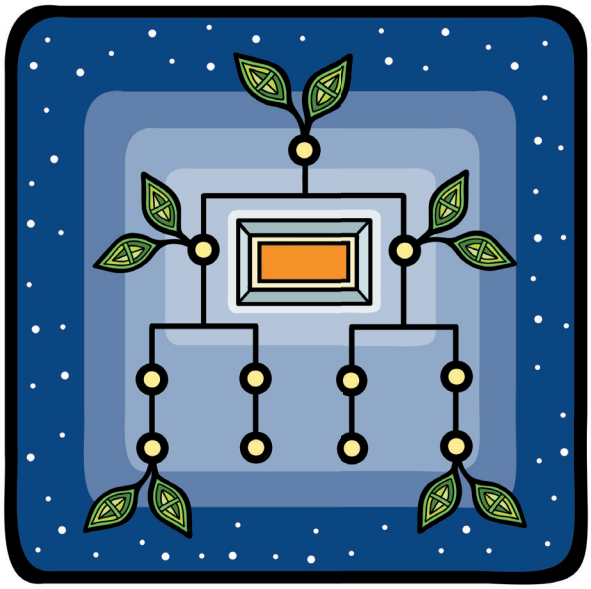


INDIGENOUS DATA **PRIVACY** FRAMEWORK

INDIGENOUS PRIMARY HEALTH CARE COUNCIL

TABLE OF CONTENTS

In mid-March 2022, the Indigenous Primary Health Care Council (IPHCC) engaged Morgan Privacy Consulting (MPC) to undertake several deliverables as part of a privacy and information security consulting engagement. One of these deliverables was the development of an "Indigenous Privacy Framework"[1] against which Privacy Impact Assessments can be conducted.

To IPHCC's knowledge, no such Indigenous Privacy Frameworks have ever been documented or made widely-available for use. Existing privacy frameworks, such as the Canadian Standards Association Model Code for the Protection of Personal Information (the "CSA Model Code") and the Generally Accepted Privacy Principles (GAPP) of the American Institute for Chartered Public Accountants and CPA Canada, offer a structured, repeatable way of assessing privacy impact.

However, these existing frameworks are based exclusively on non-Indigenous, individualistic notions of privacy.

Although there may be isolated examples in which Indigenous perspectives and considerations have been reflected in past privacy impact assessment work, it is fair to say that most Privacy Impact Assessments to date have not approached Indigenous perspectives and considerations in any structured, repeatable way.

As work on an Indigenous Privacy Framework unfolded, it became clear that this early work should be positioned as a Framework to better represent the intention that the Framework be refined through input and experience prior to adoption.

Notably, neither the IPHCC members nor the privacy community (both Indigenous and non-Indigenous) have yet had an opportunity to comment on the Framework, and the Framework has not yet been challenged by way of a "real-life" assessment.

1 For brevity, the report will often use "IPF" or "Framework".

INTRODUCTION

Moreover, IPHCC and MPC have identified the need to develop an "implementation guide" to offer greater insight on how to apply the Framework in a "real-life" assessment. Once the Framework is circulated for further input, and eventually put to the test, strengths and weaknesses will be revealed, and the Framework can be refined into a product that can be adopted and promoted.

This document is a report summarizing the Framework and its development. The Framework was developed during May and June 2022, with further refinement of the Framework through to September 2022. IPHCC intends to develop an implementation guide to support the Framework over the course of fall 2022 and winter 2023.

LITERATURE REVIEW

The creation of the Indigenous Privacy Framework was supported by a literature review on “Indigenous privacy impact assessment” (the “Review”) – the “Review” was an earlier deliverable under the MPC engagement. The goal of the Review was to find examples, or at least discussion, of Indigenous considerations in privacy impact assessment work that could be used to support a Framework.

Originally, the Review intended to focus on results that featured “Canadian” Indigenous considerations and perspectives; however, the low number of findings did not warrant restricting the scope to the Canadian context. Moreover, the low number of relevant publications a during early searches related to “Indigenous privacy assessment” motivated the inclusion of additional search terms to find publications that more broadly spoke to “Indigenous privacy”.

Even with this expanded scope, the Review was only able to find about a dozen relevant or semi-relevant publications. to recognize the distinction between Indigenous information governance and Indigenous privacy.

Most notably, none of the publications uncovered by the Review offer a ready-made framework that the IPHCC might have adopted; however, each publication offered some “food for thought” that could be used in the development of an IPF. Unfortunately, none of the publications uncovered by the Review spoke materially to Inuit or Métis privacy considerations that might be distinct from First Nations privacy considerations.

As expected, many of the Review’s investigative paths led to the OCAP® framework of the First Nations Information Governance Centre. The OCAP® framework is often incorrectly understood to be a privacy framework, which it is not. Rather, the OCAP® framework frames privacy as a component of information governance, introducing notions of “community-level” privacy to complement well-established notions of “individual-level” privacy. Although certain OCAP® principles are very relevant to an Indigenous Privacy Framework, particularly the “ownership” and “control” principles, it is important to recognize the distinction between Indigenous information governance and Indigenous privacy.

KEY FEATURES

3.1 CSA Model Code as a Starting Point

As discussed in Section 1, the CSA Model Code (CSA Q830:03 (R2019)) offers a structured, repeatable way of assessing privacy impact based on individualistic notions of privacy. The Model Code is the basis for most Canadian privacy law (including health privacy law) and existing Canadian organizational privacy policy.

Because the CSA Model Code plays such an important role in Canadian privacy, and because "individual-level" privacy considerations remain as important in an Indigenous context as they do in a non-Indigenous context, the Framework leverages the principles of the CSA Model Code as a starting point. More specifically, the Framework incorporates the CSA Model Code principles and their explanatory clauses[1] "as is" (as it pertains to individual-level privacy), establishing supplemental principles and explanatory clauses that also apply in an Indigenous context.

Although the privacy profession's application of the CSA Model Code over the last 25 years has likely revealed ways in which certain phrasings within the Model Code are problematic or could be improved, the IPF avoids the unintended consequences that might arise from "tinkering" with the existing CSA Model Code to "improve" how it addresses individual-level privacy.

That being said, the Framework is based on a definition of "personal information" which differs from that in the CSA Model Code in order to better accommodate Indigenous oral traditions. This matter is discussed further in Section 4.1. When considers how one might apply the IPF, it is intended that the CSA Model Code potion of the IPF would be applied using the revised definition of "personal" information.

