2023

DATA GOVERNANCE FRAMEWORK APPENDIX

TABLE OF CONTENTS

Appendix A: Indigenous Data Governance Jurisdictional Scan

Jurisdictional Scan on Indigenous Data Governance

Executive Summary

The purpose of this document is as follows:

1. To propose working definitions of Indigenous data sovereignty and Indigenous data governance in the context of the IPHCC.
2. To propose recommendations for how the IPMC can begin to develop an IPHCC-specific Indigenous data governance framework.

Proposed Working Definitions

To begin a discussion about Indigenous data sovereignty and Indigenous data governance, it is useful to have agreed-upon definitions for both terms. The following proposed definitions are a starting place for the development of more official definitions:

- **Indigenous data sovereignty** is the right of Indigenous communities to govern the entire life cycle of their data.
- **Indigenous data governance** refers to the principles, processes, and mechanisms by which Indigenous communities exercise their right to data sovereignty.

In the context of the IPHCC,

- The **'Indigenous community'** in question is the Indigenous-governed primary health care sector, which includes: (1) the communities and clients served by IPHCC members and (2) IPHCC member organizations.
- **'Govern'** means to exert exclusive power over.
- **'Data'** refers to all quantitative and qualitative information collected by IPHCC member organizations.
- **'Data life-cycle'** refers to the complete process by which data is created, stored, and shared. It includes: what data are collected, and from whom; how data are collected, stored, and protected; who has access to the data; how data are interpreted; at what point to share findings, and to whom; when data should be deleted; and, of course, the reason why data were collected in the first place.
- The **'principles, processes and mechanisms**' refer to, respectively:
  - Core principles that guide how the Indigenous-governed primary health care sector exercises its data sovereignty rights.
  - Policies and procedures developed based on the core principles.
  - Compliance mechanisms that ensure that the policies and procedures are being followed and the core principles are being honoured

Proposed Recommendations for Developing an IPHCC-specific Indigenous Data Governance Framework

The following proposed recommendations are based on the results of the jurisdictional scan and represent a possible path towards the development of an IPHCC-specific Indigenous data governance framework.

1. **The IPMC should lead the development of an IPHCC-specific Indigenous data governance framework to be approved by the Council.** After the IPHCC-specific Indigenous data governance framework is approved by the IPHCC, IPMC could liaise with the Alliance's Data Standards group to explore how the broader community-health sector can best support the IPHCC's vision for Indigenous data governance.

2. **The development of an IPHCC-specific Indigenous data governance framework should begin by identifying and defining a core set of data governance principles that are inclusive of the diverse Indigenous communities served by IPHCC member organizations.**
    a. The QDSS would collaborate with IPMC to determine a meaningful and inclusive process for identifying and defining this core set of data governance principles.
    b. Sources of information that can be used to develop this core set of principles include:
    c. Existing sets of First Nations, Inuit, and Metis principles (e.g. OCAP®, QI, OCAS etc.).
    d. The IPHCC Model of Wholistic Health and Wellbeing.
    e. Consultation and collaboration with members of the IPHCC community, including clients, Elders and traditional knowledge-users.

3. **Once the IPHCC has agreed upon core Indigenous data governance principles, progress should be driven by identifying goals and specific objectives for implementation.**
    a. These goals should include the development of policies and procedures, as well as compliance mechanisms, to ensure the core principles are honored.

Introduction

Indigenous data sovereignty is foundational for all work involving Indigenous data. Contextually-developed Indigenous data governance frameworks are the ideal mechanism for actualizing Indigenous data sovereignty rights (FNIGC, 2016; Smith, 2016). An essential step in the growth of the IPHCC—as an Indigenous organization, as an organization that holds Indigenous data, and as an organization that represents members who themselves hold Indigenous data—is the development of an IPHCC-specific data governance framework.

Recommendation 1: The IPMC should lead the development of an IPHCC-specific Indigenous data governance framework, to be approved by the Council.

This framework would form the foundation upon which the IPHCC would develop data-related policies, procedures, and compliance mechanisms. It would also form the basis for conversations between the IPMC and the Alliance's Data Standards group, to explore how the broader community-health sector can best support the IPHCC's vision for Indigenous data governance.

In order to begin the conversation about what Indigenous data sovereignty means in the context of the IPHCC, it is necessary to first settle on shared working definitions for both Indigenous data sovereignty and Indigenous data governance. Another useful initial step is to scan other jurisdictions and settings in order to better understand what Indigenous data governance looks like in practice.

Based on this jurisdictional scan, it seems that most Indigenous data governance frameworks have two key sub-components:

(1) a contextually-developed set of core data governance principles and

(2) a series of policies and procedures, along with associated compliance mechanisms, that will help ensure the core data governance principles are honoured.

In order to be effective, the IPHCC's data governance framework will need to be inclusive of the diverse Indigenous communities served by the IPHCC. While much can be learned from well-established data governance principles—especially Ownership, Control, Access, and Possession (OCAP®), which was developed by and for First Nations (FNIGC, 2014, 2016)—it will be important to base the IPHCC's data governance framework on principles that encompass Metis, Inuit, and First Nations perspectives. After the IPHCC has identified and defined its core data governance principles, progress can be maintained by identifying goals and specific objectives for implementation. Evidence from the jurisdictional scan suggests that clear parameters facilitate the implementation of Indigenous data governance frameworks.

Defining Indigenous Data Sovereignty

Establishing core working definitions for both Indigenous data sovereignty and Indigenous data governance, both broadly and in the specific context of the IPHCC, is necessary in order to have more nuanced conversations about how to begin the process of developing an Indigenous data governance framework for this sector.

The following definitions are based on a review of the Indigenous data sovereignty / data governance literature. Each component within the definitions are further defined and contextualized.

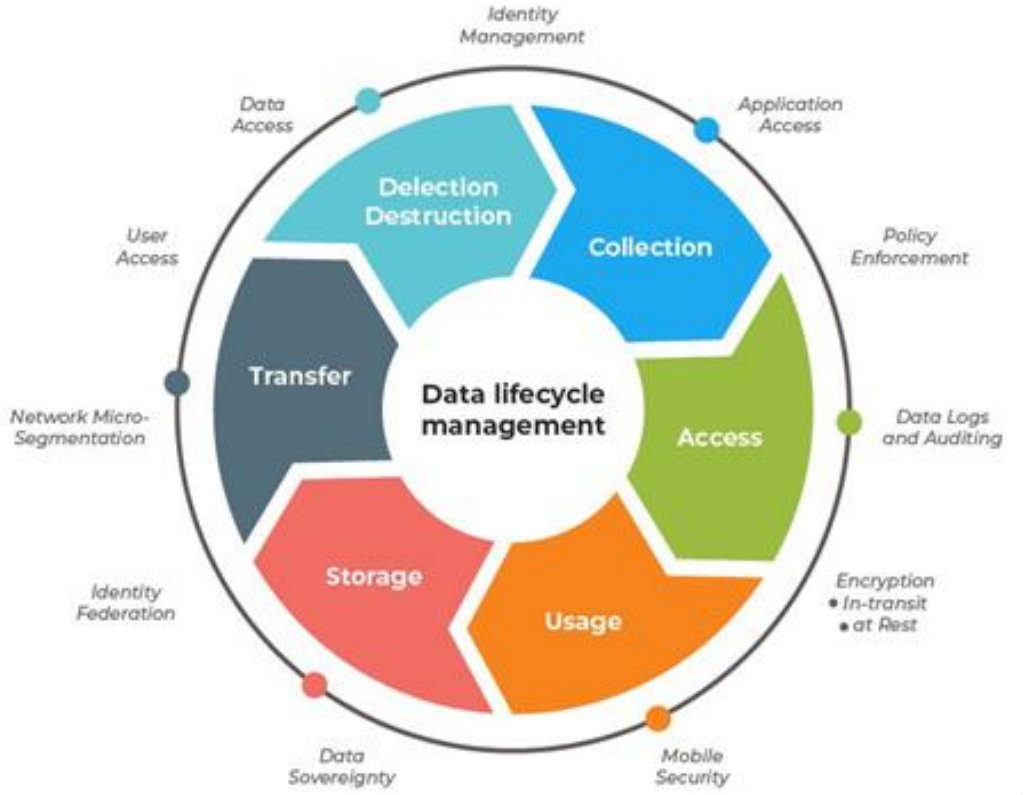
Indigenous Data Sovereignty:
The right of Indigenous communities to govern the entire life-cycle of their data.

Indigenous Data Governance:
The processes and mechanisms by which Indigenous communities exercise their right to data sovereignty.

Indigenous communities:
A self-determined Indigenous collective. Indigenous data sovereignty is likened to a nation's sovereign jurisdiction over its territory: Just as members of a nation collectively hold jurisdiction over their lands, so too do members of Indigenous nations collectively hold jurisdictional rights over their data (FNIGC, 2016). In the context of the IPHCC, the 'community' in question is the Indigenous-governed primary health care sector, which includes (1) the communities and clients served by IPHCC members and (2) IPHCC member organizations.

Govern:
To exert exclusive power over. Data governance systems typically reflect and reinforce systems of privilege and oppression within society. Within the context of colonialism, settler academics and institutions have repeatedly, and non-consensually, extracted data from Indigenous communities, using that information for purposes not aligned with communities' interests (FNIGC, 2014; Smith, 2012; Snipp, 2016). Indigenous data governance is a form of political self-determination and part of the process of decolonization.

Data:
Information about an Indigenous community. Indigenous data sovereignty applies to qualitative as well as quantitative data (FNIGC, 2020). As the First Nations Information Governance Centre (FNIGC), the organization that pioneered the development of OCAP®, puts it: OCAP® principles apply to all "information (records, reports, data) that identifies any particular First Nation or group of First Nations" (FNIGC, 2014: 2). In the context of the IPHCC, data refers to refers to all quantitative and qualitative information collected by IPHCC member organizations.



Sourced from: https://medium.com/jagoanhosting/what-is-data-lifecycle-management-and-what-phases-would-it-pass-through-94dbd207ff54

Lifecycle of data: The complete process by which information about an Indigenous community is created, stored, shared, and deleted. It includes: what data are collected, and from whom; how data are collected, stored, and protected; who has access to the data; how data are interpreted; at what point to share findings, and to whom; and, of course, why the data were collected in the first place (Snipp, 2016: 40)

Jurisdictional Scan of Indigenous Data Governance

Please see Appendix 1 for a summary of how Indigenous data governance is being applied in a variety of different settings, including: The Institute for Clinical and Evaluative Sciences (ICES') Indigenous Portfolio, British Columbia First Nations' Data Governance Initiative (BCFNDGI), FNIGC's Indigenous Governance Strategy Framework, the Alliance for Healthier communities, as well as various research projects / initiatives in Australia and New Zealand.

Several common themes are of particular relevance for developing an IPHCC-specific Indigenous data governance framework. First, the approaches outlined below have two key components: (1) a set of core Indigenous data governance principles and (2) specific goals / actions / policies designed to ensure those principles are being honoured. Secondly, the approaches outlined below tend to have a very specific scope. For example, the FNIGC, ICES, and Alliance all hold specific Indigenous datasets, while most of the examples from Australia and New Zealand relate to specific research projects or strategic plans. The following two sections unpack these observations in greater detail.

Indigenous Data Governance Principles

Recommendation 2: The development of an IPHCC-specific Indigenous data governance framework should begin by identifying and defining a core set of data governance principles that are inclusive of the diverse Indigenous communities served by IPHCC member organizations.

Identifying and defining a core set of Indigenous data governance principles would be a logical initial step for developing an IPHCC-specific data governance framework. It is important to note that, because of the diversity of Indigenous communities, both globally and on the lands that are now known as Canada, there is no single model for actualizing Indigenous data governance (FNIGC, 2016; Smith, 2016). Instead, it is the prerogative of individual Indigenous communities to define how they want to assert their right to data sovereignty; this process of definition begins with identifying and defining core data governance principles.

