>	Section 4 (Measures to protect records)
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	Section 10 (Safety measures) Section 20 (Authorized employee access to personal information without consent for the performance of duties of employees)
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 62 (Authorization to receive personal information for the discharge of duties) Section 76 (Declaration to the Commission required when establishing a file on individual) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Anytime a file is established concerning an individual, the public body must make a declaration to the Commission containing, among other things, the categories of persons who have access to the file in carrying on their duties.
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 35 (Protection of personal information) Section 37(1)(g) and (g.1) (Authorization to disclose personal information to officers and employees for purposes of carrying out their functions)
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	Section 24(3) (Treatment of personal information) Section 27(f) (Authorization to disclose personal information to officers and employees for purposes of carrying out their functions)
	<i>Municipal Government Act</i>	—

¹³⁴ The following are prescribed registries:

1. Cardiac Care Network of Ontario in respect of its registry of cardiac services.
2. INSCYTE (Information System for Cytology etc.) Corporation in respect of CytoBase.
3. London Health Sciences Centre in respect of the Ontario Joint Replacement Registry.
4. Canadian Stroke Network in respect of the Canadian Stroke Registry.

ELEMENT #7 – SAFEGUARDING PERSONAL DATA^{130,131}

Part 1 – General Safeguarding Requirements

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
New Brunswick	<i>Protection of Personal Information Act</i>	Schedule A and B, Principle 7 (Safeguards)
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹³⁵</i>	Section 36 (Protection of personal information) Section 39(1)(f) (Authorization to disclose personal information to officers and employees for purposes of carrying out their functions) Section 51(e) (Commissioner’s power to comment on privacy implications of using information technology in the storage of personal information)
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Section 33 (Protection of Personal Information) Section 36(1)(f) (Authorization to disclose personal information to officers and employees for purposes of carrying out their functions)
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Section 42 (Protection of Personal Information) Section 48(k) (Authorization to disclose personal information to officers and employees for purposes of carrying out their functions)
	<i>Access to Information and Protection of Privacy Regulations</i>	Section 6 (Disclosure to employees and service providers)
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Section 42 (Protection of Personal Information) Section 48(k) (Authorization to disclose personal information to officers and employees for purposes of carrying out their functions)
	<i>Access to Information and Protection of Privacy Regulations</i>	Section 6 (Disclosure to employees and service providers)

¹³⁵ Part IV to be proclaimed.

ELEMENT #7 – SAFEGUARDING PERSONAL DATA		
Part 2 - Requirement for a Privacy Impact Assessment¹³⁶		
Jurisdiction	Legislation	Privacy Legislation Concordance
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	—
	<i>Privacy Act</i>	—
British Columbia	<i>Personal Information Protection Act</i>	—
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 69(5): Public bodies which are ministries (i.e., excludes regional health authorities and hospitals) are required to conduct a privacy impact assessment for all new enactments, systems, projects or programs to determine whether the requirements of the Act are met. The privacy impact assessment must be conducted in accordance with the process/tool referenced in Schedule A attached hereto.
Alberta	<i>Health Information Act</i>	Sections 64, 70(2) and (3) and 71(2) and (3): Each custodian must prepare a privacy impact assessment and must submit it to the Information and Privacy Commissioner for review and comment before implementing any proposed administrative practices and information systems or any proposed change to any such existing practices and systems in accordance with the privacy impact assessment tool referenced in Schedule A attached hereto. Section 46(5) (Requirement for the Department to conduct a privacy impact assessment in certain situations)
	<i>Personal Information Protection Act</i>	—
	<i>Freedom of Information and Protection of Privacy Act</i>	—
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	—
	<i>The Freedom of Information and Protection of Privacy Act</i>	—
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
Manitoba	<i>The Personal Health Information Act</i>	—
	<i>The Freedom of Information and Protection of Privacy Act</i>	—
Ontario	<i>Personal Health Information Protection Act</i>	—

¹³⁶ While Canadian privacy legislation may be silent on the requirement to perform privacy impact assessments or risk vulnerability assessments, as a matter of administrative practice, many public sector entities may be required to perform privacy impact assessments in connection with the design and implementation of programs and/or systems involving the collection, use or disclosure of personal information. A list of privacy impact assessment tools developed by Canadian governmental or regulatory authorities is set out at Schedule A.