In developing the supplemental principles and explanatory clauses that apply in an Indigenous context, each principle and clause of the CSA Model Code was examined with respect to the question, "What Indigenous considerations, such as Indigenous perspectives on privacy (including "community-level" privacy), Indigenous governance, and Indigenous self-determination, are missing or under-represented?". Having supplemented each principle and explanatory clause of the CSA Model Code, further thought was given to each of the CSA Model Code principles to ask, "What is still missing?" – answers to this question were used to establish further supplemental principles or explanatory clauses as required.[2]

1 As indicated in the CSA Model Code, "Each of the principles is followed by a commentary on the principle. The commentaries are intended to help individuals and organizations understand the significance and the implications of the principles."

2 For those who are familiar with past work on Indigenous privacy, it should be noted that the Framework's use of the CSA Model Code as a starting point is markedly different from past efforts to leverage the CSA Model Code in an Indigenous context. Specifically, the Literature Review (see Section 2) identified a "Model Privacy Code for a First Nation", which was originally developed for the First Nations and Inuit Health Information System Privacy Committee of Health Canada and included in a toolkit developed by the First Nations Centre (FNC) of the National Aboriginal Health Organization (NAHO).

This "First Nations Model Code" is a derivative of the CSA Model Code. For the most part, the First Nations Model Code simply replaces the term "organization" (found in the CSA Model Code) with the term "First Nation", with little consideration of how privacy concepts might be perceived or applied differently in a First Nations context – as expressed in the preamble to this First Nations Model Code, it "addresses personal information privacy only. It does not address [community-level privacy] concerns".

3.2 Respecting the Differences between Indigenous Groups and Communities

In supplementing the CSA Model Code to address Indigenous considerations, the Framework tries to respect the differences that exist between Indigenous groups and Indigenous communities, particularly within Ontario (where the IPHCC intends to apply an Indigenous Privacy Framework).

For example, the governance structures supporting Ontario First Nations and Ontario Métis do not apply to the Inuit community living in Ontario. Similarly, one First Nations perspective on “community-level” privacy may differ from another, both of which may differ from Ontario Métis and Inuit.

Interestingly, an unintended consequence of this attempt to respect the diversity of Indigenous groups and communities is that the Framework can likely be tweaked to establish other privacy assessment frameworks that can be used by non-Indigenous groups to uphold privacy in a way that respects their unique perspectives and considerations.

THE FRAMEWORK

4.1 Key Terms

4.1.1 Defined Terms

The Indigenous Privacy Framework defines three key terms: "personal information", "Indigenous population", and "Indigenous population information".' [1]

- The term "personal information" is defined in the CSA Model Code as "information about an identifiable individual that is recorded in any form". The two key elements of this definition are "identifiable" and "recorded". Because of the importance of oral traditions in an Indigenous context, the Framework drops the requirement that the personal information be recorded. The Framework does not further define "identifiability", choosing instead to rely on the understanding that has developed over time since the original publication of the CSA Model Code.

- The concepts of "Indigenous population" and "Indigenous population information" are not found in the CSA Model Code.

1 In the same way that the terms "personal information" and "personal health information" are often referred to as "PI" and "PHI", respectively, it is thought that the terms "(Indigenous) population information" and "(Indigenous) population health information" might similarly be referred to as "IPI" and "IPHI", respectively, when applying the Framework.

Personal Information:

Information, in any form, about an identifiable individual. Examples of "personal information" include:

- a person's salary;
- a person's health records;
- a person's community, First Nation, heritage, nationhood, ancestry, or treaty association (e.g. Akwesasne, Attawapiskat, Barrie, Cree, Inuk, Japanese, Labrador Inuit Land Claims Agreement, Métis, Mohawk, Navajo, Ojibway, Plains Cree, Robinson-Huron Treaty, Scottish, Tibetan, Treaty 3);
- a story about the origins of an individual's Indigenous/traditional name (whether written or spoken).

Indigenous Population:

Individuals exhibiting a common characteristic. Examples of "Indigenous populations" include:

- members of a First Nation;
- a group of Indigenous people of the same nationhood or ancestry (e.g. Cree, Inuit, Métis, Mohawk, Mushkegowuk, Nunatsiavummiut, Ojibway);
- individuals residing in a postal code which captures a First Nation community;
- the Indigenous people who hunt, trap, or harvest in a specific geographic area, along a specific coastline, or along a specific waterway;
- Inuit living in the Ottawa area;
- Indigenous persons living in the Greater Toronto Area.
- students at a college that self-identify[2] as Métis; and
- members of a professional association that self-identify[2] as Indigenous

Indigenous Population Information:

Information, in any form, predominantly about an Indigenous population. Examples of "Indigenous population information" include:

- a traditional Mohawk story (whether written or verbally-recounted);
- the median life-expectancy of individuals residing in a postal code which captures a First Nation community;
- the rate of diabetes amongst Inuit living in the Ottawa area;
- the employment rate of Indigenous persons living in the Greater Toronto Area;
- an aggregate-level statistic about the income of students at a college that self-identify as Métis (e.g. averages, distribution by salary ranges, comparisons against the total student population); and the percentage of self-identifying Indigenous members of a professional association with graduate degrees.

---

2 Different organizations/entities may have different definitions or understandings of what it means to "self-identify".

Notes

- *The definition of "Indigenous population information" requires that the information be predominantly about an Indigenous population. So, for example, the rate of diabetes amongst all persons living in the Ottawa area would not be considered Indigenous population information – though there are many Indigenous persons living in the Ottawa area, the information is not predominantly about Indigenous persons in Ottawa (rather, the information is about all persons living in Ottawa, whether they are Indigenous or not).*
- *The Indigenous population associated with different Indigenous population information could vary even when the various pieces of information are determined from the same set of individuals. For example, consider a group of Inuit living in Ottawa. In the case of average salary data based on this group, the associated Indigenous population might be understood to be Inuit living in Ottawa*[1]*. However, in the case of a collection of traditional stories collected from the same group of Inuit living in Ottawa, the associated Indigenous population might be understood to be all Canadian Inuit – the stories likely represent Inuit from across Canada.*

1 It could be argued that the associated Indigenous population might be understood to be Inuit living in major cities in Southern Ontario, although salary information is reasonably unique to a city.

