




An EU-Canada joint infrastructure
for next-generation multi-Study Heart research

Deliverable D1.2

Policy “Points to Consider” tool to guide research projects, policy makers

Reference	D1.2_euCanSHare_MCG_30112020
Lead Beneficiary	McGill University
Author(s)	Bartha Maria Knoppers, Alexander Bernier
Dissemination level	Public
Type	Report
Official Delivery Date	November 30 th 2020
Date of validation by the WP Leader	24/11/2020
Date of validation by the Coordinator	25/11/2020
Signature of the Coordinator	





Version Log

Issue Date	Version	Involved	Comments
19/11/2020	1	Alexander Bernier, Bartha Maria Knoppers	First draft
23/11/2020	2	Katharina Heil, Karim Lekadir	First feedback
24/11/2020	3	Alexander Bernier, Bartha Maria Knoppers	Final revision
25/11/2020		Katharina Heil, Karim Lekadir	Revised and corrected final version.

Executive Summary

The Centre of Genomics and Policy at McGill University has conducted an analysis of the ethico-legal requirements enshrined in data privacy law and research ethics guidance in Canada and the European Union. This Points-to-Consider document is intended to synthesize the elements of that research that are of relevance to the secondary use of health data by the cohorts of the euCanSHare project.

In this summary, we have provided a general overview of our research. In Part 1, we assess the sources of the ethico-legal requirements discussed. In Part 2, we consider a number of regulatory requirements in the laws of Canada and the European Union. Elements discussed include legal prerequisites to data use, individual rights in data, and prerequisites to the international transfer of data. In Part 3, the identifiability of data, and the use of safeguards to protect data, are considered. In Part 4, the foregoing ideas are synthesized into holistic proposals for data governance.

The conclusions of this Points-to-Consider document reprise the contents of recent and forthcoming academic publications that elaborate our findings in further detail.



Table of Contents

1	Ethico-Legal Data Governance Requirements	4
1.1.	Sources and Structure	4
1.2.	Research Ethico-Legal Requirements	4
2	Data Privacy Requirements in Canada and the European Union	5
2.1.	Principles Governing the Use of Personal Data	5
2.2.	Common Consent Provisions in Canadian Law	6
2.3.	Canada: Individual Rights in Personal Data	6
2.4.	Principal Provisions of European Data Privacy Laws	6
2.5.	European Union: Individual Rights in Personal Data	7
2.6.	Transfers of Data from the European Union	7
3	Data Safeguards and Data Anonymization	8
3.1.	Safeguarding Data in Canada and the European Union	8
3.2.	Data Anonymization in Canada and the European Union	8
4	Data Governance Considerations	9



1 Ethico-Legal Data Governance Requirements

1.1. Sources and Structure

Both Canada and the European Union have adopted data privacy laws that can create challenges for the inter-institutional and international sharing of personal data.

In Canada, the applicable data privacy laws vary depending on the province in which an institution is established, and the commercial or non-commercial nature of its activities. The nature of the entity also affects which legislation is applicable. Private sector entities, federal public sector entities, provincial public sector entities, and health sector entities can be regulated by different statutes.

In the European Union and the European Economic Area, the General Data Protection Regulation (GDPR) generally applies to the use of personal data. Certain provisions of the GDPR are applicable to all entities established in the European Economic Area, and others are susceptible to differing implementations in different Member States of the European Union.

Moreover, in Canada and in the European Union, entities sharing personal data outside of Canada or those sharing personal data outside of the European Union can be required to comply with additional requirements to safeguard the rights of the individuals concerned by the data. This includes requiring entities transferring data to show evidence of a justification in law for the international transfer of data, or to use contractual safeguards or other measures to protect the integrity of data.

1.2. Research Ethico-Legal Requirements

In Canada and the European Union, researchers performing primary research involving human participants, or undertaking the secondary use of identifiable data for research purposes, are generally required to comply with applicable legal and ethical requirements. Inter alia, these include obtaining research ethics consent and/or demonstrating a lawful basis for the use of personal data according in accordance with local data privacy law.