ELEMENT #7 – SAFEGUARDING PERSONAL DATA

Part 2 - Requirement for a Privacy Impact Assessment¹³⁶

Jurisdiction	Legislation	Privacy Legislation Concordance
Ontario	<i>Personal Health Information Protection Act, General Regulation</i>	Section 6(3) subparagraph 5: A person who provides goods or services for the purpose of enabling a custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to, (i) threats, vulnerabilities and risks to the security and integrity of the personal health information, and (ii) how the services may affect the privacy of the individuals who are the subject of the information.
	<i>Freedom of Information and Protection of Privacy Act</i>	—
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	—
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	—
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	—
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	—
New Brunswick	<i>Protection of Personal Information Act</i>	—
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹³⁷</i>	—
Yukon	<i>Access to Information and Protection of Privacy Act</i>	—
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	—
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	—

¹³⁷ Part IV to be proclaimed.

Schedule A

Jurisdiction	Privacy Impact Assessment Tools
Federal	Treasury Board of Canada Secretariat - <i>Privacy Impact Assessment Policy</i> (http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paigp-pefrld2_e.asp#1.Introduction)
British Columbia	Ministry of Management Services for British Columbia, Information Policy and Privacy Branch - <i>Privacy Impact Assessment (PIA) Process</i> (http://www.mser.gov.bc.ca/privacyaccess/PIA/PIAprocess.htm)
Alberta	Information and Privacy Commissioner of Alberta - <i>Privacy Impact Assessment: Instructions and Annotated Questionnaire</i> (http://www.oipc.ab.ca/ims/client/upload/pia-instructions-1.1.pdf)
Saskatchewan	Office of the Saskatchewan Information and Privacy Commissioner - <i>Privacy Impact Assessment (Short Form)</i> (http://www.oipc.sk.ca/Web%20Site%20Documents/PIA%20Short%20Form%20-%20Official%20Version%20April,%202004.pdf)
Manitoba	Ombudsman Manitoba, Access and Privacy Division - <i>Privacy Compliance Tool Checklist</i> (http://www.ombudsman.mb.ca/pdf/Final%20Version%20PCT%20Checklist%20PDF%202003-10-07.pdf) Manitoba Health - <i>Privacy Impact Assessment (PIA) Guide</i> (Not available on-line)
Ontario	Information and Privacy Commissioner/Ontario - <i>Privacy Diagnostic Tool (PDT) Workbook</i> (http://www.ipc.on.ca/userfiles/page_attachments/pdt.pdf) Management Board of Cabinet - <i>Privacy Impact Assessment Guidelines</i> (http://www.accessandprivacy.gov.on.ca/english/pia/index.html)
Quebec	Ministère des Relations avec les citoyens et de L'immigration (Québec) - <i>Modèle de pratiques de protection des renseignements personnels – dans le contexte du développement des systèmes d'information par les organismes publics</i> (http://www.aiprp.gouv.qc.ca/publications/pdf/PRP_net.pdf)
Prince Edward Island	N/A
Nova Scotia	N/A
New Brunswick	N/A
Newfoundland and Labrador	Office of the Information and Privacy Commissioner for Newfoundland and Labrador – <i>Privacy Audit, A Compliance Review Tool</i> (www.oipc.gov.nl.ca) Centre for Health Information – <i>Privacy Impact Assessment for Researchers</i> (http://www.nlchi.nf.ca/pdf/pia.pdf)
Yukon	N/A
Northwest Territories	N/A
Nunavut	N/A

ELEMENT #8 – CONTROLLING ACCESS AND DISCLOSURE OF PERSONAL DATA

Part 1 – Specific Data Matching/Linkage Provisions^{138,139}

Jurisdiction	Legislation	Privacy Legislation Concordance
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	—
	<i>Privacy Act</i>	—
British Columbia	<i>Personal Information Protection Act</i>	Section 21 - Any linkage of personal information to other information must not be harmful to the individuals and the benefits to be derived from the linkage must clearly be in the public interest.
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 35 - Any record linkage must not be harmful to the individuals and the benefits to be derived from the record linkage must clearly be in the public interest.
Alberta	<i>Health Information Act</i>	Section 1(1)(g) (Definition of “data matching”) ¹⁴⁰ Section 68 (General prohibition on data matching) Section 69 (Permitted data matching by custodians) Section 70 (Data matching between custodians; privacy impact assessment required) Sections 71 and 32 (Data matching between custodians and non-custodians; privacy impact assessment required; obligation to notify Privacy Commissioner) Section 72 (Data matching for research; obligation to comply with provisions regarding disclosure for research purposes without consent (sections 48-56)) Section 107(5) (Offence to fail to notify Commissioner)
	<i>Personal Information Protection Act</i>	—
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 42(b) - Record linkages cannot be harmful to the individuals the information is about and the benefits to be derived from the linkage must be clearly in the public interest
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	—
	<i>The Freedom of Information and Protection of Privacy Act</i>	—
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
Manitoba	<i>The Personal Health Information Act</i>	—