4.1.2 Undefined Terms

To allow the understanding of certain concepts to evolve over time, as was the case with the CSA Model Code, the IPF has chosen not to define certain key terms. Specifically, the following key terms have not been defined in the Framework.

"Recognized representative" (of an Indigenous population/subpopulation). Instead, the IPF provides some examples of parties that might act as "recognized representative" in certain context.

"Meaningful" (consent or consultation). Instead the IPF establishes minimum requirements for "meaningful" consent and "meaningful" consultation.

"Reasonably foreseeable" (implications of withdrawing consent). Instead, the IPF provides some examples of reasonably foreseeable implications of withdrawing consent in specific situations.

"Deceptive" (consent or consultation). Instead, the IPF provides some examples of deceptive practices that might be used in seeking consent or undertaking consultation.

"Culturally appropriate" (ways/communication). Instead, the IPF provides some examples of practices that might be culturally appropriate or inappropriate.

4.2 Supplementary Principles and Explanatory Clauses

4.2.1 Accountability

The Indigenous-centric supplemental principle arising from the CSA Model Code "Accountability" principle is presented in Table 1.

For the most part, the Framework simply extends the original principle to Indigenous population information. However, in doing so, the IPF avoids reusing the term "control" to establish the condition under which an organization becomes accountable for information – to reuse this language would be contrary to many expressions of Indigenous sovereignty and data governance (including those arising as part of Inuit Qaujimajatuqangit[1], and particularly those captured by the OCAP® and OCAS[2] principles of "control"). Instead, the Framework uses the word **"hold"**, a more neutral term that is not contrary to the "control" and/or "possession" that an Indigenous population might wish to maintain with respect to information about themselves.

1 Roughly translated, Qaujimajatuqangit refers to "Inuit traditional knowledge"

2 The Manitoba Métis OCAS principles are "ownership", "control", "access", and "stewardship". For more on these principles, see the 2015 Annual Report of the Manitoba Métis Federation and/or the University of Manitoba Faculty of Health Sciences report entitled "Framework for Research Engagement with First Nation, Metis, and Inuit Peoples".

Table 1

Supplemental principles for the Indigenous Privacy Framework based on the CSA Model Code's "Accountability" principle.

CSA Model

Accountability (Principle 1): An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-today collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon

1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

1.4 Organizations shall implement policies and practices to give effect to the principles, including

a. implementing procedures to protect personal information;
b. establishing procedures to receive and respond to complaints and inquiries;
c. training staff and communicating to

Indigenous Privacy Framework

Accountability (Principle IPF1): An organization is responsible for **Indigenous population information it holds** and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

IPF 1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of **Indigenous population information**. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

IPF 1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

IPF 1.3 An organization is responsible for I**ndigenous population information it *holds***, including information that has been transferred to a third party for processing. The organization should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

IPF 1.4 Organizations shall implement policies and practices to give effect to the principles, including

a. implementing procedures to protect **Indigenous population information**;
b. establishing procedures to receive and respond to complaints and inquiries;
c. training staff and communicating to staff information about the organization's policies and practices; and
d. developing information to explain the organization's policies and procedures.

4.2.2 Identifying Purposes

The Indigenous-centric supplemental principle arising from the CSA Model Code "Identifying Purposes" principle is presented in Table 2.
For the most part, the Framework simply extends the original principle to Indigenous population information. However, in doing so, it recognizes and addresses the fact that the CSA Model Code fails to directly address the creation of personal information (e.g. an audio streaming service creates information about how many hours per day an individual listens to content). Yet, most (if not all) Indigenous population information must first be created. For example, rates of diabetes within a predominantly-Métis community must be prepared based on the personal health information of members of the community. Or, as another example, a story must be created before it is told.[1]

That being said, the Framework does not wish to be at odds with the protections afforded to Indigenous cultural property by the United Nations Declaration on the Rights of Indigenous Peoples. As such, the supplemental principles found in the IPF are not intended to be applied to the creation of cultural property (e.g. stories and ceremonies) or to restrict the creators and owners[2] of cultural property who collect, use, disclose, or otherwise handle cultural property in culturally appropriate ways. However, the IPF does apply to non-owners/non-creators of cultural property. For example, the IPF would apply to university researcher documenting Indigenous creation stories.

As well, in extending the original principle, **the Framework requires that organizations are able to explain, *to anyone*, the purposes for which Indigenous population information is being collected or created.** Although it could be argued that the emphasis should be on making Indigenous persons (or the members and representatives of the Indigenous population associated with the information) aware of these purposes, requiring the organization to be able to explain to anyone how their work impacts Indigenous populations is more consistent with the spirit of reconciliation.

---

1 Depending on the Indigenous population, stories or ceremonies might not be seen as being "created", but rather "received" (e.g. from ancestors or spirits). As discussed in Section 3.2, the Framework has tried to respect the differences between various Indigenous communities and groups; however, the Framework occasionally simplifies language in the interest of readability and ease-of-application.

2 "Creation" and "ownership" of cultural property are not clear-cut concepts. For example, it is not necessarily clear that a member of a First Nation should be entitled to share the details of a ceremony specific to their First Nation (the First Nation may not see "ownership" as vesting in the individual members). Those applying the Framework are encouraged to consider matters related to the "creation" and "ownership" of cultural property on a case-by-case basis, respecting the viewpoints of the Indigenous populations under consideration.

Table 2:

Supplemental principles for the Indigenous Privacy Framework based on the CSA Model Code's "Identifying Purpose" principle.

CSA Model

Identifying Purposes (Principle 2): The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

2.1 The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Principle 8) and the Individual Access principle (Principle 9).

2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Principle 4) requires an organization to collect only that information necessary for the purposes that have been identified.

2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Principle 3).

2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

2.6 This principle is linked closely to the Limiting Collection principle (Principle 4) and the Limiting Use, Disclosure, and Retention principle (Principle 5).

Indigenous Privacy Framework

Identifying Purposes (Principle IPF2): The purposes for which **Indigenous population information** is collected ***or created*** shall be identified by the organization at or before the time the information is collected ***or created.***

IPF 2.1 The organization shall document the purposes for which **Indigenous population information** is collected ***or created*** in order to comply with the Openness principle (Principle IPF8) and the Individual Access principle (Principle IPF9).

