## Appendix C: Table of requirements for health data social licence

*Requirements that were identified by previous groups and studies are identified with black font; edits and additions made by participants are identified with blue italic font[[1]](#footnote-1)*

| Requirement Category and “IT IS IMPORTANT THAT” requirement for health data social licence (in alphabetical order)  | Number of participants that identified the requirement as essential |
| --- | --- |
| **A: Benefits** |  |
| A1: Aggregate health data statistics (not individual data) are used, shared, and re-used widely. | 1 |
| *A2: Canada's health data ecosystem is comprehensive (e.g., integrating and building upon existing data holdings from healthcare and other settings such as employment, geographic and environmental) and modern (e.g., automated extraction, interoperable, integrating wearables and other new data sources)*  | *1* |
| A3: Health data are used, shared, and re-used to enable breakthrough discoveries that wouldn't be possible if health data were not shared.  | 1 |
| *A4: Health data controls, safeguards, and regulations are proportionate and not so burdensome that they prevent benefits from being obtained from health data.*  | *3* |
| *A5: Health data should be linked to other data sets to maximize value.*  | *1* |
| A6: Health data use, sharing, and re-use for public benefit is encouraged ("data aren't wasted").  | 6 |
| A7: Health data use, sharing, and re-use leads to benefits for communities, groups, subpopulations and/or society as whole.  | 6 |
| A8: Health data use, sharing, and re-use leads to benefits for the same people who contribute health data for a particular purpose.  | 5 |
| *A9: The benefits of health data sharing are communicated widely.*  | *2* |
| **B: Commercial Organizations** |  |
| *B1: Commercial organizations must exceed a higher standard or threshold for public benefit from health data use, sharing or re-use compared to non-commercial organizations.*  | *1* |
| B2: Commercial organizations must meet or exceed a higher standard or threshold for public benefit from health data use, sharing, or re-use compared to non-commercial organizations.  | 3 |
| *B3: Commercial organizations have the responsibility to protect, collaborate, and act on data that are collected to ensure public benefit is produced.*  | *1* |
| *B4: Health data are made available to commercial organizations when doing would produce a public benefit (for example, therapeutic interventions such as pharmaceutical companies developing new medications).* | *1* |
| B5: Health data are not sold.  | 4 |
| *B6: Health data are not used for marketing purposes.*  | *1* |
| B7: People who contribute their health data are not exploited by commercial organizations.  | 5 |
| *B8: The people, communities, and societies that contribute health data share in any commercial profit based on the data.*  | *2* |
| B9: There are additional safeguards, conditions, and protections when any commercial organization uses, shares, or re-uses health data.  | 4 |
| B10: There are additional safeguards, conditions, and protections when insurance companies use, share, or re-use health data.  | 1 |
| B11: There are additional safeguards, conditions, and protections when pharmaceutical companies use, share, or re-use health data.  | 1 |
| **C: Equity and Fairness** |  |
| C1: Health data are not used in ways that create stigma or discriminate against groups.  | 3 |
| C2: Health data for and about systemically marginalized populations (for example data about people with disabilities), are only used, shared, or re-used for purposes that the intended beneficiaries support.  | 1 |
| C3: Indigenous data sovereignty and the right to Indigenous self-determination are acknowledged and respected.  | 4 |
| C4: People who contribute their health data are not exploited by any organization or individual.  | 1 |
| C5: Systemically marginalized populations have control over how their data are used, shared, or re-used.  | 3 |
| **D: Governance and Oversight** |  |
| D1: Accountable governance bodies for health data are in place.  | 6 |
| *D2: Data collection doesn't create undue burden on healthcare workers.*  | *2* |
| D3: External third-party oversight is in place for health data (e.g., an Information and Privacy Commissioner).  | 7 |
| *D4: External third-party oversight is in place for health data (e.g., data stewards).*  | *1* |
| *D5: External third-party oversight for health data is a new collaboration formed by patients, academia, government, industry, and other relevant stakeholders.*  | *1* |
| D6: Governance and decision-making bodies (e.g., Boards of Directors) include patients and members of the public.  | 4 |
| *D7: Governments have the responsibility to protect, collaborate, and act on data that are collected to ensure public benefit is produced.*  | *1* |
| D8: Health data are held by organizations that are *seen as trustworthy by the people and organizations that contribute data to them.*  | 8 |
| *D9: Health data are only used for approved purposes.*  | *1* |
| D10: Health data are only used, shared, or re-used for purposes that are legitimate.  | 2 |
| *D11: Health data sharing is strongly supported by legislation.*  | *1* |
| *D12: It is important that trusted and prominent leaders are involved in the collection of health data within communities.*  | *1* |
| *D13: National and international agreements are in place for the use and sharing of health data.*  | *1* |
| D14: The intended beneficiaries are involved in decisions about how health data are used, shared, or re-used.  | 4 |
| *D15: There are serious penalties and consequences for illegal activities such as data theft and fraud, and unauthorized data sharing (e.g., with third parties).*  | *5* |
| D16: There is a complaint process that is available to people in cases where they believe the use, sharing, or re-use of their health data violates legislation or the consent that they have provided.  | 1 |
| D17: There is formal notice about how health data will be processed, used, shared, or re-used before health data are collected.  | 6 |
| *D18: Unless there is expressed consent for data sharing, health data are stored in Canadian jurisdictions and stay within Canadian law.*  | *2* |
| **E: Personal Control and Involvement** |  |
| *E1: Data access by organizations and people who do not usually have access is controlled by separate methods and governance.*  | *1* |
| E2: Opt-in consent is obtained before health data are collected, used, shared, or re-used (i.e., people agree in writing to the use(s)/user(s) of their data).  | 4 |
| E3: Opt-out consent is obtained before health data are collected, used, shared, or re-used (i.e., people are provided with information about the proposed use(s)/user(s) and given the option of NOT having their data used).  | 1 |