Based on the jurisdictional scan, OCAP® is a popular source of inspiration for Indigenous data governance frameworks developed in what is now called Canada. Other potential sources of inspiration include *Inuit Qaujimajatuqangit,* the principles of Indigenous cultural safety, the calls to action of the Truth and Reconciliation Commission (TRC), the calls to justice of the Inquiry into Missing and Murdered Indigenous Women and Girls (MMIWG), and the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). Interestingly, no Metis-specific frameworks were cited; however, ICES does have a partnership with the Metis Nation of Ontario.

Given its predominance, it is worthwhile to unpack OCAP® a bit further. Developed by, and for, First Nations, the OCAP® refers to Ownership, Control, Access, and Possession—principles that are defined broadly, providing room for contextual interpretation (FNICG, 2014, 2016). Ownership refers to the relationship between a community and their data; specifically, First Nations own information about themselves in a manner akin to how individuals own information about themselves (FNIGC, 2014, 2016). This right to ownership applies regardless of where data are stored (FNIGC, 2020). Control refers to the right of First Nations to govern "how information about them is collected, used and disclosed" (FNIGC, 2016: 149). Access refers to the right of First Nations to access their data, including the results of analyses conducted using their data, as well as to determine whom else can access their data (FNIGC, 2014, 2016). Possession refers to the right of First Nations to govern how their data is stored, including the appointment data stewards (FNIGC, 2014, 2016).

However, OCAP® is just the beginning of the conversation—ICES, BCFNDGI, and the FNIGC all elaborate upon the OCAP® model. ICES, for example, co-created a series of four core principles with Chiefs of Ontario (COO): Ethical relationships, formalized data governance rules, using evidence to support community policies and programs, and embracing Indigenous perspectives and worldviews.
It is also essential to note that OCAP® is not universal; other Indigenous nations have identified their own sets of core principles. *Inuit Qaujimajatuqangit* is the traditional knowledge-system of the Inuit. Unlike OCAP®, which is particular to the governance of data, *Inuit Qaujimajatuqangit* (IQ) is considerably broader, outlining rules and principles for "living a good live" (Tagalik, 2010: 1). IQ principles include: serving others, consensus decision making, acquiring skills and knowledge, collaborative relationships, environmental stewardship, and being resourceful to solve problems (Tagalik, 2010). ICES—which, like the IPHCC, holds First Nations, Inuit, and Metis data—identifies IQ as a core point of reference for people looking to better understand ICES' approach to Indigenous data governance.

When identifying and defining core data governance principles for the IPHCC, it will be important to develop a process that ensures that a diversity of perspectives are included. As a pan-Indigenous, status-blind organization, the IPHCC will need to ensure its approach to Indigenous data governance is inclusive of Metis, Inuit, and First Nations worldviews and values. To this end, insight should be drawn from existing sets of First Nations, Inuit, and Metis principles (e.g. OCAP®, QI, etc.). Consultation and collaboration with members of the IPHCC, including clients, Elders and traditional knowledge-keepers, would also strengthen the process. The IPHCC's Model of Wholistic Health and Wellbeing, which represents a vision that is already shared by the Indigenous community-governed health sector, could be an additional source of inspiration.

Implementing Indigenous Data Governance

Once core Indigenous data governance principles have been identified and defined, the next step for the IPMC would be to determine how best to put those principles into practice. Implementation can be facilitated by ensuring that the scope of the Indigenous data governance framework is clearly defined. For example, the FNIGC, ICES, and the Alliance all hold specific Indigenous datasets, while most of the examples from Australia and New Zealand relate to specific research projects or strategic plans. In other words, there must be a shared understanding of what specific data falls under the Indigenous data governance framework.

Given the diversity and complexity within the Indigenous-governed community health sector, implementation could be facilitated by identifying goals based on the sector's current objectives. For example, if research is a priority area, than an initial goal could be to develop procedures for negotiating research partnership agreements, including key language and stipulations.

Recommendation 3: Once the IPHCC has agreed upon core Indigenous data governance principles, progress should be driven by identifying goals and specific objectives for implementation.

Similarly, a common element among the Indigenous data governance frameworks included in this jurisdictional scan is the existence of a decision-making body that has the authority to govern who is able to access the Indigenous data in question, and for what purpose. In most cases this decision-making body is an Indigenous data governance committee (ICES, BCFNDGI, Mayi Kuwayu Study); ICES, for example, has representative data governance committees "populated by the relevant Indigenous organizations" for the data researchers are requesting to access (Walker, 2017: 2022). In the context of the IPHCC, an initial goal could be to define the respective roles of the IPMC and the Council with regards to screening, evaluating, and responding to requests to access IPHCC sector data.

Developing an implementation work plan with specific, clearly defined goals would make it easier to apply broad data governance principles in a highly complex context. Put differently, instead of being developed wholesale and then set in stone, the IPHCC's data governance framework would grow and evolve with the IPHCC and the Indigenous-governed health sector.

Conclusion

The findings from this jurisdictional scan offer insight for how Indigenous data sovereignty can be applied in the context of the Indigenous-governed community health sector. The recommended approach begins by agreeing upon working definitions of Indigenous data sovereignty and Indigenous data governance, both in general and in the context of the IPHCC. The IPMC would then begin the work of identifying and defining core data governance principles that reflect the diversity of Indigenous communities served by the IPHCC sector. Potential sources of inspiration for the development of those principles include existing frameworks (e.g. OCAP®, QI, etc.) and consultation with members of the IPHCC community (e.g. clients, Elders, etc.). After a set of core IPHCC data governance principles have been approved by the Council, they would be used as the basis for IPHCC data governance policies and procedures, as well as associated compliance mechanisms. Momentum would be maintained during this phase of development by identifying goals and specific objectives for implementation.

Appendix 1. Case Studies of Indigenous Data Governance

Overdose Research in British Columbia

Sabeti and colleagues (2021) provide a real-world example of health agencies employing OCAP® principles, and the Truth and Reconciliation Commission of Canada's Calls to Action, when conducting research, particularly in the form of data governance and stewardship (2021, p. 338). The research study focuses on the opioid crisis in British Columbia, and how Indigenous populations are being affected. The First Nations Health Authority (FNHA), along with the BC Centre for Disease Control (BCCDC), the BC Provincial Health Officer (BC PHO) and the BC Ministry of Health collaborate on the study to surveil and analyze data on Indigenous people who have overdosed on opioids in British Columbia (Sabeti et al., 2021).

Aligning with the principles of OCAP®, the FNHA acts as the data steward of information collected on First Nations. The BCCDC, BC PHO and Ministry of Health are each able to partner with the FNHA; however, the ownership of the data remains amongst First Nations (Sabeti et al., 2021, p. 343). The health agencies collaboratively developed a Data Access Request and Information Sharing Agreement, allowing the data to be hosted by the BCCDC while remaining under First Nations control. Data are analyzed by FNHA, with the assistance of BCCDC analysts as necessary (Sabeti et al., 2021, p. 343). The FNHA restricts access to raw data to necessary members of their own organization and the BCCDC (Sabeti et al., 2021, p. 344).

This project also applies the Truth and Reconciliation Commission's 19th Call to Action, which requires that:

- Health gaps between Indigenous and non-Indigenous people be closed, and
- Research results derived from Indigenous communities be used for progress reports and identifying health trends (2021, p. 344).

The findings from this study are being used to address opioid overdoses amongst First Nations living in BC and non-Indigenous BC residents. The information collected aid in the development of harm reduction initiatives, policies on the opioid crisis, as well as reports on how the crisis affects First Nations in BC (Sabeti et al., 2021, p. 344).

Ysleta del Sur Pueblo's ***Comprehensive Economic Development Strategy Survey***

The Comprehensive Economic Development Strategy created by the Ysleta del Sur Pueblo tribe in Texas is another example of Indigenous data governance (Rainie et al., 2017, p. 8). Dissatisfied with the quality and intention of the national census survey, Ysleta del Sur Pueblo officials developed their own survey to collect demographic and socio-economic information. The Ysleta del Sur Pueblo Economic Development Department, tribe members and the enrollment office partnered with the University of Texas to conduct a comprehensive survey that addresses the needs of the Ysleta del Sur Pueblo people (Rainie et al., 2017, p. 8).

The researchers prioritized community engagement from the inception of the study, holding focus groups to gauge the needs of the community, as well as community meetings to educate tribe members on research methodologies (Rainie et al., 2017, p. 9). The survey was administered when tribal members went to the Ysleta del Sur Pueblo's enrollment office for their mandatory annual contact information update (Rainie et al., 2017, p. 8).

The results of the survey have both internal and external uses. The Ysleta del Sur Pueblo tribe members have developed and revised policies based on the data extracted from the survey, including a new initiative on affordable housing, an area that was not adequately surveyed in the national census (Rainie et al., 2017, p. 10). The tribe also uses the survey results to support funding applications. For example, it was the only documented proof Ysleta del Sur Pueblo tribe members had to convey the economic consequences of the recent closing of local gaming operations (Rainie et al., 2017, p. 10). Research from the tribe demonstrates the strengths of employing Indigenous research sovereignty, as it facilitates Indigenous self-determination by helping ensure tribe members have power and decision-making authority (Rainie et al., 2017, p. 17).

COVID 19 Pandemic in Indigenous Populations across the U.S

The COVID 19 crisis among those that identify as Indigenous, American Indian or Native Alaskan in the U.S is an example of the negative consequences of ignoring Indigenous data sovereignty (Yellow Horse & Huyser, 2021). The coronavirus pandemic continues to disproportionately impact Indigenous communities in the U.S. As of April 2021, the Navajo Nation had the highest rates of COVID-19 per capita in the U.S, and several tribal lands across the U.S occupied the top COVID 19 hot spots (Yellow Horse & Huyser, 2021).

Despite research indicating that the COVID 19 incidence rate among Indigenous people in the U.S is projected to be 3.5 times higher than white Americans, those in the field of Indigenous research believe the realities of Indigenous people are being underestimated by federal and state statistics (Yellow Horse & Huyser, 2021). Many states that ask for participants to identify their racial and ethnic background on surveys do not account for Indigenous people of mixed heritage or they may conflate American Indian, Native Alaskan and Native Hawaiian all into one category. Other states simply do not include Indigenous ancestry among their classifications, and force those of Indigenous heritage to choose the "other" category (Yellow Horse & Huyser, 2021). Indigenous data sovereignty must be integral from conception for research initiatives involving Indigenous people, otherwise basic foundational information such as Indigenous identity can be inadequately recognized.

Tribes that attempt to address the needs of their community and access data are often met with resistance from mainstream health and research institutions. For example, the CDC refused to share COVID information with tribal epidemiologists while allowing access to state run organizations, while states like New Mexico have released data collected from tribes without their approval (Yellow Horse & Huyser, 2021). In response, some tribes are choosing not to share their nation's data with government bodies. Mainstream institutions, by failing to acknowledge and adhere to Indigenous research governance principles, are creating barriers to comprehensive and quality research. Breaches in trust such as these weaken the relationship between Indigenous and non-Indigenous research communities; poor research relationships result in data collection being used to perpetuate harm instead of utilizing its potential to empower Indigenous communities.

Appendix 2. Alternative Data Governance Models

Several models of data governance have been developed as alternatives to the dominant corporate models of collecting and using personal information, although these alternatives were not conceived within an Indigenous context, they do provide insight into how largely digitalized personal data can be stored and shared ethically. *Data sharing pools*: Multiple members share their data for review and collectively co-own stakes and rights to the information
(Micheli et al., 2020, p. 7). The strength of data sharing pools lies in its synergistic qualities, including several data holders allows for reciprocity of information exchanges and encourages innovation. Despite the possible benefits of data sharing pools, the model is vulnerable to having a single member take on a dominant presence in the collective (Micheli et al., 2020, p. 7).