IPF 2.2 Identifying the purposes for which **Indigenous population information** is collected ***or created*** at or before the time of collection ***or creation*** allows organizations to determine the information they need to collect ***or create*** to fulfil these purposes. The ***Limiting Collection and Creation*** principle (Principle IPF4) requires an organization to collect ***and create*** only that information necessary for the purposes that have been identified.

IPF 2.3 When collecting Indigenous population information, the identified purposes should be specified at or before the time of collection to the ***party*** from which the **Indigenous population information** is collected.

Note that communication of the identified purposes for which Indigenous population information is created is addressed through the Consent and Communication Principle (Principle IPF3).

IPF 2.4 When **Indigenous population information** that has been collected ***or created*** is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, consent ***or consultation*** is required before information can be used for that purpose. For an elaboration on consent and consultation, please refer to the ***Consent and Consultation principle*** (Principle IPF3).

IPF 2.5 Persons collecting ***or creating*** **Indigenous population information** should be able to explain the purposes for which the information is being collected ***or created.***

IPF 2.6 This principle is linked closely to the ***Limiting Collection and Creation*** principle (Principle IPF4) and the Limiting Use, Disclosure, and Retention principle (Principle IPF5).

4.2.3 Consent or Consultation

The Indigenous-centric supplemental principle arising from the CSA Model Code "Consent" principle is presented in Table 3.

The supplemental principle reframes the original principle as "Consent or Consultation". Although consent aligns with Indigenous sovereignty and data governance objectives (particularly the OCAP® and OCAS principles of "ownership" and "control"), the supplemental principle allows the collection, creation, use, or disclosure of Indigenous population information based upon a mixture of consent and consultation.

Unlike the CSA Model Code which simply allows exceptions to consent, the Framework offers consultation as an equally-valid alternative to consent. In some circumstances, consultation may be a more appropriate basis (than consent) on which to proceed with the creation, collection, use, or disclosure of Indigenous population information. Or, in other cases, obtaining consent from a population (or a subpopulation of it) may be impractical or impossible, even when consent can be obtained by way of recognized representatives that consent on behalf of various segments of the population (or subpopulation).[1] For example, there may not be a recognized representative of a subpopulation (or the only recognized representative may not be willing or able to entertain the matter) and there may be too many individual subpopulation members to contact individually (or no way to reach them).

Note that the supplemental principle retains the "except where inappropriate" language found in the original principle – as the note to the original principle suggests, there are conceivable circumstances where it would be inappropriate to seek consent or undertake consultation, such as in the case of public health emergencies.

The Framework avoids prescribing how consultation should be undertaken – consultation is not a core privacy concept and there is already a substantial body of knowledge associated with consultation that the IPF need not add to. However, the Framework requires that consultation be meaningful – it cannot simply be "for show". Similarly, the Framework also introduces a parallel requirement that consent be meaningful, which is a slight reframing of the consent-related expectations found in the CSA Model Code. To these effects, the IPF establishes several conditions that must be met for consent or consultation to be considered "meaningful", including conditions related to cultural appropriateness.

---

1 The "Consent or Consultation" principle of the Framework defines the consent of a subpopulation as follows. "The consent of a subpopulation (possibly the entire Indigenous population) shall consist of one or more consents that collectively represent every member of the subpopulation. These consents shall be obtained either from a) the member themselves (or their substitute decision maker if the circumstances allow); or b) a recognized representative which provides consent on behalf of a segment of the subpopulation which includes the member."

Perhaps most notably, if consultation is used, any collection, creation, use, or disclosure of the Indigenous population information must reflect what is heard during consultation. Exactly how the collection, creation, use, or disclosure sufficiently reflects what is heard during consultation might vary according to the circumstances: for example, if there is strong majority support for the planned activities, then minor modifications to accommodate reasonable dissenting opinions might suffice to proceed. Regardless, by establishing "reflect" as the applicable standard, the Framework does not explicitly require consensus to proceed with the collection, creation, use, or disclosure.

Not only must consultation be "meaningful", but any choice to proceed with a collection, creation, use, or disclosure of Indigenous population information based on consultation must respect the decision-making customs of the applicable population or subpopulation. For example, if consensus-based decision making is a custom of the population or subpopulation, then a lack of consensus (or, at least, a significant deviation from consensus) during consultation should, in many cases, indicate that the activity involving Indigenous population information should not proceed in that particular instance.

Finally, the supplemental principle does not repeat the phrase "knowledge and consent" found in the CSA Model Code. The reference to "knowledge" is redundant because meaningful consent or consultation requires that the consenting or consulted party be sufficiently informed.

Table 3:

Supplemental principles for the Indigenous Privacy Framework based on the CSA Model Code's "Consent" principle.

CSA Model

Consent (Principle 3): The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

Indigenous Privacy Framework

Consent or Consultation (Principle IPF3): The consent ***or consultation*** of **the Indigenous population** is required for the ***creation***, collection, use, or disclosure of **Indigenous population information**, except where inappropriate.

Note: In certain circumstances, Indigenous population information can be created, collected, used, or disclosed without seeking consent or undertaking consultation. For example, seeking consent and undertaking consultation might be considered inappropriate during the response to a public health emergency or other situation where creation, collection, use, or disclosure of Indigenous population information is required to support quick response – in such circumstances, the need for urgent action may only allow for notification of the Indigenous population, through their recognized representatives, after the creation, collection, use, or disclosure. As another example, there may be a requirement to create, collect, use, or disclose Indigenous population information under law.