It is generally required to obtain consent to either collect personal data from individuals for research purposes, or for their secondary use. The approval of a research ethics committee for the collection and use of personal data is also a general requirement. If researchers intend to share data with other researchers using a central platform, consent to the storage of data in a centralized database should be obtained.

If researchers intend to use previously collected data for new purposes, it is generally necessary to ensure that the original research consent provides for such research purposes. Indeed, for research uses that are not anticipated by applicable research ethics consents, a new consent may be required. If obtaining new consent is impossible or impracticable, an ethics waiver of consent from a research ethics board should be sought.

Researchers have an ongoing obligation to allow individuals to withdraw their consent where possible (if not published or already used). Withdrawal may lead to the destruction of such data. Further, researchers can sometimes be required by law to inform individuals of incidental (i.e. secondary) findings that are medically actionable, that is, for conditions where treatment or prevention are available.



2 Data Privacy Requirements in Canada and the European Union

2.1. Principles Governing the Use of Personal Data

Both Canadian data privacy laws and the GDPR require compliance with certain principles that ensure data privacy or data protection. The articulation of these principles differs slightly in Canada and in the European Union, however, they generally reflect the Fair Information Practice Principles (FIPPs) or the 1980 OECD Privacy Principles, restated here.

These principles are expressed as follows in the GDPR:

1. Lawfulness, fairness, and transparency.
2. Purpose limitation.
3. Data minimization.
4. Accuracy.
5. Storage limitation.
6. Integrity and confidentiality (security).
7. Accountability.

The principles are expressed as follows in the CSA Model Code, which is replicated in certain Canadian data privacy laws, and captured in the substantive contents of others:

1. Accountability.
2. Identifying Purposes.
3. Consent.
4. Limiting Collection.
5. Limiting Use, Disclosure, and Retention.
6. Accuracy.
7. Safeguards.
8. Openness.
9. Individual Access.
10. Challenging Compliance.

Despite their differing articulation, these principles generally function similarly. Compliance with these principles requires entities using data to be transparent regarding their uses of data and to hold the data to a high standard of security both in their hands and in the hands of third parties. These principles also require entities using data to clearly delineate the purposes of their data collection and data uses, and to refrain from collecting additional data, or using previously collected data for further purposes, absent justification. Last, these principles require that individuals be made aware of the use of their data and have the opportunity to exercise their rights relative to the data (i.e. to access their data, or to request the rectification thereof), or exercise recourses relative thereto.



2.2. Common Consent Provisions in Canadian Law

Canadian laws generally require the informed consent of the concerned individuals to collect, use, or disclose their personal data. Such consent can usually be express or implied. Unless otherwise foreseen, for health data, the consent must usually be express.

Justifications in law do exist, however, to collect, use, or disclose health data without individual consent. For instance, as previously discussed, such a consent requirement can be waived in the research context subject to the approval of a research ethics board, or the approval of the relevant health data custodian.

Health data can be collected, used, or disclosed for certain purposes without individual consent. For instance, this can be done to perform quality assurance/improvement activities. Public sector entities have broad powers to use personal data for secondary purposes so long as the benefits outweigh the potential risks. Further, such data can also be used for public health purposes, to prevent harm to an individual or a group, or to provide clinical care to the individual concerned by the data.

2.3. Canada: Individual Rights in Personal Data

Once data has been collected and used in compliance with the law, individuals nonetheless retain ongoing rights in their personal data. Individuals can request access to their personal data and can withdraw their consent to the continued collection and use of their personal data. If errors are present in an individual's personal data, they have the right to request the rectification thereof.

Individual requests relating to their personal data must generally be complied with within thirty days. Usually, entities are required to comply with such requests. However, entities can refuse to grant an individual access to their personal data if doing so would compromise the privacy of a third person, or otherwise conflict with select legally protected interests. Requests can also be denied if it is impossible or impracticable to comply with a person's request because their data cannot be located, or because compliance would require the expenditure of too many resources.

