Notice and Consent Conformance Profile Draft Recommendation Version 1.0

This Draft Recommendation has been developed by the Digital ID & Authentication Council of Canada (DIACC) Trust Framework Expert Committee (TFEC). The TFEC operates under the controlling policies of the DIACC. Comments submitted by the public are subject to the DIACC Contributor Agreement.

DIACC expects to modify and improve this Draft Recommendation based upon public comments. The purpose of the open commentary is to ensure transparency in development and diversity of truly Pan-Canadian input. Comments made during the review will be considered for incorporation to the next draft. DIACC will prepare a disposition of comments to provide transparency with regard to how each comment was handled.

Forthcoming PCTF releases will expand, clarify, and refine the content of this document. The intended target audience is inclusive of decision makers who may or may not be domain technology experts.

When reviewing this Draft Recommendation, please consider the following:

1. Do the list of trusted processes for Notice and Consent map to processes in your organization or business?
2. Is the description of the trusted processes clear and accurate?
3. Are the conformance criteria clear and measurable?
   Are there any conformance criteria you would recommend adding?
4. Do the terms used to describe Notice and Consent in the document make sense in the context(s) you are familiar with?

Table of Contents

1 Introduction to Notice and Consent Conformance Criteria

This document specifies the set of conformance criteria for the Notice and Consent Component, a component of the Pan-Canadian Trust Framework (PCTF). The Notice and Consent conformance criteria specify requirements for Notice and Consent participants to issue legally compliant and understandable notice statements, collect informed and authorized consent decisions, and enable the on-going management of those consent decisions.

Conformance criteria are central to the trust framework because they specify the essential requirements agreed to by trust framework participants to ensure the integrity of their processes. This integrity is paramount because the output or result of a trusted process is relied on by many participants – over time and across organizational, jurisdictional and sectoral boundaries.

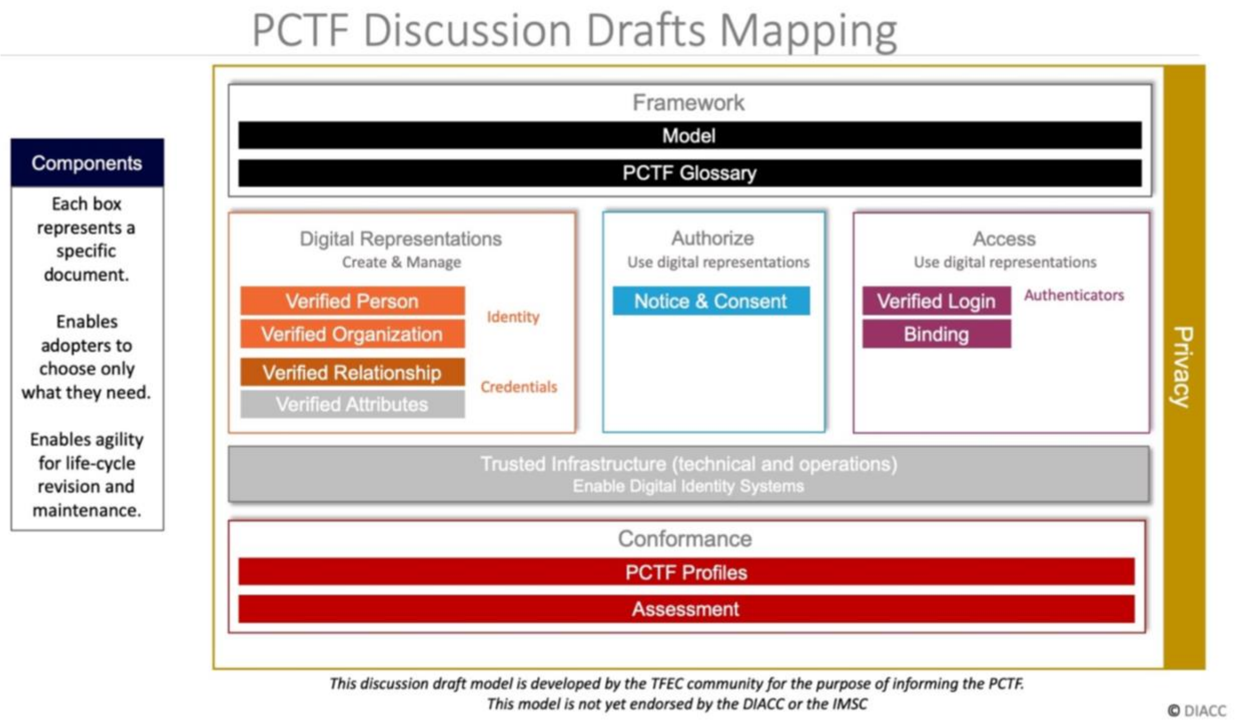
The PCTF conformance criteria are intended to complement existing privacy legislation and regulations; participants in the digital identity ecosystem are expected meet the applicable legislated requirements and regulations in their jurisdictions.