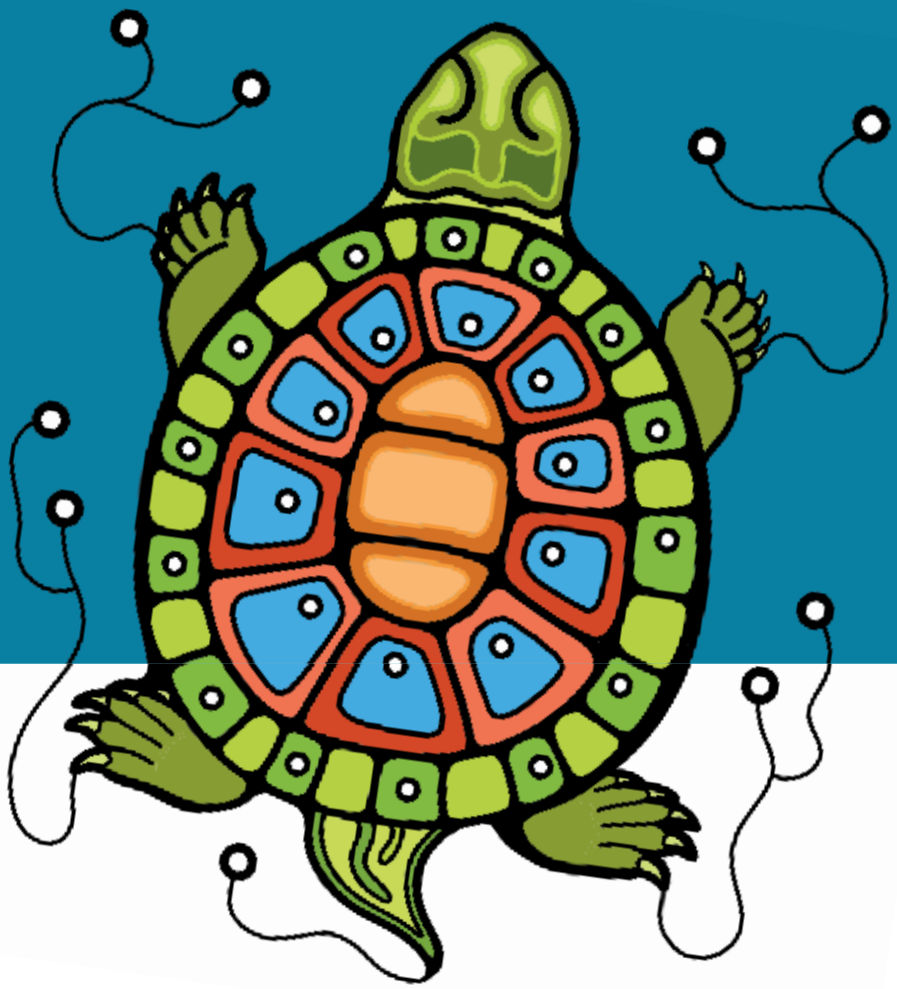
Note: A mix of consent and consultation may be used. For instance, a data-based initiative examining the health impacts on Indigenous persons who harvest or hunt near an industrial plant might seek the consent of First Nations near the plant and choose to hold a series of consultations open to all Indigenous persons who hunt in that area.

IPF 3.1 Consent ***or consultation*** is required for the collection ***or creation*** of ***Indigenous population information*** and the subsequent use or disclosure of this information. Typically, an organization will seek consent ***or undertake consultation*** for the use or disclosure of the information at the time of collection, or at or before the time of creation. In certain circumstances, consent with respect to use or disclosure may be sought (or consultation undertaken) after the information has been collected or created but before use (for example, when an organization wants to use information for a purpose not previously identified).

Table 3 Continued

CSA Model

3.2 The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.



Indigenous Privacy Framework

IPF 3.2.1 The consent of a subpopulation (possibly the entire Indigenous population) shall consist of one or more consents that collectively represent every member of the subpopulation. These consents shall be obtained either from:

- the member themselves (or their substitute decision maker if the circumstances allow or require, as the case may be); or
- a recognized representative which provides consent on behalf of a segment of the subpopulation which includes the member.

For example, in the case of data about diabetes in three nearby First Nation communities, the Band Councils of the First Nations could provide consent on behalf of their respective communities, thereby providing consent which represents all the members of the applicable Indigenous population.

IPF 3.2.2 Consent must be meaningful.
At a minimum, meaningful consent of a subpopulation (possibly the entire Indigenous population) requires the following.
Consent be obtained in culturally appropriate ways. For example, silence may have different meanings in different Indigenous cultures, so careful choices should be made around the use of opt-out consent.

The identified purposes must be explained, in culturally appropriate ways, to the individuals or parties from whom consent is sought. This requires that the purposes be stated in such a manner that the consenting individuals or parties can reasonably understand how the Indigenous population information will be used or disclosed.

IPF 3.2.3 If a subpopulation is consulted, any subsequent decision to proceed with the creation, collection, use, or disclosure of Indigenous population information of the subpopulation must respect any decision-making customs of the consulted subpopulation.

Table 3 Continued

CSA Model

3.3 An organization may not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special- interest magazines might be considered sensitive.

3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

Indigenous Privacy Framework

IPF 3.3 An organization may not, as a condition of the supply of a product or service, require **a party** to consent to the ***creation***, collection, use, or disclosure of **Indigenous population information** beyond that required to fulfil the explicitly specified, and legitimate purposes.

IPF 3.4 The form of the consent sought, or consultation undertaken, by the organization may vary, depending upon the circumstances and the type of Indigenous population information. In determining the form of consent to use or consultation to undertake, organizations shall take into account the sensitivity of the information. Although some Indigenous population information (for example, health-related Indigenous population information) is almost always considered to be sensitive, any Indigenous population information can be sensitive, depending on the context. For example, many traditional stories about a First Nation are intended to be shared. However, some stories might only customarily be shared by Elders.

IPF 3.5.1 In obtaining consent or proceeding with the use of Indigenous population information following consultation, the reasonable expectations of the members of the population are also relevant. For example, if a First Nations council collects data on the rates of vaccination in a member First Nation so that the success of a vaccination program can be communicated with other members in a monthly newsletter, then the First Nation might reasonably expect that the same data might be shared on a members-only wiki. However, the First Nation might not expect that the data to be shared on a webpage available to anyone.

IPF 3.5.2 Consent shall not be obtained through deception. Consultation must not involve deception.
Examples of deception include:

- saying that Indigenous population information will be encrypted when transmitted, but subsequently failing to do so; and
- emphasizing how a study will benefit an Indigenous population, but without relaying known information about significant expenditures required to achieve those benefits.

IPF 3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of Indigenous population information collected or created. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive.

4.2.4 Limiting Collection and Creation

The Indigenous-centric supplemental principle arising from the CSA Model Code "Limiting Collection" principle is presented in Table 4.