2.4. Principal Provisions of European Data Privacy Laws

The GDPR applies to entities established in the European Union that process data on their own behalf, or that make determinations about how other entities will use personal data. The GDPR also applies to certain entities that are not established in the European Union but offer services to persons in the EU or monitor the behavior of persons in the EU. These categories of entities are referred to as controllers.

The GDPR also imposes more limited obligations on entities that process data on the behalf of others, without making determinations about how other entities will use personal data. These entities are referred to as processors.

In the European Union, it is generally required to demonstrate a lawful basis to process the personal data of individuals. Lawful bases include processing data on the basis of consent, on the basis of the controller's legitimate interests, to protect the vital interests of an individual, or for the performance of a task carried out in the public interest. A second lawful basis can also be required to process special category data, such as biometric data, health data or genetic data. Examples of lawful bases for the processing of special category data include processing of data



on the basis of explicit consent, the processing of data manifestly made public by the individual concerned, or data that is necessary for reasons of substantial public interest. Furthermore, an additional justification in law can be required to transfer the personal data of individuals to a destination outside of the European Union and European Economic Area.

2.5. European Union: Individual Rights in Personal Data

According to the GDPR, individuals have the right to be informed that their data is being processed. Individuals further have rights to access their data or to demand the rectification of errors in their data. In certain circumstances, individuals also have the right to demand the erasure of their data, to restrict the further processing of their data, to request copies of the personal data that concerns them, or to object to their further processing of their data.

The rights of individuals can be subject to certain limits, including those established in Member State law. The rights of individuals can also be subject to certain limitations if the entity using the data is not able to determine their identity for the purposes of honoring their rights in data.

2.6. Transfers of Data from the European Union

Transfers of data outside of the EU can be presumed lawful if the country, territory, or organization that receives the data is subject to an 'adequacy decision' issued by the European Commission.

Canada is subject to an adequacy decision. However, the adequacy decision concerning Canada only applies to entities governed by the federal private-sector law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Therefore, most health sector entities will not be included in the ambit of the adequacy decision.

Transfers of personal data outside of the European Union not based on an adequacy decision issued by the European Commission can be performed based on other appropriate arrangements established in the GDPR. Presently, such arrangements only include the use of the standard contractual clauses approved by the European Commission in the contract governing the transfer of data. The use of such clauses may prove impracticable to transfer data to certain jurisdictions, such as the United States, as many research institutions are subject to national laws that prevent them from incorporating certain terms of the standard contractual clauses to their contracts.

Last, certain justifications are available for transfers performed on an exceptional basis. Such transfers can be performed, for instance, if the transfer is made for important reasons of public interest, or if the individual concerned by the data has provided explicit consent to the transfer.

Recent decisions of the Court of Justice of the European Union, *Schrems I* and *Schrems II*, require entities transferring data outside of the EEA to independently assess the legal regime of recipient countries (essential equivalence test). Researchers must determine that such laws can ensure the continued protection of the fundamental rights of citizens of the European Union prior to transferring data to external jurisdictions.

This complex legislative structure requires data users to demonstrate two or even three lawful bases to process or transfer personal health data. Further, an onerous burden is placed on health researchers intending to share personal health outside of the EEA, who must assess the contents of the recipient jurisdiction's legal regime. Consequently, transferring health data outside of the European Union can impose a proscriptive legal compliance burden on researchers.



3 Data Safeguards and Data Anonymization

3.1. Safeguarding Data in Canada and the European Union

In Canada and the European Union, entities using data are generally required to ensure that the data is kept secure. The specific measures required are often left to appreciation of the entities responsible for the use of the data.

Examples of safeguards for data can include the requiring the encryption of data, ensuring that data access systems and retain auditable records of uses made. Keeping the computers used to access or manipulate data in a locked area is a common safeguard. Retaining specialized staff to address data privacy challenges and respond to the queries of individuals about the use of their data is another.