1.1 Relationship to the Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework (PCTF) consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components. Adopting a Pan-Canadian approach, the PCTF enables the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and practices across the Canadian digital ecosystem.

Figure 1 is a logical overview of the Pan-Canadian Trust Framework. The Notice and Consent Component describes the "Authorize" block, which is part of the "use digital representations" functions. Note that the privacy requirements for the handling of personal information by the Notice and Consent processes (and all other PCTF components) within the digital identity ecosystem are defined in the PCTF Privacy Component.

PCTF Discussion Drafts Mapping


Components
Each box represents a specific document.
Enables adopters to choose only what they need.
Enables agility for life-cycle revision and maintenance.
Framework
Model
PCTF Glossary
Digital Representations
Create & Manage
Verified Person
Verified Organization
Identity
Verified Relationship
Verified Attributes
Credentials
Authorize
Use digital representations
Notice & Consent
Access
Use digital representations
Verified Login
Binding
Authenticators
Privacy
Trusted Infrastructure (technical and operations)
Enable Digital Identity Systems
Conformance
PCTF Profiles
Assessment

This discussion draft model is developed by the TFEC community for the purpose of informing the PCTF.
This model is not yet endorsed by the DIACC or the IMSC

© DIACC

Figure 1. Pan-Canadian Trust Framework Model Visual Draft

1.2 Keywords

To ensure consistent application, keywords that appear in **bold typeface** in the conformance criteria are to be interpreted as follows:

- **MUST** means that the requirement is absolute as part of the conformance criteria.
- **MUST NOT** means that the requirement is an absolute prohibition of the conformance criteria.
- **SHOULD** means that while there may exist valid reasons in particular circumstances to ignore the requirement, the full implications must be understood and carefully weighed before not choosing to adhere to the conformance criteria or choosing a different option as specified by the conformance criteria.
- **SHOULD NOT** means that valid reason may exist in particular circumstances when the requirement is acceptable or even useful, however, the full implications should be understood and the case carefully weighed before choosing to not conform to the requirement as described.
- **MAY** means that the requirement is discretionary but recommended.

Additional keywords, such as normative definitions in related standards and specifications, will also be indicated in **bold**.

1.3 Data Protection Laws and Conformance Criteria

Digital identity is, by definition, concerned with providing entities with the digital means to collect, manage and share verified personal information. Digital identity systems must, therefore, comply with data protection legislation, which includes requirements for notice and consent. The Notice and Consent Conformance Profile does not repeat legislative requirements but shows how these requirements apply within the context of the PCTF.

Multiple data protection laws cover the operations of organizations when handling personal information. At a federal level, the Privacy Act and Personal Information Protection and Electronic Documents Act (PIPEDA) apply to federal government and commercial organizations respectively. Each province and territory has its own laws that apply to the handling of personal information by provincial and territorial public bodies. As well, several provincial statutes have been deemed "substantially similar" to PIPEDA and apply to how private sector organizations handle personal information in those provinces.