¹³⁸ This table cross references provisions dealing specifically with “data matching” or “data linking”. Any data linkage/matching activity involving the use and/or disclosure of personal information requires a consideration of other statutory provisions, including the consent requirements for use and disclosure of personal information for research purposes. See table of concordance for Element #3. Public institutions may also need to consider governmental administrative guidelines/policies on data matching/linkage. See, for instance, the policy of the Treasury Board of Canada Secretariat regarding data matching available at: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP2_5-2_e.asp#pre

¹³⁹ Reference should be made to the table of concordance for Element #7 which sets out safeguarding provisions, including statutory restrictions on access to personal information.

¹⁴⁰ The *Health Information Act* (Alberta) defines “data matching” as “the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, without the consent of the individuals who are the subjects of the information”.

ELEMENT #8 – CONTROLLING ACCESS AND DISCLOSURE OF PERSONAL DATA

Part 1 – Specific Data Matching/Linkage Provisions^{138,139}

Jurisdiction	Legislation	Privacy Legislation Concordance
Manitoba	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 46 - Approval must be obtained from head of the public body to use or disclose personal information for linking or matching purposes. The head may have to refer the proposal to the review committee for advice. Section 47(4) - Any information linkage, must not be likely to harm individuals and benefits to be derived from research and any information linkage must clearly be in the public interest.
	<i>Personal Health Information Protection Act, General Regulation</i>	Section 16(3) – A research plan must include a description of how personal health information will be used in the research, and if it will be linked to other information, a description of the other information as well as how the linkage will be done.
	<i>Freedom of Information and Protection of Privacy Act</i>	—
Quebec	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—
	<i>An act respecting the protection of personal information in the private sector</i>	—
Quebec	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 68.1 (Permitted data matching/Requirement for written agreement) Section 69 (Obligation to maintain confidentiality) Section 70 (Submission of data matching agreements to Commission/ Public body; Tabling of agreement in National Assembly; Obligation to publish in Gazette)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 39(b) - Record linkages cannot be harmful to the individuals the information is about and the benefits to be derived from the linkage must be clearly in the public interest.
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 29(b) - Record linkages cannot be harmful to the individuals the information is about and the benefits to be derived from the linkage must be clearly in the public interest.
Nova Scotia	<i>Municipal Government Act</i>	Section 485(4)(b) - Record linkages cannot be harmful to the individuals the information is about and the benefits to be derived from the linkage must be clearly in the public interest.
	<i>Protection of Personal Information Act</i>	—
New Brunswick	<i>Access to Information and Protection of Privacy Act¹⁴¹</i>	Section 41 - Record linkages cannot be harmful to the individuals the information is about and the benefits to be derived from the linkage must be clearly in the public interest. Section 51(e) – Commissioner may comment on implications for protection of privacy of using or disclosing personal information for record linkage.
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Section 38 - Record linkages cannot be harmful to the individuals the information is about and the benefits to be derived from the linkage must be clearly in the public interest.

¹⁴¹ Part IV to be proclaimed.

ELEMENT #8 – CONTROLLING ACCESS AND DISCLOSURE OF PERSONAL DATA**Part 1 – Specific Data Matching/Linkage Provisions^{138,139}**

Jurisdiction	Legislation	Privacy Legislation Concordance
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Section 49 - Record linkages cannot be harmful to the individuals the information is about and the benefits to be derived from the linkage must be clearly in the public interest
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Section 49 - Record linkages cannot be harmful to the individuals the information is about and the benefits to be derived from the linkage must be clearly in the public interest