Data sharing can occur within a single pool or data pools can be shared *between* organizations as well (Carballa Smichowski, 2019, p. 226). Data pooling between organizations may be used in situations where there is a possibility of joint benefit amongst the involved parties, a low concentration of subjects to retrieve data from, and when the technical environment is conducive to sharing (Carballa

Smichowski, 2019, p. 227). Corporations may also choose to reject sharing data pools with other organizations within the same market to limit competition (Carballa Smichowski, 2019, p. 226).

Data cooperatives or Crowdsourced data commons: Similar to data sharing pools, data cooperatives or commons have several members contributing information to a single pool to be shared amongst other members or the public (Micheli et al., 2020, p. 7; Carballa Smichowski, 2019, p. 223). In data cooperatives and commons, data subjects volunteer information while maintaining control of the information they contribute. Ideally participants have democratic control of the data pool while incorporating a managing body (Micheli et al., 2020, p. 8). Each participant has equal benefit and authority in data share agreements. Data cooperatives and crowdsourced data commons are often open to the public and are developed for public-interest (Micheli et al., 2020, p. 8; (Carballa Smichowski, 2019).

Public data trusts: A single or several public stakeholders act as trustees of data regarding their citizens, allowing public consultations and independent intermediaries to ensure ethical protocols are followed (Micheli et al., 2020, p. 8). Public data trusts emphasize building relationships between public stakeholders and the civilians' data is being derived from. The intended beneficiary of this model is the public, especially on the policy level (Micheli et al., 2020, p. 8).

Personal data sovereignty and Collective bargaining on rights over personal data: Data subjects in the personal data sovereignty model have increased control of their personal information as they become key stakeholders, along with digital storage providers (Micheli et al., 2020, p. 9). This model seeks to increase the agency of its data subjects and create balanced power relationships between participants and digital platforms (Micheli et al., 2020, p. 9). Digital intermediaries can be included to assist with the storage and sharing of data (Micheli et al., 2020, p. 9). Data subjects seeking to collectively bargain may form unions to negotiate privacy agreements, particularly general conditions of use agreements (Carballa Smichowski, 2019, p. 224). Data privacy unions and collective bargaining are especially relevant when the personal data is produced socially on large corporate platforms, such as social media websites (Carballa Smichowski, 2019, p. 225)

Data requisition: Data that is stewarded by a private entity must be shared upon the request of a public actor for a fee (Carballa Smichowski, 2019, p. 227). Justification for requests and the scope of the data shared can differ among organizations employing data requisition. The French Parliament has been at the forefront of attempting to put data requisition into legislation; cases that would employ this model often involve instances of corporations owning data that has been derived from the public and can be used for public benefit (Carballa Smichowski, 2019, p. 227).

Appendix 3. Recommendations for Indigenous Research

Williams, Umangay and Brant thoughtfully propose recommendations on partnering with Indigenous communities on research studies. The authors acknowledge how research can be extractive and ultimately exploitive to individuals and entire communities (Williams et al., 2020). The recommendations attempt to subvert traditionally Western power dynamics that take place in research studies, having Indigenous people decide how they would like to be engaged with, if they agree to be a partner in the study at all (Williams et al., 2020, p. 7). The strength of the recommendations stems from the requirement that culturally safe policies in research are mandatory. In many instances, the importance and benefits of culturally safety are recognized, but its inclusion is voluntary. The authors propose removing the choice of opting into culturally safe consultation when conducting research, instead it must be integrated on an organizational and policy level (Williams et al., 2020, p. 13).

Intellectual property rights as they exist today must be refined to include work produced from Indigenous traditional knowledge. Indigenous knowledge may collectively belong to a community who must be consulted and asked to partner with if researchers attempt to use that information. Even if they agree to share their traditional knowledge with researchers, the law must reflect Indigenous communities' right to decide how the information will be used in the future (Williams et al., 2020, p. 11). Collective rights must be recognized by Canadian law both in intellectual rights and in privacy (Williams et al., 2020, p. 12).

Research timelines and funding cycles must allow time for researchers to develop trusting relationships with the community they are partnering with, in order to enable accountability to those nations. Acknowledging that building relationships takes time and are essential, research studies must not assume researchers from outside the community being partnered with can begin studying participants right away without building trust (Williams et al., 2020, p. 11). As Walter and Suina explain, prioritizing trust building is essential to removing barriers created after decades of deficit-based and exploitive research (2019, p. 240). Western research practices and their possible benefits are not often explained to participants, which can create an incomplete or negative view of research. Once an understanding about the intention and methods of research practices is met, participants can approach conversations on consent and contributions with more information (Walter & Suina, 2019, p. 240).

Equitable working relationships between non-Indigenous organizations, like mainstream research councils, and Indigenous organizations must be strengthened. Combined positions such as cross-appointments between the two organizations would offer mutual benefits for both communities and create opportunities that allow Indigenous academics to maintain ties to Indigenous communities and non-Indigenous organizations (Williams et al., 2020, p. 12).

Cultivating knowledge sharing relationships among Indigenous research cross appointees also facilitate the growth of Indigenous research organizations (Walter & Suina, 2019, p. 239). Along with efforts to foster more equitable relationships between Indigenous and Western organizations, Walter and Suina recommend strengthening the capacity of independent Indigenous organizations (2019, p. 239). Researchers working in both realms are in a position to be knowledge translators and an added resource to their communities (Walter & Suina, 2019, p. 239). Research committees must expand their knowledge of effective research methodologies and paradigms when choosing to provide resources. Studies conducted by Indigenous researchers using Indigenous methodologies are frequently delegitimized in academic spaces (Williams et al., 2020, p. 12).

Indigenous paradigms are often based on place, acknowledging the significance of relationality to one's environment. Whereas Western thought is based on reason, and can be in opposition to Indigenous ways of knowing (Williams et al., 2020, p. 4). The Albuquerque Area Southwest Tribal Epidemiology Centre (AASTEC) echo this recommendation, as recognizing the credibility of Indigenous methodologies by non-tribal organizations, including universities and government agencies, can work to disrupt the power imbalance in research practices (Walter & Suina, 2019, p. 240). Refusal research, in which Indigenous communities choose not to participate in studies they believe to be harmful or not in the interest of their people, must be respected (Williams et al., 2020, p. 13).

Refusal research may include instances of a community not wanting to share knowledge that is sacred or have painful experiences be made publicly available (Williams et al., 2020, p. 7). Instead, they may choose to redirect efforts to studies that shed light on inequities experienced by Indigenous people and how they are tied to a legacy of colonialism (Williams et al., 2020, p. 7). There needs to be a requirement that cultural safety principles be brought into evaluation protocols assessing Indigenous research by both Western and Indigenous research committees. Developed by Indigenous people, the evaluation protocols will work to ensure that studies align with Indigenous values and interests (Northern Health Indigenous Health, 2021; Williams et al., 2020, p. 13). Additionally, researchers need to explain their relationship to the community they are partnering with, and how they intend on staying accountable throughout the research process and lifecycle. This requirement must be met during the beginning stages of a study, and included in the proposal (Williams et al., 2020, p. 13). Marley suggests that research ethics should be enforced, and that violations be reported to Indigenous community and research council liaisons for appropriate handling (2018, p. 732). Culturally safe research practices can differ depending on which community is being partnered with, as each Indigenous nation is distinct. The recommendations mentioned are not exhaustive, instead they provide an entry into how to form research relationships with Indigenous communities in a good way (Williams et al., 2020). When creating research with an Indigenous community, their partnership must be essential from the beginning and throughout the entire research life- cycle (Williams et al., 2020, p. 11).

Practices aligning with Indigenous self-determination must be weaved into the foundation of Indigenous research, and is mandatory if we are to use research as tool of Indigenous sovereignty and not an avenue to maintaining colonial infrastructure (Williams et al., 2020, p. 7).

Appendix B: Important Definitions for the Data Management Framework

In the course of conducting a comprehensive jurisdictional scan, the IPHCC has systematically reviewed literature pertaining to Indigenous data sovereignty and governance. This review facilitated the compilation of definitions for two core concepts integral to our framework. These concepts – Indigenous Data Sovereignty and Indigenous Data Governance – have been carefully delineated, with key components within each definition further detailed and contextualized to suit the unique context of the IPHCC. By establishing these shared definitions, we aim to lay a solid foundation for effective collaboration and communication. This common language will not only enhance mutual understanding but also ensure consistency in the application of these principles across the various facets of our data management framework.

Indigenous Data Sovereignty: The right of Indigenous communities to govern the entire life cycle of their Data.

Indigenous Data Governance: The processes and mechanisms by which Indigenous communities exercise their right to data sovereignty.

Indigenous communities: A self-determined Indigenous collective. Indigenous data sovereignty is likened to a nation's sovereign jurisdiction over its territory: Just as members of a nation collectively hold jurisdiction over their lands, so too do members of Indigenous nations collectively hold jurisdictional rights over their data (FNIGC, 2016). In the context of the IPHCC, the 'community' in question is the Indigenous-governed primary health care sector, which includes (1) the communities and clients served by IPHCC members and (2) IPHCC member organizations.

Govern: To exert exclusive power over. Data governance systems typically reflect and reinforce systems of privilege and oppression within society. Within the context of colonialism, settler academics and institutions have repeatedly, and non-consensually, extracted data from Indigenous communities, using that information for purposes not aligned with communities' interests (FNIGC, 2014; Smith, 2012; Snipp, 2016). Indigenous data governance is a form of political self-determination and part of the process of decolonization.

Data: Information about an Indigenous community. Indigenous data sovereignty applies to qualitative as well as quantitative data (FNIGC, 2020). As the First Nations Information Governance Centre (FNIGC), the organization that pioneered the development of OCAP®, puts it: OCAP® principles apply to all "information (records, reports, data) that identifies any particular First Nation or group of First Nations" (FNIGC, 2014: 2). In the context of the IPHCC, data refers to refers to all quantitative and qualitative information collected by IPHCC member organizations.

Appendix C: SGAR

Introduction

After many years of debate, Canada formally endorsed the UN Declaration on the Rights of Indigenous Peoples (UNDRIP) on November 12, 2010. Indigenous peoples in Canada have long supported the declaration and specifically its provisions aimed at advancing self-determination (Belanger, 2011). UNDRIP is a non-binding document containing 46 articles that establish the essential standards for recognition and protection of the collective and individual rights of Indigenous peoples. Many of the articles pertain to health and wellness, including Articles 21, 23, and 24, which state Indigenous peoples have the right to access all social and health services and use their own traditional medicines and healing practices without any discrimination.

In 2016, Canada officially adopted UNDRIP; however, it has not been implemented throughout all provinces at the same rate. BC was the first jurisdiction in Canada to introduce its own legislation to implement the UNDRIP. Other provinces and territories have since followed suit and are in the early stages of implementation. The federal *United Nations Declaration on the Rights of Indigenous Peoples Act* later came into force in June 2021. The Act provides a framework for implementation, as well as reconciliation between Indigenous and non-Indigenous peoples and governments. The Act also states that all laws in Canada must align with UNDRIP, and that progress must be monitored through annual reporting to Parliament *(United Nations Declaration on the Rights of Indigenous Peoples Act,* 2021).

At its core Indigenous Data Sovereignty, affirms the rights of Indigenous Peoples to control collection, access, analysis, interpretation, management, dissemination, and reuse of Indigenous data (Kukutai and Taylor 2016; Snipp 2016). Indigenous data, born-digital or not, is a very broad category, including information, knowledge, specimens, and belongings of Indigenous Peoples or to that which they relate at both the individual and collective levels (Rainie et al. 2019; Lovett et al. 2019).