Given these considerations, PIPEDA Fair Information Principle 3 (Consent), along with guidance from the Office of the Privacy Commissioner of Canada, provide a framework that can be applied to a range of organizations and use cases and is used as the basis for the PCTF Notice and Consent Component. If conflicts arise between the Notice and Consent Component and any data protection law applicable to an organization, then the applicable law takes precedence.

1.4 Roles

The following roles are defined to cover the scope of the Notice and Consent conformance criteria. Depending on the use case, different organizations may take on one or more roles.

- **Subject –** The natural person to whom the personal data in question pertains. Note: Delegated Authority is not addressed in this version of the conformance criteria.

- **Disclosing Organization –** The organization that currently holds the personal data that the Subject consents to disclose to a Requesting Organization. In a digital identity context, this will often be an identity or attribute provider. Personal information verified by a Disclosing Organization and represented on a Subject’s device is considered to be part of the Disclosing Organization.

- **Requesting Organization –** The organization to which the Subject consents to disclose personal information. In a digital identity context, this will often be a service provider or relying party.

- **Notice and Consent Processor –** The organization that provides the notice to the Subject of the request for personal information (from the Requesting Organization), obtains and records the consent and provides the Subject with the means to manage the consent going forward, including the withdrawal of consent.

These roles help to isolate the different functions and responsibilities that participants may perform in end-to-end notice and consent processes. They do not imply any particular solution, architecture or implementation. For example, in some cases, the notice may be presented and consent collected from a network operator (acting as Notice and Consent Processor) facilitating personal information exchange between a patient (the Subject), a medical lab (Disclosing Organization) and a hospital (Requesting Organization). In other cases, the notice may be presented and consent collected directly by either the Disclosing or Requesting Organization, in which case that organization would also be the Notice and Consent Processor.

2 Trusted Processes and Conformance Criteria

2.1 Trusted Processes

The Notice and Consent Conformance Profile defines conformance criteria as essential requirements for the trusted processes defined in the Notice and Consent Component Overview, which are:

1. **Formulate Notice –** the process of determining what personal information is to be collected, used or disclosed, by whom and to whom, and for what purposes (i.e., the notice conditions). This process formulates the notice statement that will be shown to the Subject

2. **Request Consen**t **–** the process of determining that the Subject who is being asked to provide consent has the authority to do so, displaying the notice statement to the Subject, and then obtaining the consent decision (i.e., accept or decline) from the Subject

3. **Record Consent –** the process of storing the notice conditions and corresponding consent decision from the Subject, and notifying relevant parties of the consent decision

4. **Manage Consent –** the process to support the authorized on-going management of consent decisions including reviewing consent decisions, renewing consent decisions, expiring consent decisions, and revoking consent decisions

2.2 Levels of Assurance

Levels of assurance are used in certain contexts, such as those described in the PCTF Verified Login Component or the PCTF Verified Person Component, to indicate the robustness of the technology and processes employed to verify the login or the identity of an individual. Notice and consent requirements apply across all levels of assurance; there is no equivalent to “unverified” or “low assurance” for notice and consent trusted processes.

Consent should be obtained in broadly the same manner at low levels of assurance as it is at higher levels of assurance. As such, the Notice and Consent Component conformance criteria reflect the following:

- Disclosure of sensitive data (e.g., health-related attributes) should only be done with an appropriate level of assurance for the associated Verified Person and Verified Login (see CONS 3) and in accordance with relevant legislation.

- Consent can be recorded in different ways with different levels of robustness. For example, a flag in a database could indicate the user checked a box. For the consent given, a digital signature may provide a greater level of non-repudiation than clicking a checkbox. This version of the Notice and Consent Conformance Profile does not differentiate between such approaches but does require a minimum level of robustness of the consent process to satisfy regulatory requirements (see RECO 1).

2.3 Notice and Consent Conformance Criteria

Conformance criteria are organized by the Trust Processes defined in the Notice and Consent Component. For ease of reference, a specific conformance criterion may be referred by its category and reference no. (e.g., "**NOTI 1**" refers to "Formulate Notice Conformance Criteria Reference No. 1").