It is generally accepted that the safeguards adopted must account for the sensitivity of the personal data concerned. Consequently, health data have often been understood by regulators to require more onerous safeguards than other categories of data.

Safeguards for personal data are also often understood to require the implementation of physical, technological, and organizational measures. Further, safeguards must account for the destruction of data at the end of the data's lifecycle and be incorporated to staff training.

Data privacy laws in Canada and the European Union impose a number of other compliance obligations regarding the use of data, such as the obligation to retain records about the data held and the uses made thereof.

3.2. Data Anonymization in Canada and the European Union

If data is not identifiable, it is considered to be anonymized and is therefore not subject to the application of data privacy legislation or research ethics guidance.

In both Canada and the European Union, data identifiability is generally assessed contextually, with an appreciation for the circumstances in which the data is used. The data is considered identifiable if there exists a reasonably foreseeable risk that the individual concerned by the data can be identified.

In Canada, a dataset is generally considered to be anonymized if the risk that any individual record comprised in the dataset will be re-identified is below five percent. The analysis is holistic and accounts for all methods that could be used to perform re-identification, including illicit or accidental re-identification. In Canada, data is considered to relate to an individual if it relates to an individual in its content.

In the European Union, data is generally considered to be anonymized if there exists no means for a controller, processor, or reasonably proximate third party to perform the reidentification of the concerned individual. Reasonable means are given a broad interpretation. Consequently, data may often be considered identifiable unless it is practically impossible to perform the re-identification of the individual concerned.

In the European Union, data is considered to relate to an individual if it relates to an individual in its content. It is also considered to be personal data if it is processed for the purpose of affecting an individual's interests, or if the use thereof has the effect of influencing an individual's interests. For these reasons, the concept of personal data in the European Union is broader than it is in Canada.

If a biomedical consortium can anonymize its data, then it is possible to share and reuse the data with considerable flexibility without being subject to a rigorous legal compliance burden. The



anonymization of data can nonetheless have negative effects on ongoing health data utility or scientific quality that would preclude the adoption of such a strategy in many cases.

4 Data Governance Considerations

Both Canada and the European Union have a data privacy legislation that demonstrates a common structure subject to differing implementations according to context. It can be challenging to adopt a single policy for pan-Canadian or pan-European data governance because of the significant discrepancies in territorial or sectoral implementations of data privacy law. These difficulties are amplified by ambiguities as to the content of data privacy legislation, and interpretive disagreement relating thereto.

To create holistic data governance practices for an international health data sharing consortium across Canada and the European Union, it is a recommended best practice to adopt consortium-wide policies regarding anticipated data storage and data access procedures, and to allow participating researchers to tailor their compliance thereto with the specific legal requirements of their local institution and local regulatory requirements.

The use of a mature data governance infrastructure can be helpful in doing so. For instance, this can include the adoption of consortium-wide oversight bodies including an executive committee that includes representation from the different regions participating in the cohort. If possible, data should remain under the oversight of a singular data access committee responsible for evaluating and acceding requests to personal data according to common consortium policies.

If data cannot be submitted to common oversight, it is practicable to create a network for researchers from participating institutions to share data and access proposals amongst themselves. Each exchange of data is then subject to the verification by a local data custodian. However, such an approach creates challenges to the fluid movement of data among participating institutions. Further, it is not clear that this creates any real advantages in data privacy or data security, as local institutions generally do not have the specialized personnel required to assess the risks inherent in a proposed data use. The networked approach can consequently result in the duplication of compliance processes across multiple institutions, and the frustration of data sharing and data harmonization efforts.

Note: On Nov. 17th, the Canadian government introduced a new bill, entitled *Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts (Digital Charter Implementation Act)*.

If implemented, the law will replace much of Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) with the *Consumer Privacy Protection Act*. The new law will apply to organizations in Canada in the use of personal information in the course of their commercial activities. The new law will modify many provisions of PIPEDA, including turning Canada's privacy principles into codified obligations and creating a number of new purposes for which organizations can use personal information without individual consent.