| E4: People can access information that is stored about their consents for health data and modify or withdraw their consents.  | 3 |
| E5: People can correct inaccuracies in the health data that have been compiled about them.  | 5 |
| E6: People (and caregivers that they authorize) can *easily access* health data have been compiled about them in a usable format (e.g., one that can be read by a computer or electronic device) and *in a timely manner so that they can make informed decisions about their health and health care.*  | 8 |
| *E7: People (and caregivers they authorize) can easily access health data that have been compiled about them in a usable format (e.g., one that can be read by a computer or electronic device) in real time so that they can make informed decisions about their health and health care.*  | *1* |
| *E8: People (and caregivers that they authorize) can access the health data that have been compiled about them in a format that is easily understood (e.g., charts and other data visualizations)*  | *1* |
| *E9: People can obtain the aggregate results and findings from research that makes use of their data.*  | *1* |
| E10: The contribution of health data is voluntary.  | 2 |
| *E11: There are alternative mechanisms for the involvement of people who do not have access to technology.*  | *3* |
| *E12: There are mechanisms for people to authorize access to their data by organizations and people that would not usually have access to their data.*  | *1* |
| *E13: When data are collected at the point of healthcare service delivery, communications address and mitigate the risk that patients (who are often in a vulnerable state) feel pressured to provide consent or agree to data access.*  | *2* |
| **F: Privacy and Security** |  |
| *F1: All organizations (not just commercial organizations) are held to a higher standard when they use or provide access to data for purposes that do not have an obvious and direct public benefit (e.g., surveillance).*  | *1* |
| F2: Cybersecurity and other safeguards are in place to protect all health data, including de-identified data and anonymized data.  | 6 |
| *F3: Cybersecurity and other safeguards are in place to protect anonymized health data collected for planning or research purposes.*  | *1* |
| *F4: Cybersecurity and other safeguards are in place to protect health data that is collected for individual care.*  | *1* |
| *F5: Data cannot be transferred or made accessible to a third party and cannot be used for purposes other than those for which they were granted. Any breach of the rules exposes the parties to legal action.* | *1* |
| *F6: Data that include a name and other identifying information are routinely shared with authorized individuals involved in the care of the named person.*  | *7* |
| *F7: Explicit consent by the individuals contributing health data must be given in cases where identifiable health data will be used.*  | *2* |
| *F8: Identifiable data is made available for specific research purposes and with the consent of the individual.*  | *2* |
| *F9: If consent from participating individuals is obtained, health data can be transferred or made accessible to third parties.*  | *1* |
| F10: In certain circumstances (e.g., when data are no longer needed for the purpose for which they were collected) health data are erased or deleted if a data subject requests (“the right to be forgotten”).  | 1 |
| *F11: Only data that have been truly anonymized (e.g., data that exclude names and other identifying information about individuals and communities) can be shared.*  | *2* |
| *F12: People are notified immediately of breaches that involve their data.*  | *1* |
| *F13: The default practice is to remove the names of individuals and other identifying information about individuals and communities from health datasets that are shared for research or planning purposes.*  | *7* |
| F14: The number of people who have access to identifying information is kept to a minimum.  | 3 |
| F15: The privacy of people who contribute health data is protected.  | 5 |
| F16: There are additional safeguards, conditions, and protections when genetic data are used, shared, or re-used.  | 1 |
| *F17: There are auditing and consequences for non-compliance (e.g., absence of safeguards required by regulation or by an organization's own policies).*  | *2* |
| *F18: There are defined roles and accountabilities for all people involved in collecting, processing, using, sharing or re-using data.*  | *6* |
| F19: There are safeguards to prevent re-identification.  | 2 |
| *F20: There is a cybersecurity recovery plan in place so that records can be restored after a cybersecurity attack in a timely manner.*  | *3* |
| *F21: There is an accurate record of who accesses health data established based on individual login activities.*  | *1* |
| **G: Transparency, *Communications and Data Literacy*** |  |
| *G1: Educational materials to increase data literacy are available in formats tailored to meet the needs of specific audiences from kindergarten to the general public.* | *3* |
| *G2: Health data, and communications about health data, are available in the official language of the patient's choice.* | *1* |
| *G3: Individuals involved in communicating personal health information to patients should do so in a clear and transparent manner.* | *1* |
| *G4: Organizations involved in data collection, processing, use, or re-use are respectful, polite and welcoming when contacted by patients and members of the public.* | *1* |
| *G5: There are different ways of communicating how health data are collected, used, shared, and re-used, and by whom, including communications tailored to “meet people where they are” and address the needs of people who have low levels of education and no prior knowledge of health data collection, use, sharing and re-use.* | *2* |
| G6: There is a process for people to pose and get answers to their questions about how data are used, shared, or re-used by whom, and for what purposes. | *7* |
| G7: There is transparent and plain language about when, how, why and with whom health data are used, shared, or re-used without the consent of the data subjects. | *6* |
| G8: There is transparent and plain language, *including language that is understandable by the general public (e.g., 8th grade reading level)* about who has access to what data for what purposes *throughout the entire data lifecycle (from data collection to dissemination of findings).* | *8* |

1. *In cases where a participant wanted an edit that would change the scope or meaning of a requirement that other participants had already selected in its original form, we created a second requirement rather than assume that the change would be agreed upon. As a result, there are four pairs of requirements that have similar wording (B1 and B2, D3 and D4, E6 and E7, F3 and F4).* [↑](#footnote-ref-1)