ELEMENT #8 – CONTROLLING ACCESS AND DISCLOSURE OF PERSONAL DATA

Part 2 - Data-sharing Agreements for Research Purposes¹⁴²

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	Schedule 1, 4.1.3 (Organization must use contractual means to provide for comparable level of protection when personal information is being processed by a third party)
	<i>Privacy Act</i>	Section 8(2)(j) (Requirement and content of data sharing agreements)
British Columbia	<i>Personal Information Protection Act</i>	Section 21(1) (Requirement and content of data sharing agreements) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Prohibition from using personal information to contact a person to participate in the research (section 21(1)(c)).
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 35 (Requirement and content of data sharing agreements) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Prohibition from using personal information to contact a person to participate in the research.
Alberta	<i>Health Information Act</i>	Section 54(1) (Agreement between researcher and custodian) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Data sharing agreement must include obligation of recipient to pay the costs of (i) preparing information for disclosure, (ii) making copies of health information, and (iii) obtaining consents. Data sharing agreement must also contain obligation of researcher not to attempt to contact an individual who is the subject of the information in order to obtain additional information unless the individual has consented.
	<i>Health Information Regulation</i>	Section 8(4) (Additional requirements when health information is used or disclosed outside Alberta)
	<i>Personal Information Protection Act Regulation</i>	Sections 12(2), 12(3) and 14(3) (Requirement and content of data sharing agreement) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Data sharing agreement must include obligation of recipient of information to not contact any individual to whom the personal information relates, directly or indirectly, without the prior written authority of the public body and that the person must notify the public body in writing immediately if the person becomes aware that any of the conditions set out in the agreement have been breached.
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 42 (Requirement for data sharing agreement)
	<i>Freedom of Information and Protection of Privacy Regulation</i>	Section 8 (Content of data sharing agreement) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Data sharing agreement must include obligation of recipient of information to not contact any individual to whom the personal information relates, directly or indirectly, without the prior written authority of the public body and notify the public body in writing immediately if the person becomes aware that any of the conditions set out in the agreement have been breached and that, if a person fails to meet the conditions of the agreement, the agreement may be immediately cancelled and that the person may be guilty of an offence pursuant to the Act.

¹⁴² This table deals with data sharing agreements entered into specifically for research purposes. Privacy statutes may also contain a requirement to enter into written agreements for other purposes.

ELEMENT #8 – CONTROLLING ACCESS AND DISCLOSURE OF PERSONAL DATA

Part 2 - Data-sharing Agreements for Research Purposes¹⁴²

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Alberta	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	Section 29(1) (Requirement and content of data sharing agreements)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 29(2)(k) (Requirement for data sharing agreements)
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
Manitoba	<i>The Personal Health Information Act</i>	Section 24(4) (Requirement and content of data sharing agreement)
	<i>Personal Health Information Regulation</i>	Section 8.3 (Content of data sharing agreements)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 47(4)(c) and (d) (Requirement for data sharing agreements)
Ontario	<i>Personal Health Information Protection Act</i>	Section 44(1) and (5) (Requirement for data sharing agreements)
	<i>Freedom of Information and Protection of Privacy Act, General Regulation</i>	Section 10 (Content of data sharing agreements)
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	Section 21 (No requirement for data sharing agreement although the Commission may impose conditions on disclosure of information for research purposes)
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 125 (No requirement for data sharing agreement although the Commission may impose conditions on disclosure of information for research purposes)
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 39 (Requirement for data sharing agreements – no content specified)
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	Section 29 (Requirement for data sharing agreements – no content specified)
	<i>Freedom of Information and Protection of Privacy Regulations</i>	Section 9 (Content of data sharing agreement) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Data sharing agreement must include agreement of recipient not to contact any individual to whom personal information relates, directly or indirectly, without the prior written authority of the public body and to notify the public body in writing immediately if the person becomes aware that any of the conditions set out in this section have been breached. Agreement must be in prescribed form.
	<i>Municipal Government Act</i>	—

ELEMENT #8 – CONTROLLING ACCESS AND DISCLOSURE OF PERSONAL DATA

Part 2 - Data-sharing Agreements for Research Purposes¹⁴²

Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
New Brunswick	<i>Protection of Personal Information Act</i>	—
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act</i>	Section 41 (Requirement for data sharing agreements)
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Section 38 (d) (Requirement for data sharing agreements)
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Section 49 (c) and (d) (Requirement for data sharing agreements)
	<i>Access to Information and Protection of Privacy Regulations</i>	Section 8 (Content of data sharing Agreements) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Data sharing agreement must include provisions requiring: an identification of any other persons who will be given access to the personal information by the recipient; a condition that the recipient must not contact any individual to whom the personal information relates, directly or indirectly, without the prior written authority of the public body; notice to the public body in writing immediately if the person becomes aware that any of the conditions set out in the agreement have been breached; a condition that, if a recipient fails to meet the conditions of the agreement, the agreement may be immediately terminated by the public body.
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Section 49(c) and (d) (Requirement for data sharing agreements)
	<i>Access to Information and Protection of Privacy Regulations</i>	Section 8 (Content of data sharing Agreements) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Same as for the Northwest Territories