Reference	**Conformance Criteria**
BASE	**Baseline**
	The organizations performing the roles defined herein must comply with all the baseline Privacy Conformance Criteria stipulated in the Privacy Conformance Profile.
NOTI	**Formulate Notice**
1	The Notice and Consent Processor **MUST** have processes in place to ensure that appropriate notice statements concerning the collection, use or disclosure of personal information are formulated (as per **NOTI 5**) and provided to Subjects, at or before the time personal information is collected.
2	The Notice and Consent Processor **MUST** have appropriate processes, resources and oversight in place to ensure that notice statements conform to the Formulate Notice trusted process, include all required information, and are updated in a time frame that does not compromise a Subject’s ability to provide informed and valid consent when the requirements or purpose for collecting, using or disclosing personal information change.

3	The Notice and Consent Processor **MUST** determine what information is required to be included in its notice statements based on all applicable legal, policy and contractual requirements. In a digital identity system, collected information could include: • the personal information about the Subject being requested by the Requesting Organization; • the purpose for which the personal information is being requested; • the details of the Requesting Organization(s); • contact information (e.g., the title, business address and business telephone number) of an authorized person who can answer the Subject’s questions about the collection; • the legal authority for collecting the personal information; • the period of time for which the personal information requested will be stored or used; • whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure (in the background) for the same purpose (e.g., to allow the Subject to “broadcast” updates to their personal information, such as change of address, in an efficient but controlled manner); • how to withdraw consent (for on-going disclosure); and • details of the potential sources of the requested personal information, be they Disclosing Organizations or the Subject concerned The Notice and Consent Processor **MUST** ensure that the information to be included in a notice statement is precisely defined. In a digital identity context, this could include, for example, the specific personal information to be shared and the necessary metadata.
4	The Notice and Consent Processor **MUST** ensure that a new notice statement is provided to a Subject when the organization decides to use or disclose personal information that it has already collected from the Subject for a new purpose (that is not consistent with the purpose(s) provided in the original notice statement). The new notice statement **MUST**: • identify the new purpose(s) and the specific personal information that will be used or disclosed for the new purpose(s); • include other applicable information that may be required (such as the type of information set out in by **NOTI 3**); and • request the Subject’s consent to use or disclose the personal information for the new purpose(s).

5	The notice statement **SHOULD** be presented in writing and **MUST** be provided in a manner that enables Subjects to reasonably understand how their personal information will be used or disclosed. This includes providing notice in a manner that is: • intelligible (using clear and plain language); • concise; • easily visible; • transparent; and • accessible. Where it is not practical for the notice statement to include additional details pertaining to the request (e.g., full terms and conditions, detailed metadata), a convenient means **SHOULD** be provided to allow the Subject to review those details, ideally as part of the digital workflow being delivered. This **MUST** not be used as a means to make the notice statement less visible, transparent or accessible. The establishment of a digital identity may involve the use of non-digital channels to collect personal information. In these cases, processes **MUST** be employed to ensure that the notice, however delivered, satisfies the above points.
6	In some scenarios, a single notice statement may include requests for consent from multiple organizations, for example, when disclosing attributes from multiple sources. Where the notice statement includes requests from multiple organizations, the notice **MUST** be constructed such that it can be split into the parts pertaining to each organization, for the purposes of recording and storing the consent (see RECO 2 below).
CONS	**Request Consent**
1	The process of requesting the consent of a Subject **MUST** include the presentation of the notice statement and verification of the Subject, as follows: • the notice **MUST** precede the action of the Subject providing consent; • if the notice does not disclose personal information in the notice statement then verification of the Subject is not required prior to display; • if the notice discloses personal information in the notice statement then the identity of the Subject **MUST** be verified prior to display; and • regardless of when the notice occurs, prior to a consent being relied upon, the Subject **MUST** have been successfully verified.

