

DECLARATION OF PERSONAL HEALTH DATA RIGHTS IN CANADA

PURPOSE & INTENT:

The Declaration of Personal Health Data Rights in Canada is a future-looking and living document, informed by its global context. It acknowledges the boundaries set by existing health information and privacy laws across Canada plus other mechanisms such as Research Ethics Boards (REBs), with the expectation that laws, REBs, and organizations will move towards the spirit of this Declaration.

The Declaration aims to build consensus among patients, citizens, and groups representing them, create awareness, spur conversations, and inform policies and decision-making. It seeks to promote the equal importance of both privacy and sharing.

BACKGROUND:

- I. People own their personal health data¹ while custodians of those data own the records.² The Supreme Court of Canada established this as legal fact in 1992 when they found that:

“Information about oneself revealed to a doctor acting in a professional capacity remains, in a fundamental sense, one’s own. While the doctor is the owner of the actual record, the information is held in a fashion somewhat akin to a trust and is to be used by the physician for the benefit of the patient. The confiding of the information to the physician for medical purposes gives rise to an expectation that the patient’s interest in and control of the information will continue.”³

- II. Since people own their personal health data and their “interest in and control of the information will continue”, people must be able to access their personal health data to be able to exercise control over it on an ongoing basis. Individuals need to be able to control the accuracy of the data, to be able to consent to their data being processed and shared for different purposes, and to access complete and useable copies of their data.

A steward is anyone who holds personal health data, including—but not limited to—health and social service providers, corporations, government agencies, researchers, and non-profit organizations.

¹ “Personal health data” mean “personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about their health status. This includes genetic data.” (Modified from GDPR definition found: <https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation>) (Accessed October 22, 2020) ² “Records” mean “a compilation of data covering aspects of an individual’s physical, mental, and social health” whether they be hard copies (e.g. paper) or electronic (e.g. software application). (Modified from “health record.” Medical Dictionary for the Health Professions and Nursing. 2012. Farlex 23 Feb. 2021 <https://medical-dictionary.thefreedictionary.com/health+record>) (Accessed February 23, 2021) ³ *McInerney v. MacDonald*, [1992] 2 S.C.R. 138 <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/884/index.do> (Accessed May 20, 2020) ⁴ “Access” means “the right or opportunity to reach, use, or visit.” Access implies no barriers including but not limited to ability to pay, technology, connectivity, literacy to use or interpret. (Concise Oxford Dictionary of Current English. Ninth Edition. Oxford: Clarendon Press. 1995. Page 8.) ⁵ “Processing” means “any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” (GDPR definition from <https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation>) (Accessed October 22, 2020)

✓As explained by Brian Beamish, former Information and Privacy Commissioner

The office of Ontario states: “The right of access to one’s own records of personal information, including records of personal health information, is a cornerstone of fair information practices and a fundamental tenet of all privacy legislation. The right of an individual to access his or her records is essential to the exercise of other statutory and common law rights, including the right of an individual to determine for himself or herself what shall or shall not be done with his or her own body, the right of an individual to ‘informational self-determination’ and the right of an individual to require the correction or amendment of personal health information about themselves. It is also vital in ensuring continuity of care, for example, where an individual has decided to seek health care from another health care provider.”⁶

III. Since people own their personal health data, they have corresponding rights, including the right of access, over the personal health data they provide to service providers, non-profit organizations, governments, researchers, and corporations for a range of purposes related to their health and to health care.

✓The European Union’s General Data Protection Regulation (GDPR) established in 2018 the most current legislative thinking on people’s data rights arising from their data ownership.⁷ To the list of rights created by the GDPR⁸, five more rights were added to this document: the right to consent, the right to de-identification⁹, the right to benefit, the right to security, and the right to engagement.

✓This document is limited in its scope to focus on individual personal health data rights. In the context of First Nations, Métis, and Inuit health data, the collective principles of Ownership Access Control and Possession (OCAP)¹⁰, Ownership Access Control and Stewardship (OCAS), and Inuit Qaujimajatuqangit (IQ) apply.¹¹

IV. Since a variety of stakeholders, such as governments, health care providers, researchers, corporations, and clinicians, need to process, share, and link health data sets to generate evidence for a variety of purposes, including those that support individual and public health, people have a right to benefit¹² from the processing or sharing of their personal health data for research or any other purposes. To benefit, people recognize the importance of sharing their personal health data, while recognizing stewards’ duty to respect, protect, and fulfill personal health data rights. ¹³