ELEMENT #9 – SETTING REASONABLE LIMITS ON RETENTION OF PERSONAL DATA		
Retention and Destruction of Personal Information^{143,144}		
Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	Schedule 1, 4.5, 4.5.2 and 4.5.3 (Limiting use, disclosure and retention) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> Data retention guidelines should include minimum and maximum retention periods.
	<i>Privacy Act</i>	Section 6 (Retention of personal information used for an administrative purpose)
	<i>Privacy Act Privacy Regulations</i>	Section 4 (Retention of personal information that has been used by a government institution for an administrative purpose) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> Personal Information shall be retained (a) for at least two years following the last time the personal information was used for an administrative purpose unless the individual consents to its disposal and (b) where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his rights under the Act. However, the information may be destroyed in an emergency in order to prevent the removal of the information from the control of the institution (section 4). A copy of every request for access received as well as a record of any information disclosed pursuant to such a request must be maintained for a period of 2 years following the date of the request (section 7).
British Columbia	<i>Personal Information Protection Act</i>	Section 35 (Retention of personal information) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> If an individual's personal information is being used to make a decision that directly affects the individual, the information must be retained for at least one year.
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 31 (Retention of personal information) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> If an individual's personal information is being used to make a decision that directly affects the individual, the information must be retained for at least one year.
Alberta	<i>Health Information Act</i>	Section 3 (Storage and Destruction, Other Enactments) Section 41 (Maintaining certain disclosure information) Section 60(2)(b) (Safeguards for proper disposal) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> A custodian that discloses a record containing individually identifying diagnostic, treatment and care information must retain that information for a period of 10 years following the date of the disclosure (section 41(2)).
	<i>Personal Information Protection Act</i>	Section 35 (Retention of information)

¹⁴³ This table sets out the statutory requirements for the general obligation in privacy legislation with respect to retention and destruction of personal information. Note that retention, return and disposal of records may be addressed in the research agreement entered into between the custodian and researcher, as required under applicable privacy legislation. Note also that under the Food and Drug Regulations – Division 5 – C.05.012 (4) records for clinical trials must be retained for 25 years.

¹⁴⁴ See statutory requirements regarding the obligation to have written policies and procedures, including for retention and destruction of personal information, in table of concordance for Element # 7.

ELEMENT #9 – SETTING REASONABLE LIMITS ON RETENTION OF PERSONAL DATA		
Retention and Destruction of Personal Information^{143,144}		
Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Alberta	<i>Freedom of Information and Protection of Privacy Act</i>	Section 35 (Accuracy and retention) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> If an individual's personal information is being used to make a decision that directly affects the individual, the information must be retained for at least one year or such shorter time as approved by the individual in writing, the public body and the body that approved the retention and disposition schedule if applicable.
	<i>Municipal Government Act</i>	Sections 214(2) and (3) (Destruction of records) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ A council may pass a bylaw respecting destruction of records and documents of the municipality. The bylaw must provide that if an individual's personal information will be used by the municipality to make a decision that directly affects the individual, the municipality must retain the personal information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.
Saskatchewan	<i>The Health Information Protection Act</i>	Section 17 (Retention and destruction policy)
	<i>The Freedom of Information and Protection of Privacy Act</i>	—
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
Manitoba	<i>The Personal Health Information Act</i>	Section 17 (Retention and destruction of information) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Written retention policy must be established. ▪ Trustee who destroys personal health information must keep a record of (i) the individual whose personal information is destroyed (ii) the time period to which the information relates, (iii) the method of destruction, and (iv) the person responsible for supervising the destruction.
	<i>Personal Health Information Regulations</i>	Section 2 (Written policy to be established)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 40 (Retention of information) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ If personal information about an individual is used to make a decision that affects the individual, the public body must establish and comply with a written policy concerning the retention of the personal information (subsections 40(1) and (2)).
Ontario	<i>Personal Health Information Protection Act</i>	Section 13 (Handling of records) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Information shall be retained for as long as necessary to allow the individual to exhaust any recourse under the Act where a request for access has been made.
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 40(1) (Retention of personal information) Section 40(4) (Disposal of personal information)