Steps for Effective Indigenous Data Governance

WHAT TO DO TO WHEN YOU RECEIVE INDIGENOUS DATA

STEP 01
Secure

Implement robust data security measures to protect the collected Indigenous data from unauthorized access, breaches, or misuse.

STEP 02
Govern

Develop and maintain a local data governance framework approach that assures Indigenous Data sovereignty is upheld in your organization.

STEP 03
Act

Establish an Indigenous oversight body that holds the organization accountable for breaches, misuse, and data/research request for Indigenous Data.

STEP 04
Report

Develop reporting structures that outline data breaches, access request, research request and ethical concerns which involves Indigenous data to the oversight body (Monthly, Quarterly Annually)

Step 1

Secure

Implement robust data security measures to protect the collected Indigenous data from unauthorized access, breaches, or misuse.

Step 2

Govern

Develop and maintain a local data governance framework approach that assures Indigenous data sovereignty is upheld in your organization.

Step 3

Act

Establish an Indigenous oversight body that holds the organization accountable for breaches, misuse, and data/research request for Indigenous Data.

Step 4

Report

Develop reporting structures that outline data breaches, access request, research request and ethical concerns which involves Indigenous data to the oversight body (Monthly, Quarterly Annually)

Step 1

Secure

Implement robust data security measures to protect the collected Indigenous data from unauthorized access, breaches, or misuse.

Organizations should approach Indigenous data with the utmost respect and sensitivity. Indigenous data refers to the information collected from Indigenous individuals and communities, which can include personal, cultural, and traditional knowledge. It is crucial to recognize that Indigenous data is not just data; it represents the experiences, history, and identity of Indigenous peoples.

- Privacy and Security Guidelines
- Apply encryption, secure storage, access controls, and regular security audits to safeguard the data throughout its lifecycle.
- Establish regular integrity and unauthorized access audit checks.
- Develop clear policies and procedures for data handling, including protocols for data sharing, retention, and disposal.
- Ensure that the data abide by federal, provincial/territorial compliance for data storage.
- Informed Consent and Cultural Protocols
- Obtain informed consent from individuals and communities before sharing the collected data.
- Ensure that the consent process is culturally appropriate and respects Indigenous protocols/sovereignty.
- Engage with Indigenous communities and stakeholders to develop data collection/management frameworks that align with their cultural values, protocols, and aspirations.
- Anonymization and De-identification
- Prioritize anonymization and de-identification techniques to protect the privacy of individuals and communities when sharing or analyzing data.

Breaches, unauthorized access, or misuse of Indigenous patient/client data must be reported to the oversight body and/or the Privacy Commissioner Immediately. See **ACT** guideline below for more details.

Follow best practices to ensure that data cannot be re-identified and assess the risks of re-identification before sharing or publishing any data.

By implementing these guidelines and measures, organizations can demonstrate their commitment to respecting Indigenous rights, fostering trust, and protecting the privacy and security of Indigenous Data. It is important to engage in continuous learning and adaptation, considering the diverse needs and contexts of Indigenous communities when designing data collection strategies.

Step 2

Govern

Develop and maintain a local data governance framework approach that assures Indigenous data sovereignty is upheld in your organization.

Governance is a crucial aspect of collecting and handling Indigenous Data. It ensures that the data is managed in a way that respects Indigenous data sovereignty, which refers to the rights and authority of Indigenous communities over their Data. Developing and maintaining a robust local data governance framework is essential to uphold these principles in your organization. Below are some key points and guidelines to consider:

Understanding Indigenous Data Sovereignty

- Begin to develop the organizational culture to support safe and respectful treatment and handling of Indigenous data once collected.
- Identify who owns the data and what rights are associated with the data located within your data domain.

Implement Data Management Procedures

- Develop guidelines for data management, including data storage, retention, and disposal practices. These procedures should align with Indigenous values, cultural norms, and legal requirements.
- Adopt already existing guidelines from Indigenous partners and stakeholders who have already developed them from an Indigenous perspective.
- Create a notification mechanism or a process for handling Indigenous data when access requests are received.

Monitor and Review Governance Framework

Set up a process for continuous monitoring and periodic review of the data governance framework. Regularly assess its effectiveness, solicit feedback from Indigenous-led organizations, like IPHCC, and make necessary improvements.

Training and Capacity Building

Invest in training programs and capacity-building initiatives for employees involved in data collection and management. Ensure that the data collectors understand the importance of Indigenous data sovereignty and the significance of their role in upholding it. IPHCC has developed learning modules that speak to Indigenous self-identification and Indigenous cultural safety. See our website for more details www.learningportal.iphcc.ca

Addressing Ethical Considerations

Ethical challenges may arise when using Indigenous data. These include but are not limited to:

- Lack of meaningful engagement
- Unacceptable data privacy and protection practices (See **SECURE** guideline).
- Cultural misrepresentation and appropriation
- Disregarding Indigenous knowledge systems
- Violating intellectual property and data sovereignty rights
- Historical trauma and re-traumatization

Ensuring community benefits and avoiding re-traumatization calls for intentional and meaningful data-sharing agreements and trauma-informed practices. Balancing Indigenous and Western knowledge systems necessitates collaborative research, respecting both perspectives.

Developing and maintaining a local data governance framework that upholds Indigenous data sovereignty is a legal and ethical imperative and a profound step towards fostering meaningful relationships and reconciliation with Indigenous communities. By implementing the Secure, Govern, ACT, and Report (SGAR) model, your organization can demonstrate its commitment to respecting the rights and self-determination of Indigenous peoples over their data.

Step 3

Act

Establish an Indigenous oversight body that holds the organization accountable for breaches, misuse, and data/research request for Indigenous Data.

Establishing an Indigenous Governance Body

Organizations collecting Indigenous data must be accountable to their local FNIM community by ensuring an Indigenous data governance process is in place. Mirroring the Ontario Health's *Indigenous Data Governance Matters* process, it is strongly recommended that organizations establish a governance body that oversees the collection, use, interpretation, and dissemination of Indigenous data. The Indigenous Governance Body should be comprised of FNIM community members and/or organizations (e.g., First Nation, MNO chapter, IPHCO, Inuit association, local Indigenous advisory group).

FNIM representatives participate on a voluntary basis; however, best practice includes providing honorariums as forms of appreciation for time spent on Body activities.

Establishing a Supportive Operational Team

It is recommended that the organization establish an operational support team for the Indigenous Governance Body that will support the review/approval process for requested data activities.

Roles may include:

- Privacy and Security Officer: Focuses on data protection and compliance with privacy standards.
- Ethics Review Officer: Ensures that all data activities adhere to ethical guidelines.
- Information Management Specialist /Researcher/Epidemiologist: Manages data accuracy and integrity.
- Legal and Policy Advisor: Provides guidance on legal matters and policy implications.

The responsibilities of the Supportive Operational Team will include:

- Develop a process to receive Indigenous data requests, both internally and externally to the organization.
- Conduct preliminary review of Data Engagement Request forms to vet and ensure appropriateness.
- Once established criteria has been met, forward request form to Indigenous Governance Body for review. If questions are raised, further clarification is needed, or changes are required, the form will be returned to the Support Operational Team for management of requested information.
- The Supportive Operational Team will connect with the requester, instructing them to update the request form accordingly. Once changes are made, the Supportive Operational Team will resubmit to the Indigenous Governance Body for final review and decision-making. All data decisions will lie with the Indigenous Governance Body, who will have final say if the request is rejected or approved.
- Additional SOT responsibilities can include, but are not limited to regulation functions such as:
- Establishing audit schedules
- Conducting investigations and audit review
- Enforcing policies and procedures
- Review and update the Indigenous data governance approach/policies.
- Conduct audits based on the organization's schedule.
- Reporting (Privacy Commissioner, SLT/ELT, BOD, see 'REPORT' for more details)

Recruitment Strategies

Recognizing that organizations may have existing relationships with all local FNIM communities and/or organizations. As such, the outlined recruitment strategies are some suggested pathways for achieving Indigenous representation on the Indigenous Governance Body.

Strategy	Description	Resources
Engaging Community Elders	Collaborating with esteemed community elders is pivotal to ensure data governance aligns with Indigenous values. Their wisdom in cultural protocols and history ensures cultural integrity.	• IPHCC Indigenous Patient, Family and Community Engagement Toolkit • Ontario Federation of Indigenous Friendship Centres • Local Tribal Councils • Regional Indigenous Elders Councils
Forging Partnerships with Indigenous Organizations	Establishing partnerships with recognized Indigenous organizations, provides access to a diverse pool of Indigenous experts, enriching oversight body perspectives.	• IPHCC Gashkiwindoon Toolkit • Ontario Native Women's Association • Indigenous Primary Health Care Council • Assembly of First Nations • Metis Nation of Ontario • Inuit Tapiriit Kanatami
Internship and Mentorship Programs	Tailored programs for emerging Indigenous leaders foster capacity-building and contribute to oversight body sustainability. Nurturing expertise within the community enhances the body's effectiveness.	• Indspire • Métis Youth Program (MYP) • The National Inuit Youth Council (NIYC)
Recognizing Indigenous Youth Voices	Amplifying Indigenous youth voices in the oversight body ensures innovation and intergenerational collaboration. By valuing their contributions, your organization benefits from fresh perspectives.	Ontario Indigenous Youth Partnership Project
Community Consultations	Regular community consultations serve as a foundation for identifying individuals with community trust and respect. Involving community members in the selection process ensures alignment with community aspirations and values.	• IPHCC Effective Engagement Toolkit • Ne Iikaanigaana Toolkit • ·Local Indigenous Community Networks

Meaningful Engagement

To genuinely uphold the principles of accountability and respect within your data governance endeavors, continuous and meaningful community engagement is paramount. This engagement should extend beyond a single event, becoming an ongoing practice intricately woven into your data processes.

The Indigenous Governance Body should actively seek input, feedback, and consent from the communities when making decisions related to Indigenous data collection, usage, and sharing. This ongoing interaction ensures that decisions made within your data governance framework resonate with the diverse perspectives and aspirations of those directly impacted by these processes.

Cultural Safety Training

Indigenous cultural safety training through the IPHCC will help the Supportive Operational Team understand the historical context, cultural significance, and sensitivity surrounding Indigenous data and establish a critical foundation for respectful, transparent, and culturally appropriate engagement with FNIM communities and organizations

Step 4

Report

Develop reporting structures that outline data breaches, access request, research request and ethical concerns which involves Indigenous data to the oversight body (Monthly, Quarterly Annually)

This phase of the SGAR model is a critical component of the data governance process. Reporting structures that promote accountability and transparency in managing data breaches, access requests, research inquiries, and ethical concerns are crucial requirements for handling Indigenous data.

Frequency of Reporting

To ensure continuous monitoring and accountability, reporting should be conducted at regular intervals and as urgent matters arise. The frequency of reporting can be categorized into four main timelines: urgent, monthly, quarterly, and annually.

A process to address urgent matters requiring immediate actions should be established, such as developing crisis management and response plans to address any emergency situations related to data breaches, unauthorized access or misuse.

- Monthly reports provide a detailed overview of recent activities.
- Quarterly reports offer a comprehensive assessment of the organization's data governance practices and help identify trends or recurring issues.
- Annual reports serve as a comprehensive review of the entire year, highlighting achievements, challenges, and improvements made in Indigenous data handling.

Reporting Responsibilities of the Supportive Operational Team

The Supportive Operational Team plays a pivotal role in the "REPORT" phase. They are responsible for reviewing and analyzing the reports submitted by various stakeholders. The Supportive Operational Team must thoroughly investigate reported incidents, breaches, or concerns related to Indigenous data and take appropriate actions based on their findings. They should have the authority to enforce policies, implement corrective measures, and provide recommendations to improve data governance practices. Additionally, the Supportive Operational Team is responsible for providing a timely summary/report to the Indigenous Governance Body on the issues and actions taken. Finally, the Supportive Operational Team should collaborate with relevant stakeholders to ensure that reported matters are handled with sensitivity, respect, and cultural appropriateness.