6 Information and Privacy Commissioner of Ontario. Order HO-009. October 2010. <https://decisions.ipc.on.ca/ipc-cipvp/hipa/en/135119/1/document.do> (Accessed June 1, 2020) 7 Information and Privacy Officer of Ontario. Privacy Fact Sheet: General Data Protection Regulation. July 2018. <https://www.ipc.on.ca/wp-content/uploads/2018/07/fs-privacy-gdpr.pdf> (Accessed May 20, 2020) 8 The list of GDPR rights are: to be informed; to access and correction; to data portability; to object to processing; to restrict processing; to complain; and to erasure. (Ibid.) 9 “De-identification” means “the process of removing personal data from a record or data set” (from <https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf>) (Accessed October 22, 2020) 10 OCAP® is a registered trademark of the First Nations Information Governance Centre (FNIGC) <https://fnigc.ca/ocap-training/> (Accessed September 3, 2020) 11 University of Manitoba, Faculty of Health Sciences. Framework for Research Engagement with First Nation, Metis, and Inuit Peoples. Page 14. https://umanitoba.ca/faculties/health_sciences/medicine/media/UofM_Framework_Report_web.pdf (Accessed September 9, 2020) 12 “Benefit” means “something that produces good or helpful results or effects or that promotes well-being” (Merriam-Webster online dictionary <https://www.merriam-webster.com/dictionary/benefit>) 13 This takes its inspiration from the Caldicott Principles. The UK Caldicott Guardian Council. A Manual for Caldicott Guardians. The Caldicott Principles. <https://www.ukcg.org.uk/manual/principles> (Accessed October 22, 2020)

DECLARATION OF PERSONAL HEALTH DATA RIGHTS IN CANADA:

1

Right to be informed: Individuals must receive formal notice prior to the collection of their personal health data. Individuals have the right to be informed, using concise, accessible, plain language¹⁴, about how a custodian will be processing or commercializing¹⁵ their personal health data. The steward must provide the individual with information, including:

- the identity and contact details of the steward,
- the intended purposes of processing or commercializing the data,
- the legal basis for processing or commercializing the data,
- who will receive the data,
- where and how their data are stored,
- how long the data will be retained,
- how the data will be protected, and
- their personal health data rights.

2

Right to consent: Individuals have the right to consent, and withdraw consent, to the processing or commercialization of their personal health data. Different intended purposes require different¹⁶ degrees of consent, either implied consent¹⁶ or express consent¹⁷.

Health care provision, including the circle of care

Because accurate and timely information is important for patient safety and optimal outcomes, consent is implied. Since patients are an active member of and participant in the circle of care they define, it is imperative that they have access to all information about them and that they contribute to that information.

¹⁴ “Plain language” means “communication your audience can understand the first time they read it.” This includes communicating in different languages and/or formats based on the needs of the individual. (from <https://plainlanguage.gov/about/definitions/>) (Accessed October 22, 2020)

¹⁵ “Commercialize” means “to organize something to make a profit” (from the online Cambridge English Dictionary

<https://dictionary.cambridge.org/dictionary/english/commercialize>) (Accessed April 29, 2021)

¹⁶ “Implied consent” means “the assumption that a person has given permission for an action, which is inferred from his or her actions, rather than expressly or explicitly provided” (from the Legal Dictionary <https://legaldictionary.net/implied-consent/>) (Accessed April 29, 2021)

¹⁷ “Express consent” means “a clear and voluntary indication of choice, usually oral or written, and freely given in circumstances where the available options and their consequences have been made clear” (from Segen’s Medical Dictionary

<https://medical-dictionary.thefreedictionary.com/express+consent>) (Accessed April 29, 2021)

¹⁸ “Circle of care” means “a group of providers caring for a patient who need to know information to provide that care, plus the patient themselves and any caregivers designated by the patient” (based on the Canadian Medical Protective Association definition https://www.cmpa-acpm.ca/serve/docs/ela/goodpracticesguide/pages/communication/Privacy_and_Confidentiality/circle_care-e.html) (Accessed August 19, 2020)

Research for public benefits¹⁹ — using de-identified data

Where necessary and proportionate²⁰ data sharing and analysis of de-identified data are being undertaken for public benefits, implied consent is sufficient. If the purposes at any point include commercializing personal health data, express consent becomes required. Individuals can choose to withdraw their consent at any time, with their data no longer being shared or used from the point of their withdrawal of consent forward.

Research — using identifiable data

Research for any purpose that requires identifiable data must ensure an individual provides express consent using information that is plain language and accessible based on the needs of the individual giving consent. An individual can withdraw their consent at any time.