ELEMENT #9 – SETTING REASONABLE LIMITS ON RETENTION OF PERSONAL DATA		
Retention and Destruction of Personal Information^{143,144}		
Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Ontario	<i>Freedom of Information and Protection of Privacy Act, General Regulations</i>	Section 5 (Retention) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> Information shall be retained for at least one year after use, unless the individual to whom the information relates consents to its earlier disposition. The minimum period of retention of personal information contained in a telecommunications logger tape is 45 days rather than one year.
	<i>Freedom of Information and Protection of Privacy Act, Disposal of Personal Information Regulation</i>	Sections 2 to 6 (Disposal of personal information) <u>Supplemental Requirements to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> Authorization of the head of the institution must authorize the destruction of the information. The head shall ensure that the institution maintains a disposal record setting out what personal information has been destroyed and the date.
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	Section 30(1) (Retention of personal information) Section 30(4) (Disposal of personal information)
	<i>Municipal Freedom of Information and Protection of Privacy Act, General Regulation</i>	Section 5 (Retention of personal information) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> Personal information to be retained for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, unless the individual to whom the information relates consents to its earlier disposal.
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	Section 12 (Use of file) Section 36 (Retention where request for access or rectification has been denied)
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 73 (Destruction) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> Section 73 does not apply to the processing of personal information collected and used as a working tool by a natural person and which is used by him for scientific research purposes to the extent that the information is not disclosed to any person other than the person concerned or to a body other than that to which he belongs, and that it is used judiciously (section 78).
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 33 (Retention when information is used to make a decision) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> If an individual's personal information is being used to make a decision that directly affects the individual, the information must be retained for at least one year.
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	Section 24(4) (Treatment of personal information) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> If an individual's personal information is being used to make a decision that directly affects the individual, the information must be retained for at least one year.

ELEMENT #9 – SETTING REASONABLE LIMITS ON RETENTION OF PERSONAL DATA		
Retention and Destruction of Personal Information^{143,144}		
Jurisdiction	Legislation	Privacy Legislation Concordance and Selected Supplemental Requirements
Nova Scotia	<i>Municipal Government Act</i>	Section 483(4) (Retention of personal information) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Where a municipality uses an individual's personal information to make a decision that directly affects the individual, the municipality shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.
New Brunswick	<i>Protection of Personal Information Act</i>	Schedule A, Principle 5 and Schedule B, Principle 5 (Limiting use, disclosure and retention)
Newfoundland	<i>Access to Information and Protection of Privacy Act¹⁴⁵</i>	Section 37 (Retention of personal information) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ If an individual's personal information is being used to make a decision that directly affects the individual, the information must be retained for at least one year.
Yukon	<i>Access to Information and Protection Privacy Act</i>	Section 34 (Retention of personal information) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Public body must retain information it uses to make a decision affecting an individual for at least one year after such use.
Northwest Territories	<i>Access to Information and Protection Privacy Act</i>	Section 44 (Duties of public body) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Public body must retain information it uses to make a decision affecting an individual for at least one year after such use.
Nunavut	<i>Access to Information and Protection Privacy Act</i>	Section 44 (Duties of public body) <u>Supplemental Requirement to CIHR Privacy Best Practices:</u> <ul style="list-style-type: none"> ▪ Public body must retain information it uses to make a decision affecting an individual for at least one year after such use.

¹⁴⁵ Part IV to be proclaimed.

ELEMENT #10 – ENSURING ACCOUNTABILITY AND TRANSPARENCY IN THE MANAGEMENT OF PERSONAL DATA

Part 1- Accountability and Transparency¹⁴⁶

Jurisdiction	Legislation	Privacy Legislation Concordance
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	Schedule 1, 4.1 (Accountability) Schedule 1, 4.8 (Openness)
	<i>Privacy Act</i>	Sections 10 and 11 (Obligations regarding personal information banks)
British Columbia	<i>Personal Information Protection Act</i>	Section 4 (Compliance with the Act) Section 5 (Policies and Procedures)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 2 (Purposes of this Act) Section 69(2) and (3) (Personal information directory of ministries) Section 69(5) (Duty of a ministry to prepare privacy impact assessment) Section 69(6) (Directory of personal information banks to be maintained by public body that is not a ministry) Section 70 (Policy manuals to be made available)
Alberta	<i>Health Information Act</i>	Section 2 (Purposes of the Act) Section 62 (Duty to identify responsible affiliate) Section 63 (Duty to establish or adopt policies and procedures) Section 64 (Duty to prepare privacy impact assessment) Section 66(6) (Accountability for information disclosed to an information manager)
	<i>Health Information Regulation</i>	Section 8(2) (Designating responsible individual) Section 8(6) (Custodian responsible for affiliates' compliance)
	<i>Personal Information Protection Act</i>	Section 5 (Compliance with Act) Section 6 (Policies and Procedures)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 2 (Purposes of this Act) Section 87 (Directory of public bodies) Section 87.1 (Directory of personal information banks) Section 88 (Records available without request) Section 89 (Access to manuals)
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	Preamble (Accountability obligations) Section 9 (Right to be informed)
	<i>Freedom of Information and Protection of Privacy Act</i>	Section 64 (Directory to be produced) Section 65 (Access to manuals)
	<i>Local Authority Freedom of Information and Protection of Privacy Act</i>	Section 53 (Directory of local authorities including place at which applications for access to records should be made for each)
Manitoba	<i>The Personal Health Information Act</i>	Section 2 (Purposes of this Act) Section 25(5) (Information transferred to information manager for processing deemed to be maintained by the transferring trustee)