The supplemental principle reframes the original principle as "Limiting Collection and Creation". Again, in extending the original principle, the supplemental principle recognizes that most Indigenous population information must first be created (see Section 4.2.2), and that consultation might be needed as an alternative to consent when working with populations (see Section 4.2.3).

In translating the concept of "fair and lawful means" to Indigenous population information, the supplemental principle notes that "any consideration of lawfulness must include the applicable by-laws, resolutions, or similar. established by a relevant Indigenous body, such as a First Nation".

CSA Model

Limiting Collection (Principle 4): The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.1 Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Principle 8).

4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.3 This principle is linked closely to the Identifying Purposes principle (Principle 2) and the Consent principle (Principle 3).

Table 4:

Indigenous Privacy Framework supplemental principles arising from the CSA Model Code "Limiting Collection" principle.

Indigenous Privacy

Limiting Collection and Creation (Principle IPF4): The collection and creation of Indigenous population information, shall be limited to that which is necessary for the purposes identified by the organization. Indigenous population information shall be collected and created by fair and lawful means.

Note: In the context of Indigenous population information, any consideration of lawfulness must include the applicable by-laws, resolutions, or similar. established by a relevant Indigenous body, such as a First Nation.

IPF 4.1 Organizations shall not collect or create Indigenous population information indiscriminately. Both the amount and the type of information collected and created shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected and created as part of their information-handling policies and practices, in accordance with the Openness principle (Principle IPF8).

IPF 4.2 The requirement that Indigenous population information be collected and created by fair and lawful means is intended to prevent organizations from collecting or creating information by misleading or deceiving anyone about the purpose for which information is being collected or created. This requirement implies that consent not be obtained through deception and that consultation not involve deception, as contemplated in the Consent and Consultation principle (Principle IPF3).

IPF 4.3 This principle is linked closely to the Identifying Purposes principle (Principle IPF2)) and the Consent or Consultation principle (Principle IPF3).

4.2.5 Limiting Use, Disclosure, and Retention

The Indigenous-centric supplemental principle arising from the CSA Model Code “Limiting Use, Disclosure, and Retention” principle is presented in Table 5
.
For the most part, the Framework simply extends the original principle to Indigenous population information. However, in doing so, the supplemental principle does not allow for the disposition of Indigenous population information contrary to wishes of the population, except as required by law. This requirement attempts to uphold Indigenous sovereignty and data governance (particularly the OCAP® and OCAS principles of “ownership” and “control”).

Moreover, the supplemental principle does not offer “anonymization” as an option for disposition of Indigenous population information (unlike how the original principle does for Personal Information). Use of anonymization would likely result in a data product about a larger Indigenous population, which would be misleading about the larger population because it is based on a smaller population. With respect to privacy, anonymization is practice better suited to information about specific individuals, not populations.

Again, in extending the original principle, the supplemental principle recognizes that most Indigenous population information must first be created (see Section 4.2.2), and that consultation might be needed as an alternative to consent when working with populations (see Section 4.2.3).

Table 5:

Indigenous Privacy Framework supplemental principles arising from the CSA Model Code "Limiting Use, Disclosure, and Retention" principle.

CSA Model

Limiting Use, Disclosure, and Retention (Principle 5): Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

5.1 Organizations using personal information for a new purpose shall document this purpose (see Clause 2.1).

5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

5.4 This principle is closely linked to the Consent principle (Principle 3), the Identifying Purposes principle (Principle 2), and the Individual Access principle (Principle 9).

Indigenous Privacy Framework

Limiting Use, Disclosure, and Retention (Principle IPF5): Indigenous population information shall not be used or disclosed for purposes other than those for which it was collected or created, except with consent or consultation (see Principle IPF3), or as required by law. Indigenous population information shall be retained only as long as necessary for the fulfilment of those purposes; however, Indigenous population information shall not be disposed of without consent or consultation (see Principle IPF3), except as required by law.

IPF 5.1 Organizations using Indigenous population information for a new purpose shall document this purpose (see Clause IPF2.1).

IPF 5.2 Organizations should develop guidelines and implement procedures with respect to the Indigenous population information. These guidelines and procedures should include minimum and maximum retention periods, and address consent and consultation related to the disposition of Indigenous population information (see Principle IPF3). Indigenous population information that has been used to make a decision about the Indigenous population or a member of the Indigenous population shall be retained long enough to allow the member or a recognized representative of the Indigenous population access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

IPF 5.3 Indigenous population information that is no longer required to fulfil the identified purposes should be destroyed or erased, subject to the wishes of the Indigenous population as determined through consent or consultation (see Principle IPF3) or as required by law. Organizations shall develop guidelines and implement procedures to govern the destruction of Indigenous population information.

IPF 5.4 This principle is closely linked to the Consent or Consultation principle (Principle IPF3), the Identifying Purposes principle (Principle IPF2), and the Individual Access principle (Principle IPF9).