Commercial purposes

Any purposes involving the commercialization of personal health data must ensure individuals provide express consent, using information that is plain language and accessible based on the needs of the individual giving consent. Individuals can withdraw their consent at any time and their data will be removed from the point of their withdrawal of consent forward.

3

Right to access, portability & correction: Individuals have the right to request a portable copy of the personal health data they provided to a custodian and to the correction of their data where they identify inaccuracies. Individuals have the right to receive their data in a structured, commonly used, machine-readable format at no cost. For individuals without digital devices and/or internet, timely and portable access will be provided to them in another format (e.g. hard copy) ideally at no cost.

¹⁹ “Public benefits” means “there are five key features that a data sharing initiative designed to deliver public benefits should be able to demonstrate: 1. That it enables high-quality service delivery which produces better outcomes for people, enhancing their wellbeing; 2. That it delivers positive outcomes for the wider public, not just individuals; 3. That it uses data in ways that respect the individual, not just in the method of sharing but also in principle; 4. That it represents and supports the effective use of public resources (money, time, staff) to enables [sic] the delivery of what people need/want from public services; 5. That the benefits are tangible, recognised and valued by service providers and the wider public.” (From page 10 of “Data for Public Benefit” https://understandingpatientdata.org.uk/sites/default/files/2018-04/Data%20for%20public%20good_0.pdf) (Access April 29, 2021) ²⁰ “Necessity is a fundamental principle when assessing the restriction of fundamental rights, such as the right to the protection of personal data... It is fundamental when assessing the lawfulness of the processing of personal data... [W]hen assessing the processing of personal data, proportionality requires that only that personal data which is [sic] adequate and relevant for the purposes of the processing is [sic] collected and processed.” (From https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en) (Accessed April 29, 2021) ²¹ “Portability” means “to obtain data that a data steward holds on a data subject and to reuse it for the data subject’s own purposes. Individuals are free to either store the data for personal use or to transmit it to another data steward” (from <https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-right-to-data-portability>) (Accessed April 29, 2021)

4

Right to de-identification: Whenever feasible and reasonable, individuals have the right for their personal health data to be de-identified prior to their being shared with anyone other than themselves or their circle of care for purposes for which they have given consent. All de-identified data must meet minimum standards prior to sharing. 22

5

Right to benefit: Individuals have the right to benefit from their personal health data, including from their data being processed or shared for research or any other purposes. In order to benefit, people recognize the importance of sharing their personal health data, while recognizing custodians' duty to respect, protect, and fulfill personal health data rights. 22

6

Right to object to processing: Individuals have the right to object to the non-care related processing of their personal health data, such as processing for direct marketing.

7

Right to restrict processing: Individuals have the right to restrict the processing of personal health data in specific situations, such as where the individual contests the accuracy of the data, or where the individual has objected to the processing of their data and is awaiting the decision of a complaint.

8

Right to a complaint process: Individuals have the right to a complaint process by their data protection authority if they believe the processing or commercialization of their personal health data violates legislation.

9

Right to privacy and security: Individuals have a right to have their personal health data processed in a way that meets current standards and regulations of privacy and security.

10

Right to erasure (24): Individuals have the right to request that their personal health data be erased, which is sometimes called the right to be forgotten. This right only applies in certain specific circumstances, such as where the data are no longer necessary for the purpose(s) for which they were processed.

11

Right to engagement: Patients, and their caregivers, have the right to be part of decision-making related to personal health data to ensure their views, perspectives, and values are meaningfully incorporated into decision-making processes.

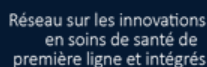
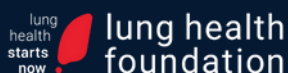
22 Minimum de-identification standards include the rigorous assessment of the probability of re-identification prior to sharing and the enactment and enforcement of strong penalties against the willful re-identification of such data. Standards will change over time and should always aim for the most rigorous possible respect, protection, and fulfillment of personal health data rights.

23 This takes its inspiration from the Caldicott Principles. The UK Caldicott Guardian Council. A Manual for Caldicott Guardians. The Caldicott Principles. <https://www.ukcgc.uk/manual/principles> (Accessed October 22, 2020)

24 The right of erasure comes from the General Data Protection Regulation. It is not absolute and only applies in certain circumstances. For more details, including exemptions, visit: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/> (Accessed October 22, 2020)

Endorsements as of September, 2025

Organizations



If you are an organization or individual who wants to endorse, visit:

<https://saveyourskin.ca/summit-working-groups/>