¹⁴⁶ This table cross references statutory provisions regarding the general accountability and transparency requirements set out in privacy legislation. Privacy legislation also provides individuals with a right of access to their personal information, which this table does not address. Also, privacy legislation may provide that the body/organization must inform the relevant regulatory authority before personal information may be used or disclosed for research purposes. Such requirements have been referenced in the table of concordance for Element #3.

ELEMENT #10 – ENSURING ACCOUNTABILITY AND TRANSPARENCY IN THE MANAGEMENT OF PERSONAL DATA

Part 1- Accountability and Transparency¹⁴⁶

Jurisdiction	Legislation	Privacy Legislation Concordance
Manitoba	<i>Personal Health Information Regulation</i>	Section 2 (Written security policy and procedures) Section 6 (Orientation and training of employees)
	<i>The Freedom of Information and Protection of Privacy Act</i>	Section 2 (Purposes of this Act) Sections 75(1) and (2) (Directory to be maintained) Section 75(3) (Obligations regarding personal information bank) Section 76 (Records to be made available)
Ontario	<i>Personal Health Information Protection Act¹⁴⁷</i>	Section 10 (Information Practices) Sections 15 to 17 (Accountability and Openness)
	<i>Personal Health Information Protection Act, General Regulation</i>	Sections 6(3) subparagraph 2 (Health information network provider to provide plain language description of services provided and safeguards in place to protect against unauthorized use and disclosure) Sections 6(3) subparagraph 3 (Information to be made available to the public by health information network provider) Sections 6(3) subparagraph 4 (Information to be made available to health information custodians) Sections 6(3) subparagraph 5 (Health information network provider to perform assessment of risks to security and integrity of personal health information in providing services and detailing affect on privacy)
	<i>Freedom of Information and Protection of Privacy Act</i>	Sections 31 to 36 (Information to be published or available) Sections 44 to 46 (Obligations regarding Personal Information Banks)
	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	Section 1 (Purposes of this Act) Section 24 (Publications of information re institutions) Section 25 (Information available for inspection) Section 26 (Head shall make annual report) Section 34 (Obligations re personal information bank index)
	<i>Municipal Freedom of Information and Protection of Privacy Act, General Regulation</i>	Section 4(2) (Where notice re collection of personal information has not been given, the head shall make available for public inspection a statement describing the purpose of the collection of personal information and the reason that notice has not been given)
Quebec	<i>An act respecting the protection of personal information in the private sector</i>	Section 17 (Accountability for information disclosed outside Quebec)
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	Section 67.3 (Register to be kept of every disclosure of personal information) Section 71 (Personal information files must be established) Section 76 (Declaration to the Commission required when establishing a file on individual)
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	Section 2 (Purposes of this Act) Section 73 (Records available without request)
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	Section 2 (Purposes of this Act) Section 48 (Directory respecting records of public body)
	<i>Municipal Government Act</i>	Section 462 (Purpose of this Part)

¹⁴⁷ Note that the privacy practices and procedures of entities prescribed for the purposes of section 45 and 39(1)(c) of the Act, as well as health data institutes, must be approved by the Information and Privacy Commissioner.

ELEMENT #10 – ENSURING ACCOUNTABILITY AND TRANSPARENCY IN THE MANAGEMENT OF PERSONAL DATA

Part 1- Accountability and Transparency¹⁴⁶

Jurisdiction	Legislation	Privacy Legislation Concordance
New Brunswick	<i>Protection of Personal Information Act</i>	Schedule A, Principle 1 (Accountability) Schedule A, Principle 8 (Openness)
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹⁴⁸</i>	Section 3 (Purpose) Section 67(1)(c) (Designation and delegation by the head of public body) Section 69 (Directory of information)
Yukon	<i>Access to Information and Protection of Privacy Act</i>	Section 1(1) (Purpose of the Act) Section 63 (Information Directory) Section 64 (Records available without request)
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	Section 1 (Purpose of this Act) Section 70 (Directory of public bodies and records) Section 71 (Policy manuals must be made available to the public) Section 72 (Records available without request)
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	Section 1 (Purpose of this Act) Section 70 (Directory of public bodies and records) Section 71 (Policy manuals must be made available to the public) Section 72 (Records available without request)