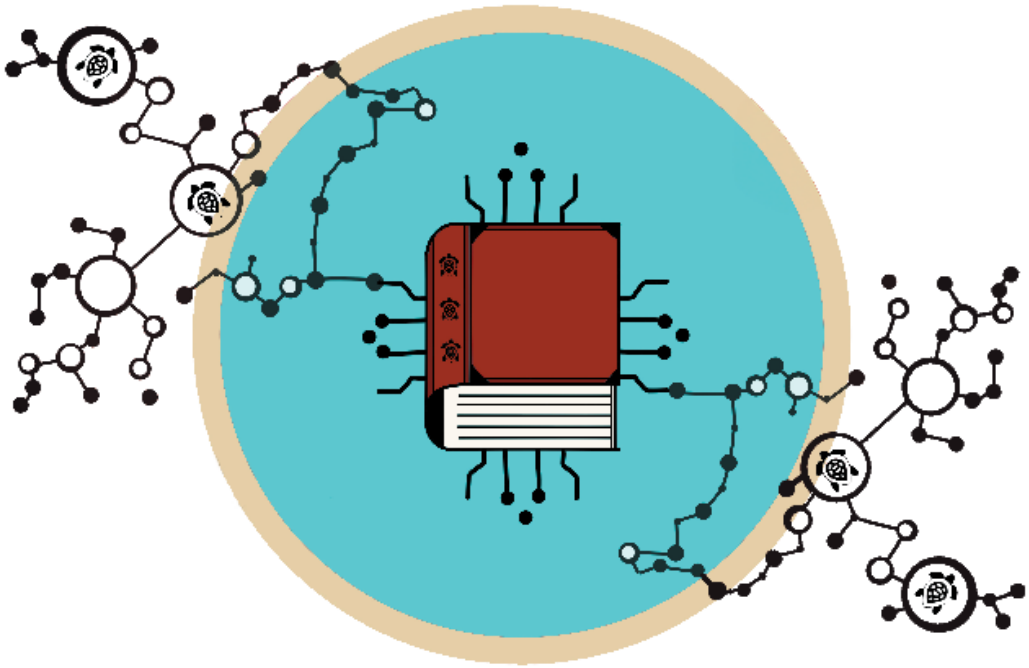
4.2.6 Accuracy

The Indigenous-centric supplemental principle arising from the CSA Model Code "Accuracy" principle is presented in Table 6. The Framework simply extends the original principle to Indigenous population information. Again, in extending the original principle, the supplemental principle recognizes that most Indigenous population information must first be created (see Section 4.2.2),

Table 6:

Indigenous Privacy Framework supplemental principles arising from the CSA Model Code "Accuracy" principle.

CSA Model
Accuracy (Principle 6): Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.
6.2 An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.
6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.



Indigenous Privacy Framework

Accuracy (Principle IPF6): Indigenous population information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

IPF 6.1 The extent to which Indigenous population information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the Indigenous population. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the Indigenous population or a member of it.

IPF 6.2 An organization shall not routinely update Indigenous population information, unless such a process is necessary to fulfil the purposes for which the information was collected or created.

IPF 6.3 Indigenous population information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.2.7 Safeguards

The Indigenous-centric supplemental principle arising from the CSA Model Code "Safeguards" principle is presented in Table 7.

The Framework simply extends the original principle to Indigenous population information, but with one notable difference: the Framework requires that more sensitive information be safeguarded with a higher level of protection, whereas this extra protection is optional in the CSA Model Code .

CSA Model

Safeguards (Principle 7): Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 3.4.

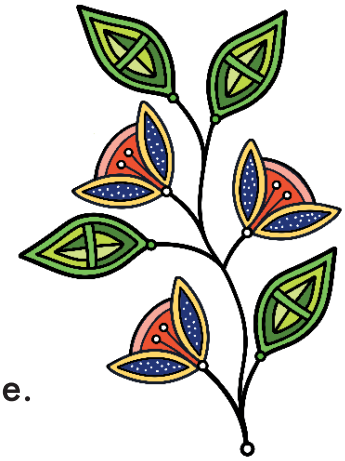
7.3 The methods of protection should include
physical measures, for example, locked filing cabinets and restricted access to offices;
organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and technological measures, for example, the use of passwords and encryption.

7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 5.3).

Table 7:

Indigenous Privacy Framework supplemental principles arising from the CSA Model Code "Safeguards" principle.



Indigenous Privacy Framework

Safeguards (Principle IPF7): Indigenous population information shall be protected by security safeguards appropriate to the sensitivity of the information.

IPF 7.1 The security safeguards shall protect Indigenous population information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect Indigenous population information regardless of the format in which it is held

IPF 7.2 The nature of the safeguards will vary depending on the sensitivity of the Indigenous population information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information must be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause IPF3.4.

IPF 7.3 The methods of protection should include

- physical measures, for example, locked filing cabinets and restricted access to offices;
- organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- technological measures, for example, the use of passwords and encryption.

IPF 7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of Indigenous population information.

IPF 7.5 Care shall be used in the disposal or destruction of Indigenous population information, to prevent unauthorized parties from gaining access to the information (see Clause IPF5.3).

4.2.8 Openness

The Indigenous-centric supplemental principle arising from the CSA Model Code "Openness" principle is presented in Table 8. The IPF simply extends the original principle to Indigenous population information.

The original principle has been extended to Indigenous population information. As discussed, with respect to the "Identifying Purpose" principle (IPF2 – see Section 4.2.2), the Framework requires that organizations are able to explain, to anyone, the purposes for which Indigenous population information is being collected or created.

CSA Model

Openness (Principle 8): An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

8.1 Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

8.2 The information made available shall include

a. the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
b. the means of gaining access to personal information held by the organization;
c. a description of the type of personal information held by the organization, including a general account of its use;
d. a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
e. what personal information is made available to related organizations (e.g., subsidiaries).

8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

Table 8:

Indigenous Privacy Framework supplemental principles arising from the CSA Model Code "Openness" principle.

Indigenous Privacy Framework

Openness (Principle IPF8): An organization shall make readily available to individuals specific information about its policies and practices relating to the management of Indigenous population information.

IPF 8.1 Organizations shall be open about their policies and practices with respect to the management of Indigenous population information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is culturally appropriate and generally understandable.

For example, if an organization manages Inuit population information, it might be considered culturally appropriate to provide a summary of its information practices in Inuktitut.

IPF 8.2 The information made available shall include

a. the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
b. the means of gaining access to Indigenous population information held by the organization;
c. a description of the type of Indigenous population information held by the organization, including a general account of its use;
d. a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
e. what Indigenous population information is made available to related organizations (e.g. subsidiaries)

IPF 8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.2.9 Indigenous Access

The Indigenous-centric supplemental principle arising from the CSA Model Code "Individual Access" principle is presented in Table 9. The supplemental principle reframes the original principle as "Indigenous Access".

The original principle has been extended to Indigenous population information by providing access and correction rights to the associated Indigenous population through its members and recognized representatives.

CSA Model

Individual Access (Principle 9): Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor client or litigation privilege.

9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

9.2 An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

Table 9:

Indigenous Privacy Framework supplemental principles arising from the CSA Model Code "Indigenous Access" principle.

Indigenous Privacy Framework

Indigenous Access (Principle IPF9): Upon request, members and recognized representatives of an Indigenous population shall be informed of the existence, use, and disclosure of their Indigenous population information and shall be given access to that information. The members and recognized representatives shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the Indigenous population information it holds about an Indigenous population. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the Indigenous population upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other Indigenous populations, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor client or litigation privilege.

IPF 9.1 Upon request, an organization shall inform members and recognized representatives of an Indigenous population whether or not the organization holds information about their Indigenous population. Organizations are encouraged to indicate the source of this information. The organization shall allow the members and recognized representatives access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

IPF 9.2 A member or recognized representative of an Indigenous population may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of information about their Indigenous population. The information provided shall only be used for this purpose.