The "REPORT" phase of the SGAR model is a crucial element in upholding accountability and transparency when collecting Indigenous data. By establishing robust reporting structures, organizations can actively identify, and address issues related to data breaches, access requests, research inquiries, and ethical concerns in a timely manner. The regularity of reporting, through urgent, monthly, quarterly, and annual reports ensures continuous monitoring and evaluation of data governance practices. Moreover, the Indigenous Governance Body plays a central role in reviewing/approval of reports and providing recommendations for improvement. Through this accountable and transparent approach to Indigenous data governance, organizations can foster trust, respect Indigenous Data sovereignty, and strengthen their commitment to the well-being and self-determination of Indigenous communities.

Maturity Model

It is crucial for any organization that collects, processes, and stores Indigenous data to have a comprehensive understanding of its current stage in data governance and sovereignty. By completing this maturing model, organizations can gain valuable insights into the ongoing process of comprehending and establishing policies and procedures that align with Indigenous data sovereignty best practices.

	Awareness *Phase 1*	Planning *Phase 2*	Implementation *Phase 3*	Optimization *Phase 4*
Phase Description	Organization recognizes the importance of cultural safety and is working to develop and implement policies and procedures aimed at addressing health equity considerations for Indigenous people.	Organization has made a commitment to providing culturally safe care to Indigenous persons, and is beginning to engage in specific discussions with Indigenous communities about appropriate governance of Indigenous data.	Organization is actively ensuring ongoing cultural safety, and is equipped to ensure appropriate governance of Indigenous data.	Organization has fully implemented and is continuously improving its culturally safe care and Indigenous data governance practices.
Key characteristics	Organization displays a commitment to engaging with communities represented by clients to understand strengths and needs. Organization is creating a cultural safety strategy in collaboration with Indigenous clients and communities.	Organization has a developed cultural safety strategy. Organization is developing relationship template agreements with communities. Discussions regarding data governance/ sovereignty are occurring. Organization is working on creating Indigenous data governance structures, processes and policies.	Data sharing agreements in place with partners and Indigenous communities. Data governance policies and processes implemented.	Data governance policies and processes fully implemented. Organization actively monitors and refines its cultural safety and data governance Practices. Consistent engagement with Indigenous communities to adapt and evolve the practices.

Appendix D: Draft Data Sharing Agreement Template

Disclaimer: The information in this template is for discussion purposes only. Any final document sharing agreement using this template needs to be reviewed by a lawyer to ensure that the particular factual context of that agreement is consistent with the current law and meets the objectives of the parties to the agreement.

KEY TAKEAWAYS

- Document Sharing Agreements will be very fact and situation dependent. Terms that may be very reasonable for one agreement may be "overkill" or "underkill" in a different context.
- Canada is currently updating its privacy laws to better reflect protection of Indigenous knowledge – But, in general the law (as well as the standard practices of lawyers and organizations) is still far from being compliant with OCAP, OCAS, and QI principles, and often Agreements themselves can play a role in educating partners about the obligations regarding Indigenous Data Sovereignty.
- Even for those on the forefront of promoting Indigenous Data Sovereignty the "best practices" from a legal perspective are still very much a work in progress and just like agreements will vary on the situation.
- Technological development is causing rapid changes in the law regarding privacy and data protection generally, which is something to keep in mind in thinking about the timeline for Document Sharing Agreements.
- Data breaches are becoming more common (and increasingly expensive) problems and dealing with the costs associated with these is becoming a key part of most Data Sharing Agreements.

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
PARTIES TO THE AGREEMENT		
BETWEEN: [Name of Member (the "IPHCC Member")] **AND:** [External Partner] (referred to collectively as the "Parties")	**In this section, the parties to the agreement should be clearly identified with any acronyms defined.**	1. Who needs to be involved in the Agreement to achieve your data sharing goals? 2. Do those organizations have commonly used acronyms?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
PREAMBLE		
The Parties seek to protect the Data they share pursuant to this agreement and ensure that it is managed in a manner consistent with applicable laws and standards regarding personal privacy, and the principles of Indigenous Data Sovereignty, which is understood by the Parties to be the ethical data collection and research principles that have been developed by First Nations, Métis, and Inuit Communities commonly referred to as OCAP*, OCAS*, and QI*[1]*. **Those principles recognize:** • That Indigenous community or group information can be owned and governed in the same way as individual data. • That First Nations, Métis, and Inuit Communities have the right to own and govern their data regardless of where it is housed. • That First Nations, Métis, and Inuit Communities have the right to decide how their data is shared and with whom. • The IPHCC Member holds Data, including Traditional Knowledge, on behalf of First Nations, Métis, and Inuit individuals and Communities, subject to obligations that are consistent with Indigenous Data Sovereignty. This means that the IPHCC Member is obliged: • To clearly identify to individuals and Communities it serves the purposes for how their data is collected, created, held, or otherwise used; and To prevent misuse of Data, such as through cultural appropriation and inappropriate profit motives, and general unauthorized use. The guiding principle for the Parties in this Agreement for collection, use, or disclosure of Data, including Traditional Knowledge, is informed consent. Consent is informed when individuals who share their data know the purpose of the collection, use or disclosure and that they may give or withhold their consent. *[1] See S.1 for the definition of these terms.*	**Agreement preambles are not legally binding, but are helpful for understanding the intention behind the agreement.** **Use the Preamble to describe the context that has led to the agreement, and the purpose for sharing the data.** **The Preamble is also a good place to set out key principles of Indigenous Data Sovereignty or governance, any applicable privacy principles, and any other obligations concerning privacy and data.** **The Preamble can clarify ownership rights over the data shared as well as any work products (e.g., reports, studies, assessments, etc.) expected to be developed using that data. Where the data to be shared includes Traditional Knowledge or medicine, this would be an appropriate place to underscore the collective nature of the right and existing obligations to safeguard that knowledge or medicine.**	1. What are your organizations obligations and values with respect to the Data? 2. How do you want those obligations and values to guide the Agreement? 3. What do you want the other party to know is important to you when they engage with you through the Agreement?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DEFINITIONS		
Agreement means this Agreement, [including the Schedules to this Agreement], as it [or they] may be amended or supplemented from time to time. **Applicable law** means all applicable laws, including any statute, regulation or by-law, directive, rule, requirement, policy having the force of law, order, judgment, injunction, award or decree of any governmental authority which is binding on the Parties and in effect from time to time, including all applicable provincial and federal laws and regulations. For greater certainty Applicable Law includes the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A ("*PHIPA*") and the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c F.31 ("*FIPPA*"). "**Circle of care"** means the persons participating in and activities related to the provision of health care to the individual who is the subject of the Personal Health Information and includes necessarily incidental activities such as laboratory work and professional consultation. **Data** includes know-how, practices, processes, databases, tables, lists, designs, photographs, drawings, specifications, assessments, reports and samples. It also includes Indigenous Data, Personal Health Information and Traditional Knowledge as defined under this Agreement. **Data Keeper** means the organization responsible for receiving and maintaining the Personal Health Information, Data and Indigenous Data shared under this Agreement. **[Optional: Data Committee** means the committee established in accordance with (provision/Schedule) of the Agreement.]	Clarify the meaning of any terms that are necessary to interpret the agreement. This may include terms that are not standard or commonly known, unique to this agreement, or whose meaning depends on the context of this agreement. Importantly, 'Data' and 'Information' are not standard terms – what is written here are examples. The definition provided for Data can be as specific or broad as the Parties desire. They should think about what information could be captured by those terms such that the purpose(s) of sharing can be met and so that privacy and confidentiality provisions apply as intended. It may help to think about who could be disclosing the Data, the form it could take, the intended purpose(s), whether disclosure could be direct or indirect and if it extends to work product created as a result of the shared Data. Some thought could be given to whether the Parties wish to use the terms Data and Information interchangeably or in specific ways. This will depend on what the Parties expect to be sharing. One way to go about this is to define Information along the lines that "Personal Health Information" and "Personal Information" are defined in the applicable legislation, using Data as a catch-all for anything else. The Definitions section is also a place to note any acronyms or abbreviations (e.g., PHIPA, FIPPA, OCAP, etc.).	1. What will be included as 'Data'? 2. What types of information will be shared (i.e., clinical notes, population level information, etc.)? 3. Will 'Data' and 'Information' be used interchangeably, or will they carry distinct meanings? 4. Are there definitions from privacy legislation that overlap with the terms you plan to use?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DEFINITIONS		
Effective Date means the date the Agreement is executed [or another relevant time]. ***FIPPA*** means the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c F.31. **Health Information Custodian** means a person or organization described in s. 3 of *PHIPA* who has custody or control of Personal Health Information as a result of or in connection with performing the person's or organization's powers or duties or the work described in s. 3(1). **Identifying Information** means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual, as defined in s. 4(2) of *PHIPA.* **Incident** means any inappropriate or unauthorized access to or use of the Data which has, or may have, resulted in a breach of the Agreement or applicable laws and includes, but is not limited to the loss, theft or unauthorized access to the Data. **Indigenous Data** means any data held by the Data Keeper pursuant to this Agreement and any subsequent Service Agreement, which is capable of identifying an Indigenous person, Indigenous communities, Indigenous membership, status or residence on an Indian reserve. **Information means Personal Information, Personal Health Information and all other information collected, used, created or managed by the Parties during this Agreement.**		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DEFINITIONS		
Information Practices in relation to a Health Information Custodian, means the policy of the custodian for actions in relation to Personal Health Information, including, a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of Personal Health Information, and (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information, as defined in s. 2 of the *PHIPA.* **Knowledge Keeper** means a person who holds Traditional Knowledge. **OCAP®** refers to First Nations data sovereignty principles of ownership, control, access, and possession. **OCAS** refers to Métis data sovereignty principles of ownership, control, access, and stewardship. **Personal Health Information**, means identifying information about an individual in oral or recorded form, if the information, (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual, (c) is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019, (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual, (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, (f) is the individual's health number, or (g) identifies an individual's substitute decision-maker, as defined in s. 4(1) of the PHIPA, subject to subsections (3) and (4).		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DEFINITIONS		
Personal Information means recorded information about an identifiable individual, including, (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, telephone number, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they relate to another individual, (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, and (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual, as defined in s. 2(1) of the FIPPA. ***PHIPA*** means the *Personal Health Information Protection Act*, *2004*, S.O. 2004, c. 3, Sched. A. It is the law that governs the collection, use and disclosure of Personal Health Information by a Health Information Custodian. **QI** refers to Inuit data sovereignty principles of Inuit Qaujimajatuqangit. **Traditional Knowledge** means the sum of knowledge, skills, and practices based on the theories, beliefs, and experiences held by Indigenous peoples used in the maintenance of health as well as in the prevention, diagnosis, improvement or treatment of physical and mental illness. It is dynamic, holistic, intergenerational and linked to experience of and connection to lands. It also includes but is not limited to knowledge of special ecological places, knowledge of fauna and flora, seeds, medicines, traditional medicine and plants, culturally significant practices and locations. Traditional Knowledge may be transmitted orally, in written form, and through song, dance, paintings, rituals, ceremonies, visual manifestations, symbols and artwork. **Traditional Practitioner** means an individual who has gone through all the appropriate lessons and actions approved by a mentor and is recognized by the community whose Traditional Knowledge they hold as a credible practitioner.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
PURPOSES		
2.1 [insert list of purposes].	Further describe the context and intention of the Agreement if it is not sufficiently clear from the Preamble. It is a best practice to link the purposes to the permitted uses for the data either by referring to that section in the agreement or by referring to a schedule that clearly sets out what uses are permitted to fulfill the purposes.	1. What is the purpose of the data sharing agreement? 2. What are you trying to achieve by sharing the Data? 3. What are the best practices for sharing that type of data?