¹⁴⁸ Part IV to be Proclaimed

ELEMENT #10 – ENSURING ACCOUNTABILITY AND TRANSPARENCY IN THE MANAGEMENT OF PERSONAL DATA

Part 2 - Statutory References to Research Ethics Board¹⁴⁹

Jurisdiction	Legislation	Privacy Legislation Concordance
Federal	<i>Personal Information Protection and Electronic Documents Act</i>	—
	<i>Privacy Act</i>	—
British Columbia	<i>Personal Information Protection Act</i>	—
	<i>Freedom of Information and Protection of Privacy Act</i>	—
Alberta	<i>Health Information Act</i>	Section 27(1)(d) (Approval of Ethics Committee) ¹⁵⁰ Section 50 (Role of Ethics Committee)
	<i>Personal Information Protection Act Regulation</i>	Section 14(3) (Approval of Research Ethics Review Committee)
	<i>Freedom of Information and Protection of Privacy Act</i>	—
	<i>Municipal Government Act</i>	—
Saskatchewan	<i>The Health Information Protection Act</i>	Section 29(2)(ii) (Approval of research ethics committee)
	<i>The Freedom of Information and Protection of Privacy Act</i>	—
	<i>The Local Authority Freedom of Information and Protection of Privacy Act</i>	—
Manitoba	<i>The Personal Health Information Act</i>	Section 24 (Approval of health information privacy committee and institutional research review committee)
	<i>Personal Health Information Regulation</i>	Section 8.1 (Functions of health information privacy committee)
	<i>The Freedom of Information and Protection of Privacy Act</i>	—
Ontario	<i>Personal Health Information Protection Act</i>	Section 44(1) (Approval of Research Ethics Board) Section 44(3) and (4) (Considerations and Decisions of Research Ethics Board)
	<i>Freedom of Information and Protection of Privacy Act</i>	—

¹⁴⁹ This table cross references the statutory provisions to research ethics bodies. Note that while Canadian privacy statutes may be silent with respect to ethics boards or committees, there is a requirement under many public sector statutes for research to be approved by the head or the Minister in charge of the administration of the particular statute. Refer to table of concordance for Element # 3 regarding statutory conditions that research ethics bodies or other approving bodies/persons must consider before allowing the use or disclosure of personal information without consent for research purposes.

¹⁵⁰ The following committees and boards are designated as ethics committees by the Health Information Act Designation Regulation:

- Alberta Cancer Board – Research Ethics Committee
- College of Physicians and Surgeons of Alberta – Research Ethics Review Committee;
- Alberta Heritage Foundation for Medical Research – Community Health Ethics Research Review Committee;
- University of Alberta – Health Research Ethics Board;
- University of Calgary – Conjoint Health Research Ethics Board;
- University of Lethbridge – Human Subject Research Committee

ELEMENT #10 – ENSURING ACCOUNTABILITY AND TRANSPARENCY IN THE MANAGEMENT OF PERSONAL DATA

Part 2 - Statutory References to Research Ethics Board¹⁴⁹

Jurisdiction	Legislation	Privacy Legislation Concordance
Ontario	<i>Municipal Freedom of Information and Protection of Privacy Act</i>	—
Quebec¹⁵¹	<i>An act respecting the protection of personal information in the private sector</i>	—
	<i>An act respecting access to documents held by public bodies and the protection of personal information</i>	—
Prince Edward Island	<i>Freedom of Information and Protection of Privacy Act</i>	—
Nova Scotia	<i>Freedom of Information and Protection of Privacy Act</i>	—
	<i>Municipal Government Act</i>	—
New Brunswick	<i>Protection of Personal Information Act</i>	—
Newfoundland and Labrador	<i>Access to Information and Protection of Privacy Act¹⁵²</i>	—
Yukon	<i>Access to Information and Protection of Privacy Act</i>	—
Northwest Territories	<i>Access to Information and Protection of Privacy Act</i>	—
Nunavut	<i>Access to Information and Protection of Privacy Act</i>	—

¹⁵¹ Article 21 of the Quebec Civil Code states that research may be conducted involving minors and incapacitated adults only with the approval and monitoring of an ethics committee. Ethics committees are formed or designated by the Minister of Health and Social Services.

¹⁵² Part IV to be Proclaimed