Table 9 Continued

CSA Model

9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

9.4 An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

Indigenous Privacy Framework

IPF 9.3 In providing an account of third parties to which it has disclosed Indigenous population information, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed Indigenous population information, the organization shall provide a list of organizations to which it may have disclosed Indigenous population information.

IPF 9.4 An organization shall respond to a member's or recognized representative's request within a reasonable time and at minimal or no cost. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

IPF 9.5 When a member or recognized representative successfully demonstrates the inaccuracy or incompleteness of information about their Indigenous population, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

IPF 9.6 When a challenge is not resolved to the satisfaction of the member or recognized representative, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.2.10 Challenging Compliance

The Indigenous-centric supplemental principle arising from the CSA Model Code "Challenging Compliance" principle is presented in Table 10.

The original principle has been extended to Indigenous population information by providing compliance challenge rights to the associated Indigenous population through its members and recognized representatives.

Table 10:

Indigenous Privacy Framework supplemental principles arising from the CSA Model Code "Challenging Compliance" principle.

CSA Model
Challenging Compliance (Principle 10)ww: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.
10.1 The individual accountable for an organization's compliance is discussed in Clause 1.1.
10.2 Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.
10.3 Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.
10.4 An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

Indigenous Privacy Framework

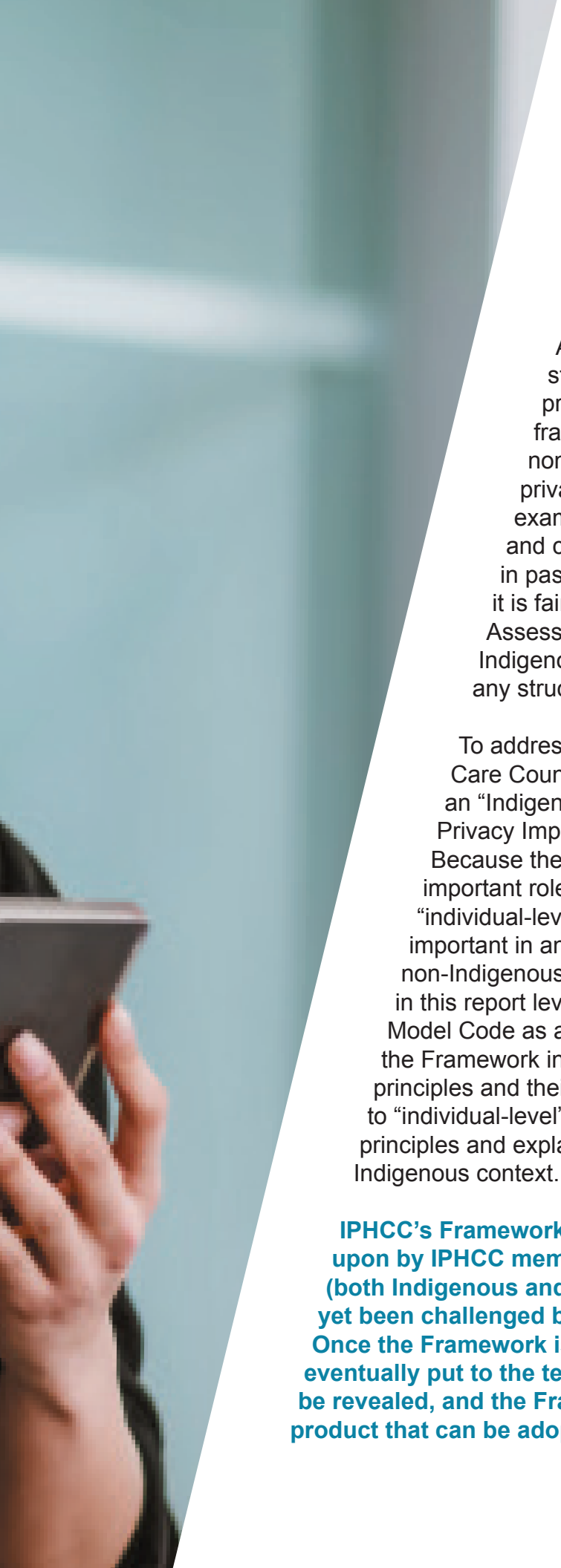
Challenging Compliance (Principle IPF10): Members and recognized representatives of an Indigenous population shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

IPF 10.1 The individual accountable for an organization's compliance is discussed in Clause IPF1.

IPF 10.2 Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of Indigenous population information. The complaint procedures should be easily accessible and simple to use.

IPF 10.3 Organizations shall inform members and recognized representatives who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist.

IPF 10.4 An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.



CONCLUSION

Existing privacy frameworks, such as the **Canadian Standards Association Model Code for the Protection of Personal Information** (the "CSA Model Code") and the **Generally Accepted Privacy Principles** (GAPP) of the American Institute for Chartered Public Accountants and CPA Canada, offer a structured, repeatable way of assessing privacy impact. However, these existing frameworks are based exclusively on non-Indigenous, individualistic notions of privacy. Although there may be isolated examples in which Indigenous perspectives and considerations have been reflected in past privacy impact assessment work, it is fair to say that most Privacy Impact Assessments to date have not approached Indigenous perspectives and considerations in any structured, repeatable way.

To address this gap, Indigenous Primary Health Care Council (IPHCC) has set about to establish an "Indigenous Privacy Framework" against which Privacy Impact Assessments can be conducted. Because the CSA Model Code plays such an important role in Canadian privacy, and because "individual-level" privacy considerations remain as important in an Indigenous context as they do in a non-Indigenous context, the Framework presented in this report leverages the principles of the CSA Model Code as a starting point. More specifically, the Framework incorporates the CSA Model Code principles and their explanatory clauses (as they pertain to "individual-level" privacy), establishing supplemental principles and explanatory clauses that also apply in an Indigenous context.

IPHCC's Framework has not yet been commented upon by IPHCC members or the privacy community (both Indigenous and non-Indigenous), and it has not yet been challenged by way of a "real-life" assessment. Once the Framework is circulated for further input, and eventually put to the test, strengths and weaknesses will be revealed, and the Framework can be refined into a product that can be adopted and promoted.