DESCRIPTION OF DATA AND OWNERSHIP		
3.1 The Data shared in this Agreement includes: **3.1.1** [insert list] **3.2** Subject to the rights of the individual to whom the Data relates and the Indigenous community to which the Traditional Knowledge belongs, Data provided by the IPHCC Member is and will remain the property of the IPHCC Member.	Describe the type/s of data that will be shared and the scope of sharing. Detailed information can be attached in an Appendix.	1. Who owns the data to be shared? 2. If it is Traditional Knowledge or Indigenous Data, then what obligations and policies does your organization already follow to protect it? 3. How will your internal policies and the principles of OCAP, OCAS, and QI be followed in describing who owns the data? 4. What information do you hope to hold from the External Partner? 5. What constraints or obligations does the External Partner have about ownership of information?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DURATION		
4.1 This Agreement will commence on the Effective Date and shall continue in effect until the earlier of [date or duration from Effective Date] or the date of Termination, subject to 4.2. **Renewal, Extension and Amendment** **4.2** This Agreement may be renewed, extended or amended with the written consent of all parties. **Termination for Convenience** Any Party may terminate this Agreement at any time, without cause, upon delivery of not less than [# of month/s] written notice to the other Party. **Return and Destruction of Information** Upon expiration of the Agreement or Termination, the Parties shall make best efforts to return all Data received. This excludes any Data necessary to comply with legal or regulatory compliance or practice, provided any such retained Data remains subject to the disclosure and use restrictions under this Agreement, even in case of Termination. **Survival of Terms** Terms and conditions relating to the creation, use, disclosure, destruction and ownership of the Data and confidentiality shall survive the termination and expiry of this Agreement	**Term:** The text at 4.1 is an example. The question to consider when defining the term is the Agreement for a definite term or indefinite? It is also important to consider how the agreement can be terminated. The factors that would go into determining the term of an agreement could include: The timeframe needed for both Parties to perform their contractual obligations, Goals of the agreement, External obligations related to the Data. If the Data is being shared for a project, this section should describe what the Parties will do to the Data once the project is complete. **Renewal and Extension:** This section sets out any additional allowances, procedures or restrictions about the duration of the agreement. Renewals can be made automatic. **Return and Destruction of Information:** The obligations can be more or less stringent depending on the objectives of the Parties (e.g., immediate return/destruction of Data, reasonable efforts, at the Party's request, etc.). A more flexible option is to provide that the Parties will determine the procedures to return or destroy Data when the time comes. The Parties could include a provision that the IPHCC Member can request a certification by the External Partner that the return/destroy requirements have been met, with caveats for Data received or stored digitally so long as no attempt is made to recover such Data from servers or backup sources and that any such retained Data remains subject to the disclosure and use restrictions. **Survival of Terms:** This section ensures that the data cannot be impermissibly used or accessed after the project is complete	1. How long will the data-sharing relationship last? 2. Is the relationship with the External Partner project specific or ongoing? 3. Under what circumstances do you see the relationship coming to an end? 4. What happens to the Data when the Agreement comes to an end or is terminated?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
TRANSFER OF DATA		
5.1 Data will be securely transferred in the following ways:	This section should set out the technical and physical requirements for the transfer of data to the Data Keeper(s).	1. How will you transfer the Data to the External Partner? 2. How and where will you and/or the External Partner store the Data? 3. Who will manage the database?
PERMITTED USES & DISCLOSURES		
6.1 The Data and Information under the terms of this Agreement is provided solely for the stated purpose [cite to the Preamble, or the Purpose section, if used, or list those purposes here]. The External Partner shall ensure that only the Users set out in the Appendix have access to the Data, with restrictions on their level of access tied to their Permitted Uses. **6.3** Except as permitted or required by law, and subject to the exceptions and additional requirements, if any, that are prescribed by regulation or otherwise, the External Partner shall not, in relation to any Personal Health Information shared with it, collect, use, disclose, retain or dispose of Personal Health Information except in accordance with this Agreement.	This is the section to set out how the External Partner is permitted to use the Data. A best practice is to be as detailed as possible, so that the Data cannot be used in ways the IPHCC Member hasn't consented to. Think about how uses of the Data will be logged and reported. The IPHCC Member should determine if there are disclosures permissible in certain circumstances without its prior written consent. This may have to do with the type of use to be made of such a disclosure, or the format in which it is provided. **Different uses:** If the Data will be used for future purposes or ongoing work that is not listed in the Agreement, there must be a process to obtain authorization from the Parties. This could involve the creation of a Data Committee or some other body that will manage the requests and make recommendations to appropriate authorities.	1. How can the External Partner use the Data that is shared? 2. How and when can the Data be disclosed to third parties? 3. How must consent to disclose be communicated? 4. Are there times when consent is not required to share the Data? 5. Where Traditional Knowledge may be disclosed, how has/will consent be sought from the community, Knowledge Keeper or the Traditional Practitioner? 6. Who within the External Partner's organization may need to use the Data to fulfill the goals or Purpose(s) of the Agreement?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
PERMITTED USES & DISCLOSURES		
6.4 Subject to Sections 6.6 and 6.7, the External Partner shall not disclose, publish or disseminate the Data to anyone without the prior written consent of the IPHCC Member. Where disclosed, the External Partner shall ensure proper context is provided so that the original meaning is not altered and that Personal Health Information is redacted. **6.5** The External Partner shall not, without the prior written consent of the IPHCC Member, use the Data for any purposes not expressly authorized by this Agreement (see Permitted Use Appendix), including, but not limited to, any matter being litigated or negotiated by or with the External Partner. **6.6** Should the External Partner become legally compelled to disclose any Data, prior to disclosing such data, the External Partner will provide the IPHCC Member with prompt written notice and shall reasonably cooperate with IPHCC Member should the IPHCC Member seek a protective order or other remedies to prevent disclosure. If only a portion of the Data falls under this exceptions, then only that portion of the Data shall be excluded from the use and disclosure restrictions of this Agreement. **Different Uses** **6.7** If the External Partner wishes to use the Data differently or for other purposes than described in the Agreement, they shall seek and gain prior written permission from the IPHCC Member.		7. What happens if the External Partner is legally compelled to disclose information? 8. If different uses of the Data may be desirable at a future time, how will the Parties address that?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
LIMITATIONS ON COLLECTION, USE, DISCLOSURE, AND RETENTION		
7.1 The Parties agree and warrant that the Data shall be used and disclosed only and strictly for the purposes specified in this Agreement. **7.2** The restrictions on use do not apply to: **7.2.1** Data that was already known to the External Partner free of restriction/subject to lesser restriction, or was publicly available. **7.2.2.** Data that must be disclosed under applicable law, subject to the requirements set out in Section 6.6. **7.3** The IPHCC Member may: **7.3.1** Remove, anonymize, aggregate or redact any identifying particulars associated with particular individuals or communities from the Data as it deems appropriate while maintaining the effective utility of the Data for the Permitted Uses, prior to giving its consent to any disclosure. **7.3.2** Refuse to disclose any part of its Data or require the return or destruction of any Data in accordance with Section 4.4. **Verification** **7.4** The External Party will provide the IPHCC Member the chance to review and approve a draft of any document, writing or communication which will disclose, summarize or refer to all or part of the Data to third parties at least [# of days] prior to such disclosure.	If it provides better clarity, the IPHCC Member can also add a separate section to set out what it will NOT allow the other Party to do with the Data. As with the previous section, this will depend on context so it's beneficial to be detailed. **Verification:** This section gives the first Party an opportunity to revise or approve any communications about the data or data sharing before they occur. **Delegation and subcontracting:** This section sets out whether either party is permitted to create service agreements with consultants and service providers, for example, to clean and match the shared data	1. Are there any prohibited uses that should be stipulated (*e.g.*, no commercial uses of Traditional Knowledge)? 2. Is there Data that can be used outside the Permitted Uses (*e.g.*, Data that is publicly available or must be disclosed for a lawful purpose)? 3. Can the parties modify the Data before sharing it to remove identifying information irrelevant to the Purpose(s) and Permitted Uses of the Agreement? 4. Can the Parties refuse to share Data, or demand its return or destruction? 5. How can the Parties verify the Data is represented properly in any materials the External Partner generates using the Data? 6. Are there third parties whose services are or may be required to carry out the Permitted Uses of the Data? 7. What are the third party obligations for upholding the security, confidentiality and privacy standards under the Agreement?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
LIMITATIONS ON COLLECTION, USE, DISCLOSURE, AND RETENTION		
Delegation and Subcontracting **7.5** The External Partner may allow a third party contractor to access the Data for the purpose of assisting the External Partner with its Permitted Uses set out in Section 6 (above) provided that the External Partner ensures, through contract with the third party, that: **7.5.1** Data, or any part or product thereof, provided to the contractor shall either be destroyed or returned to the disclosing Party upon completion of any contract, including service contract; and **7.5.2** The contractor shall maintain in the strictest confidence all Data made available by or acquired from the External Partner and shall not disclose to any third party, copy or use any Data except in performance of the contract with the External Partner; **7.5.3** The contractor shall maintain the same privacy and security standards as required by the External Partner under this Agreement and shall provide an undertaking to the IPHCC Member to abide by the terms of this Agreement. **7.6** The External Partner shall not directly or indirectly disclose, allow access to, transmit, transfer or make available to any individual, for any use whatsoever, the Data other than to an employee, professional advisor, contractor or agent of the External Partner who has a need to know such information solely for the Permitted Uses and who has agreed in writing to maintain the same privacy and security standards as required by the External Partner under this Agreement. **7.7** The External Partner shall remain responsible for any breach by a contractor or any person who receives Data from the External Partner at any time.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
CONFIDENTIALITY & SECURITY		
8.1 This Agreement and the information exchanged by the Parties leading to and pursuant to this Agreement is confidential. Neither Party may disclose, in whole or in part, the content of the Agreement without the prior written consent of the other party [, except that: *set out exceptions, if appropriate*]. **8.2** The External Partner acknowledges and agrees that all Data, whether received or created before or after the commencement of the Agreement, will be received in the strictest confidence and will be held by the External Partner only in accordance with and subject to the terms of the Agreement. **8.3** Data provided by the IPHCC Member to the External Partner shall be treated in a confidential manner by the External Partner, shall not be accessible to the general public, except with the prior written consent of the IPHCC Member, and [*if the External Partner is a government institution subject to FIPPA, then:* the Data shall be deemed, to the extent possible, to fall within the ss. 15.1, 17, 18 or 21 exemptions under *FIPPA*, whichever is more appropriate]. **8.4** The obligations of confidentiality contained in this section will not apply to any Data, as the case may be, to the extent that the External Partner can conclusively demonstrate that such Data: **8.4.1** Was, at the time of disclosure to the External Partner, in the public domain;	The specific content of this section will depend on whether there is one Data Keeper or a committee, and what privacy and information legislation applies. **Security:** The Parties could agree to review and abide by each other's security policies. ***FIPPA* Exemptions:** *FIPPA* grants the public the right to request information held by governments. There are exceptions to that right to disclosure. For example, the government may refuse to disclose the information if it were reasonably expected to reveal information shared in confidence from an Indigenous community. The problem is that the disclosure decisions under *FIPPA* are made by different departments. To the extent possible, it is a good practice to label Data shared with a government with a watermark indicating that it is personal and confidential or provided in confidence by an Indigenous government. Reaching agreement with a government party about how information will be characterized by them internally is important for protecting Data from undesired public disclosure.	1. Is the existence of the Agreement confidential? 2. Is disclosure of confidential information to third parties permitted with consent? If yes, then how should that consent be given? 3. Are there circumstances in which disclosure of confidential information is permitted without consent? 4. What legislative responsibilities do the Parties have to ensure confidentiality and privacy, if any? 5. What internal measures does a Party have in place to comply with legislated standards while limiting undesired public disclosure? 6. What happens if a Party is legally compelled to disclose information? 7. What policies are in place to ensure the security of the Data? 8. How will the Parties train staff in the proper handling of the Data? 9. Do you want a person or committee responsible to oversee compliance with the Agreement? 10. If yes to #9, then: - What is their role? - What are their powers? - How will they ensure proper care of Indigenous Data and Traditional Knowledge?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
CONFIDENTIALITY & SECURITY		
8.4.2 After disclosure to the External Partner, is published or otherwise becomes part of the public domain through no fault of the External Partner's actions; **8.4.3** Was in the External Partner's possession at the time of disclosure to the External Partner, and was not the subject of a pre-existing confidentiality obligation; **8.4.4** Was disclosed independently to the External Partner by a third party who was not subject to any confidentiality obligations in respect thereof, and in any event, provided that such information was not of a nature that had it been Data, the IPHCC Member would have required that it be kept confidential; or **8.4.5** Was independently developed by the External Partner without the use of any Data. **8.5** The Parties confirm that they have legislative responsibilities to ensure the confidentiality and privacy of personal information as set out in FIPPA and Personal Health Information as set out in PHIPA. The Parties agree that they will only access, collect, use, modify, retain and dispose of Data as outlined in this Agreement or as they are legally obliged to do.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
CONFIDENTIALITY & SECURITY		
8.6 Should the External Partner or the IPHCC Member receive a request under *FIPPA* or similar legislation for the disclosure of any of Data, the External Partner will not be considered to have breached its confidentiality obligations under this section for disclosing any confidential Data, as the case may be, to the extent that: **8.6.1** The External Partner immediately notifies the IPHCC Member and provides the IPHCC Member with the opportunity to express its views regarding any impacts that may arise from the requested disclosure; **8.6.2** Does not obstruct or interfere with any effort by the IPHCC Member to seek a protective order or other remedy to prevent, object to, enjoin, narrow the scope of, or otherwise contest the requested disclosure; **8.6.3** Discloses only those parts of the Data the External Partner is legally obligated to disclose if the IPHCC Member is unable to obtain a protective order or other similar remedy within the time period appropriate in the circumstances; and **8.6.4** The External Partner makes and reasonably pursues a request, that is reasonable and customary in the circumstances, to the applicable governmental authority, for confidential treatment of the information to be disclosed pursuant to such applicable laws.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
CONFIDENTIALITY & SECURITY		
Security **8.7** All parties are responsible for the security of the Data entrusted to them under this Agreement and shall safeguard the Data against accidental or unauthorized access, disclosure, use, modification and deletion. **8.8** The Parties agree to have policies and procedures in place to secure electronic data retention, backup, disposal and destruction, data protection, access control, identification and authentication, password governance, security breach response, network and work station security, firewall administration, remote access, disaster recovery, logging and auditing controls. **8.9** Upon request, each Party shall provide the other Party with a description of how the security and confidentiality of the Data are protected. **8.10** Each Party shall ensure that all its employees have completed appropriate privacy and security education. **[Optional] Data Committee** **8.11** A committee will be established [jointly] to oversee implementation of the Agreement, including by: • Developing standards and procedures required for the overall administration and coordination of the agreement. • Establishing/overseeing the appropriate subcommittees. Overseeing the processing of Data access requests and requests for Different Uses. • Providing an annual report to Parties. • Setting out rules to exercise its powers, duties and functions (e.g., attendance, quorum, etc.).		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DISPUTE RESOLUTION & BREACH PROCEDURES		
Inspection and Audit **9.1** By using the Data the Parties acknowledge that their access to and use of the Data may be logged and made available to the each other [and/or the Data Committee] for audit purposes. **9.2** When requested, and subject to *PHIPA*, *FIPPA* and other laws as applicable, a Party will, after having received written notice, allow the requesting Party or its authorized representatives to: **9.2.1** inspect and copy any Records in the possession or under the control of the Party which relate to login information regarding access of Data or the subject matter of this Agreement. **Reporting Incidents** The Parties will: Promptly notify each other of any Incident, by any person that has become known to it; Promptly furnish each other with details of such Incident, and assist in investigating or preventing the recurrence of any Incident; Cooperate with one another in any litigation and investigation against third parties deemed necessary by the IPHCC Member to protect the Data, to the extent such litigation or investigation is related to this Agreement; and Promptly use reasonable efforts to prevent a recurrence of any Incident.	This section sets out what will happen if there is an impermissible use of or access to the data. **Notification of breach:** The template as drafted imposes strict obligations on the Parties following a breach, but it can be drafted to provide greater flexibility. The Parties could say something like: "In the event of a Breach, Parties shall determine a process to resolve the issue expediently and shall cooperate and assist in any civil or other investigations carried out by either Party or a person or body with legislative authority to conduct such investigation involving the Data in its custody or control." **Termination for breach:** This section allows either party to end the agreement if there was an impermissible use of or access to the Data.	1. What are the reporting procedures for Incidents and Breaches? 2. Who carries what responsibility to resolve Breaches? 3. How will Breaches be investigated? 4. What remedies can be sought in response to a Breach? 5. How will disputes be resolved? 6. If something goes wrong, how will responsibility be allocated? 7. Who is liable if there is a Breach? And to what extent? 8. What insurance options are available to protect the Parties against lawsuits and other claims regarding the use of the Data?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DISPUTE RESOLUTION & BREACH PROCEDURES		
9.4 The Parties [and/or the Data Committee] shall retain a record of all Incidents. **Notice of Breach** **9.5** In the event of an actual or suspected breach of any of the provisions of this Agreement, the Party with knowledge of the breach or suspected breach shall: **9.5.1** immediately send a notice in writing to the other Party ("Notice of Breach") by email to the email address on the first page of this agreement notifying them of such breach. The Notice of Breach shall specify the nature of the breach or default and the section in the Agreement in respect of which, in the Party's opinion, a breach or default occurred. **9.5.2** Upon the other Party's receipt of the Notice of Breach, the parties shall confer in good faith to discuss resolution of the breach or default. **9.5.3** In the event the parties have not resolved the breach or default within thirty (30) days of the other Party's receipt of the Notice of Breach, the Party may decide to terminate this Agreement.	**Responsibility and Liability:** a Breach can lead to significant costs and damages. Investigations of data breaches alone can cost hundreds of thousands of dollars or more. Deciding in advance who will be responsible for a Breach and how investigations will take place is a major point for discussion with the External Partner. The law in this area is changing all the time and legal assessments about assessing risk in the Agreement is especially important. **Indemnification:** With this section, the parties can choose to agree not to sue each other for monetary payment in the event that the agreement is violated. **Insurance:** Insurance to cover the costs of data breaches or other liability is important for the Parties. It may be possible, in certain circumstances, to ask an External Partner to add the IPHCC member to their insurance policy. Insurance options should be clearly explored between both Parties during negotiation of any document sharing agreement.	

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DISPUTE RESOLUTION & BREACH PROCEDURES		
Investigation of a Breach **9.6** The Parties reserve the right to investigate known or suspected breaches of the Agreement. The Parties shall fully cooperate with any such investigation, including by providing access to all documentation requested orally or in writing by either Party or its agents supporting the investigation, and by providing any other assistance that may reasonably be requested in connection with said breach. **9.7** The Parties acknowledge that the Data is proprietary and confidential and that the IPHCC Member would suffer irreparable harm and unquantifiable damages if any of the provisions contained in this Agreement with respect to the Data are breached or not performed by the External Partner in accordance with the provisions of this Agreement. The Parties hereby agree that the IPHCC Member shall have the right to seek an immediate injunction and any other available remedy it deems necessary before a court of competent jurisdiction, with regard to any breach or threatened breach of the provisions of this Agreement relating to the Data and to specifically enforce such provisions, in addition to (where applicable) a right to monetary damages or any other remedy available to the IPHCC Member and/or any affected individuals under applicable law or this Agreement.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DISPUTE RESOLUTION & BREACH PROCEDURES		
9.8 The Parties [and/or Data Committee] shall maintain a record of all Breaches. **9.9** In the event of a Breach, the respective Party shall have the obligation to notify the affected individual(s), as required. Both Parties will collaborate to ensure appropriate stakeholders are involved in the notification process. **Obligation to Remedy Breach** If a Party has breached this Agreement, it shall immediately make best efforts to remedy the Breach as soon as possible. **Dispute Resolution** The Parties agree that they shall at all times attempt to resolve any disputes with respect to issues arising out of the Agreement in an amicable fashion, through negotiation. The Parties agree that the existence of any dispute shall not interfere with the performance by the Parties of their respective obligations under the Agreement. The steps to resolve a dispute shall be as follows: Any Party shall notify the other by written notice (“Notice”) of the existence of a dispute and a desire to resolve the dispute.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DISPUTE RESOLUTION & BREACH PROCEDURES		
The Party receiving such Notice shall have a reasonable period of time to consider and, if it believes fit, address the concern, such period not to exceed 15 business days unless the Parties agree otherwise. If the dispute is not addressed to the reasonable satisfaction of the Party who provided the Notice of same, the Parties shall consult in good faith to discuss the dispute and possible remedial action which could be taken to address it. This step shall be completed within 30 business days after the Notice is first received, unless the Parties agree otherwise. If the Parties jointly submit the dispute to mediation, the Parties will jointly appoint a mutually acceptable mediator, seeking assistance from the Ontario Superior Court of Justice if they have been unable to agree upon such appointment within fifteen (15) business days following the Parties' agreement to mediate the dispute in accordance with the National Mediation Rules of the ADR Institute of Canada, Inc. The place of the mediation shall be [insert location], Ontario and the language of the mediation shall be in English.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DISPUTE RESOLUTION & BREACH PROCEDURES		
The costs of the mediator will be shared equally between the Parties. Each Party will bear its own costs incurred for its participation in the mediation including costs of representation by counsel. If all of the efforts to resolve the dispute are unsuccessful within thirty (30) business days of entering into an agreement to mediate, and the Parties are otherwise unable to resolve the matter, the matter shall be referred to an arbitration to be conducted in the Province of Ontario. A single arbitrator shall be chosen by mutual agreement between the Parties and the decision of the arbitration shall be final and binding on the Parties. If the parties fail to agree upon an arbitrator within ten (10) days of delivery of the arbitration notice, either Party may apply to the Ontario Superior Court to appoint such arbitrator, who shall be a person who has been called to the bar of the province of Ontario. **Termination for Breach** **9.13** If the breaching Party does not remedy the breach to the satisfaction of the other Parties, any one of the non-breaching Parties may, by notice in writing, immediately terminate this Agreement.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
DISPUTE RESOLUTION & BREACH PROCEDURES		
Indemnification **9.14** Unless prohibited by law, the External Partner agrees to indemnify and hold harmless from any damages, costs, liability, expenses, losses, and settlement amounts (a "Claim") that the IPHCC Member may incur or suffer relating to breach of this Agreement by the External Parter or flowing from information shared by the External Partner with contractors or third parties, except where it is due to the negligent actions or omissions of the IPHCC Member. **9.15** The IPHCC Member shall provide reasonable assistance, information, and authority to permit the External Partner to defend and settle a Claim. The IPHCC Member may, at their own cost, retain legal counsel for the purposes of observing the defence and settlement of a Claim. **Liability Insurance** **9.16** Each Party shall maintain in full force and effect general liability insurance sufficient to cover its liability under this Agreement. Each Party will give 30 days prior written notice of any material change to, cancellation, or non-renewal of its insurance coverage.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
GENERAL		
Governing Laws This agreement is governed by the laws of the Province of Ontario, without regard to conflict of laws principles that would require the application of the laws of another jurisdiction. The parties irrevocably submit to the exclusive jurisdiction of the courts of Ontario. **Severability** **10.2** If any part, term or provision of this Agreement shall be held illegal, unenforceable, or in conflict with any law of a federal, provincial or local government having jurisdiction over this Agreement, to the extent practicable the validity of the remaining portions or provisions shall not be affected thereby and the Parties shall forthwith move to amend this Agreement to capture the spirit of the provision held to be illegal, unenforceable, or in conflict with any law. **Interpretation** **10.3** Any reference in this Agreement to gender includes all genders, and words importing the singular include the plural and vice versa. **10.4** The inclusion of a table of contents, the division of this Agreement into articles and sections and the insertion of headings are for convenient reference only and are not to affect or be used in the construction or interpretation of this Agreement.	These are standard clauses that should be included. **Governing Laws:** This section sets out which laws (i.e.. Provincial or Federal) that apply to this agreement. **Assignment:** This section prevents either Party from transferring their obligations to a third party. However, it may be that you want the option to assign the agreement. In that case, you will want to specify who it can be assigned to and under what conditions. **Costs:** The External Partner may assume the costs for managing the data it uses pursuant to this Agreement, or the Parties could arrange for cost-sharing. **Waiver:** It is advisable to stipulate that there is no implied waiver of rights to enforce the Agreement resulting from a failure to act or delayed action.	1. What laws govern the agreement? 2. Can the rights and obligations in the Agreement be assigned to a third party? If so, how? 3. Can the Agreement be amended? What is the process for that? 4. Who bears the cost for sharing the Data and compliance with the Agreement?

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
GENERAL		
Amendments **10.5** This Agreement may not be amended except upon mutual agreement, in writing, by the Parties. Any amendment to this Agreement will only be effective from the date of approval. **Assignment** **10.6** No part or whole of this Agreement may be assigned by either Party [unless prior written consent of the other is obtained. The consent required shall not be unreasonably withheld or delayed, and if any requested assignment is not objected to within 30 days of such written request, the failure to object shall be deemed consent for the purposes of this section]. **Costs** 10.7 Each Party shall be responsible for their own costs [including legal costs] relating to the maintenance of the Data that is the subject of this Agreement. **Whole Agreement** **10.8** This Agreement [including the Schedules] constitutes the whole Agreement between the Parties unless duly modified in writing and signed by both Parties.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
GENERAL		
Notices **10.9** Every notice or written communication provided for or permitted by this Agreement shall be in writing and delivered [by email and/or registered mail] to: [Contact information] [Contact information] **Waiver** **10.10** No waiver of any term of this Agreement is binding unless it is in writing and signed by all the Parties entitled to grant the waiver. No failure to exercise, and no delay in exercising, any right or remedy under this Agreement will be deemed to be a waiver of that right or remedy. No waiver of any breach of any term of this Agreement will be deemed to be a waiver of any subsequent breach of that term.		

TEMPLATE TEXT	COMMENTS	QUESTIONS TO ASK
SIGNATURES		
[signature] [name] [title] **I have the Authority to Bind the IPHCC Member** [signature] [name] [title] **I have the Authority to Bind the External Partner**		

APPENDIX SAMPLE OF PERMITTED USES

ROLE	CAN VIEW	ALLOWED ACTIONS IN PATIENT RECORDS
Administrator	All	Notes
Data Entry Clerk	Only messages	None/Can only view messages and perform data imports
Doctor	All	All, including prescriptions
Emergency or On-Call Doctor	All	All, including prescriptions
Medical Student	All	Notes, immunizations, and treatments
Mental Health Counsellor	All	Notes, immunizations, and treatments
Nurse	All	Notes, immunizations, and treatments
Nurse Practitioner	All	All, including prescriptions
Pharmacist	All	All, including prescriptions
Psychiatric Nurse	All	Notes, immunizations, and treatments
Psychiatrist	All	All, including prescriptions
Resident	All	All, including prescriptions; cannot lock notes
Administrative Assistant	All	Notes
Social Worker	All	Notes, immunizations, and treatments

Appendix E: Relationship Agreement Template

THIS RELATIONSHIP AGREEMENT (the "Agreement") made and entered into this _____ day of _____, _____ (the "Execution Date"),

BETWEEN:

(Party 1)
- and -
(Party 2)
(Individually the "Party" and collectively the "Parties").

PARTNER INFORMATION:

(Background Information on Party 1)

(Background Information on Party 2)

IN CONSIDERATION OF the Parties entering into this Agreement, the Parties to this Agreement agree as follows:

This Relationship Agreement sets the terms and understanding between (Party 1) and (Party 2) to move forward and continue with collaborative efforts currently in place to support Indigenous health with an emphasis on diabetes care.

Purpose and Intent

In acknowledgement of Indigenous legal principles that have guided Indigenous People since time immemorial, we first give recognition to the ancestors, spiritual connections, lands, waters, air and living beings that connect us to one another. This recognition reminds us of our responsibilities to creation and to each other, and that Indigenous health requires connection.

This Relationship Agreement is signed in the context of a continuing journey of truth-telling about the history of Indigenous Peoples and is recognized as a step towards healing and reconciliation. Truth-telling acknowledges the positive stories, strengths, and unique knowledge, as well as the injustices faced by Indigenous Peoples throughout our shared history.

This Agreement seeks to right the negative impact of colonial processes on Indigenous Peoples' health and wellbeing and create space for Indigenous voices at all governance and decision-making levels without prejudice or oppression.
As Parties, (Party 1) and (Party 2) have come together in the spirit of:

- Resurgence of Indigenous health in Indigenous hands,
- Reconciliation as a step toward healing,
- Transformation to Indigenous health pathways that clients can trust in a way that empowers them.
- Recognizing Culture-as-Healing and the importance of wholistic health care that encompasses not only the physical aspect of self, but the mental, emotional, and spiritual as well.

The Parties are aware of, agree to, and support one another's mission and vision. Together, the Parties envision an ongoing relationship for as long as there is Indigenous health. As both Parties evolve, the relationship will continue, regardless of any changes in leadership.

Relationship Foundations

This relationship is rooted in the following principles:

Culturally Safe: Parties create an environment that is free from racism and discrimination for everyone. This will be actualized by both Parties ensuring that all employees within their individual organizations are offered Indigenous cultural safety training.

Mutual Benefit: Parties view the collaborative relationship as beneficial. Any shared deliverables will be guided by the development of a workplan agreed to by both parties.

Shared Decision-Making: Parties work collaboratively for a common purpose and make space for all voices when making decisions pertaining to this relationship.

Fair & Equitable: equal participation, open and transparent actions, and respect for each other.

Reflective: Parties are reflective and evaluate regularly and will adjust if needed.

Solutions-Oriented: Parties review and respond to problems in a thoughtful and timely way, and guide developed resources, that are shared among the parties, with a trauma-informed lens.

Communicative: Parties have open, transparent, and honest dialogue and will establish a meeting schedule among the parties to help inform the relationship. This will be actualized by Parties being reflective and evaluate regularly through meeting twice a year and as needed. In addition, Parties will ensure timely response to shared mission/goals inquiries.

Transformative: Parties work collaboratively to change systems to ensure the clients we serve are supported in their health choices. This will be actualized by Parties actively working together to create a work environment that is free from racism and discrimination for everyone. As well as being mutually responsive and supportive to incidents brought forward in support of Indigenous people navigating the system.

Common Vision: As Parties, we have an opportunity to work collaboratively for greater collective benefits. We will work jointly on initiatives that are relevant to both parties and will improve Indigenous health outcomes, remove barriers for clients on their health journeys, seek solutions to significant systemic issues and evaluate continually for the purpose of transformation.

Organizational awareness: Parties are aware of one another's capacity and scope (being aware of the high demands to make sure we are supporting rather than putting pressure on one another). This will be operationalized by:

- Hosting a mini gathering between teams to understand each other and gain a better understanding of each other's strengths.
- Ensuring the most appropriate Party is represented on specific tables such as committees, working groups, government initiatives etc. Sharing information where appropriate on who is being supported and how so that work continues to harmonize.
- The relationship will take time to build and there is a recognition that there will be growing pains along the way. The Parties will ensure that what is promised is honoured and only commit to activities that can be fulfilled. Any challenges in doing so will be shared openly and honestly so that the parties can adjust accordingly.

Capacity building: The Parties will seek opportunities to build capacity within both organizations, among clients, and external partners where appropriate. This will be actualized through collaboration on and sharing of train the trainer opportunities, resource development, event partnership. Any agreed to activities will be reflected in a shared workplan to help guide the deliverables.

Knowledge translation: The Parties will support one another on broadly sharing Indigenous health information in order to increase reach/awareness of events/sessions, resources and tools that can be offered to organizations and IPHCOs.

Collective Voice: There is strength in numbers. The Parties agree to support each other in the realm of advocacy (e.g., Indigenous Cultural Safety, funding opportunities where possible, outdated policies), as well as explore strategic support on moving priority areas forward to collectively be a catalyst to create an environment for change.

Proposal support: The Parties will seek opportunities for collaboration on proposal submissions where applicable and where commonalities exist, support one another with relevant proposals (e.g., letters of support). In this area of the relationship, the Parties will support but do not speak on behalf of one another.

Overcoming Differences

The process of overcoming challenges speaks to the nature and foundation of a culture in a similar way as ceremony and language does. The ability to look to traditional ways of knowing and doing during these times speaks to how well those teachings are embodied. Conflict is a natural part of life; it is not negative or positive. The greatest learning and respect lie with how we choose to deal with the conflict.

Unresolved conflict can lead to broken communication and relationships dissolving. As Parties, we value the strength of this relationship and commit to participating in a process of resolving conflict in a way that is:

- Open
- Honest
- Respectful
- Fair
- Intent on finding resolution

Any difference between the Parties arising out of the interpretation or application of this Agreement will be settled amicably through informal discussion and resolution. The issue will be brought to the attention of respective leadership team, conflict resolution principles will be applied, along with the Seven Grandfather teachings, talking circles and bringing in support from Elders and/or Knowledge Keepers.

Fostering the Relationship

As Parties, we have a responsibility to the spirit of this agreement. The acknowledgement of this spirit requires that we treat this agreement as a living document, by continuing to breathe life into its intent. Each year as Parties, we will reflect on the progress of the relationship by undertaking an evaluation process and undertake a feasting ceremony to celebrate the work done the previous year, set the intention for the coming year, and recognize creation that has allowed us to do this important work.

When meeting, Parties will take notes, highlighting agreed upon activities. At points of reconnecting, Parties will review progress against activities. Throughout the year, the Parties will populate a repository of collaborative activities and reflect on them at the feast.

Data Governance

The Parties recognize and respect the right to Indigenous self-determination and autonomy. This Agreement does **not represent** a data sharing agreement. When requested, and appropriate consents have been granted Parties may choose to share Indigenous specific data with Parties for the purpose of providing or improving culturally safe and relevant health services. The sharing of information will be respectful of privacy and confidentiality principles. In addition, will be responsible for coordinating its terms in accordance with applicable laws and community input.

Binding Effect

This agreement is not intended to create any binding contractual or financial obligations. Any legally binding financial commitments or other obligations be accompanied by Service Agreements and contracts that clearly outline deliverables among all parties.

Further, this agreement does not have the authority, nor the intent, to address the range of issues arising from Aboriginal and Treaty rights.

Termination

This Agreement may be terminated by either party upon written notice, provided that the terms of this agreement shall remain in
effect until such termination occurs.

Amendments

This Agreement may not be amended in whole or in part without the unanimous written consent of both Parties.

Governing Law:

This Agreement will be construed in accordance with and exclusively governed by the laws of The Province of Ontario.

Term of the Agreement

Enter term here.

Signatures

IN WITNESS WHEREOF the Parties have duly affixed their signatures under hand on this day of, _____, _____.

X _____ X _____

Name (Party 1)

Name (Party 2)

If signed in person, add an acknowledgement of the land where the agreement was signed.