2	One or more of the Notice and Consent Processor, Disclosing Organization or the Requesting Organization **MUST** verify that the individual providing consent is the Subject in question and therefore authorized to perform the consent action. A number of scenarios may arise including: • The Requesting Organization is requesting previously collected personal information from a Disclosing Organization: In this case, the Notice and Consent Processor and Disclosing Organization **MUST** take steps to verify (or authenticate) that the individual performing the action is the Subject in question. • The Requesting Organization is collecting new personal information from the Subject that is to be associated with the Subject: In this case, the Requesting Organization and Notice and Consent Processor **MUST** take steps to verify (or authenticate) that the individual performing the action is the Subject in question. The Requesting Organization is collecting new personal information from a new Subject: In this case, the process **MUST** be performed in conjunction with the Verified Person and Verified Login processes to ensure that the Subject is verified and subsequent access to the Subject’s personal data is under their control. Subjects **SHOULD** be able to verify themselves in a quick and secure manner.
3	The level of assurance for verification or authentication **MUST** be sufficient for the sensitivity of personal data to be disclosed. The Disclosing Organization typically determines the sensitivity of the data to be shared based on the context (e.g., type of information, intended use).
4	The action required to be taken by the Subject to provide consent **MUST** be clear, explicit and straightforward. If the Subject is offered a choice within the requested consent (e.g., to share a subset of the requested personal information), the action required to make the choice **MUST** be clear, explicit and straightforward.
5	The Notice and Consent Processor **MUST** ensure that consent is affirmative, specific, informed, and unambiguous.
6	If the Subject’s consent is requested as part of a written statement that also concerns other matters, the request for consent **MUST** be presented in a manner that: • is clearly distinguishable from the other matters; • is in an intelligible and easily accessible form; and • uses clear and plain language.

7	The Disclosing Organization **MUST** have processes in place that enable it to easily demonstrate that a Subject has consented to the collection, use or disclosure of their personal information, or that it has legislated authority for the collection, use or disclosure of the personal information. In the case, where the Notice and Consent Processor is a separate organization to the Disclosing Organization, then the Disclosing Organization **MUST** ensure that suitable processes are in place at the Notice and Consent Processor.
8	Before requesting consent from a Subject, the Requesting Organization **MUST** determine whether the Subject can withdraw their consent at a later date or whether legal or contractual restrictions prevent or limit the withdrawal of consent. If there is no clear and easily understood way to withdraw the consent, this **MUST** be disclosed in notice statement when the information is being requested.
9	Where a Subject has the right to withdraw their consent at a later date, the Requesting Organization (or the Notice and Consent Processor acting on their behalf) **MUST**: • inform the Subject of this right (subject to reasonable notice and applicable conditions or restrictions) at the time consent is requested; • inform the Subject of how to exercise this right; and • ensure that the process for withdrawing consent is as easy for the Subject as providing consent.
RECO	**Record Consent**
1	Once the Subject has provided consent, the Notice and Consent Processor **MUST** capture the following evidence: • sufficient information to identify who has given consent. Where possible this **MUST** be linked to a Verified Person; • the date, time or other contextual information around when and how the consent was made; • the version of the notice statement provided and the personal information requested (i.e., the type of information, not the content or actual information itself); • the consent decision which **MUST** be one of accept or decline, for each consent choice presented; and • if applicable, the expiration date/time of consent.

201	2	The Notice and Consent Processor **MUST** provide the evidence (described in **RECO 1**) to the relevant Requesting and Disclosing Organizations. The Notice and Consent Processor **SHOULD** inform the Subject of the identity of the Requesting and Disclosing Organizations receiving the evidence. Where the notice statement includes requests for consent from multiple organizations, the notice statement **MUST** be split up so that each organization only receives the evidence relevant to them. Evidence relating to one organization **MUST NOT** be provided to another organization.
202	3	Disclosing and Requesting Organizations **MUST** store the evidence uniquely (i.e., only store the evidence once for each consent given) and immutably, such that any update or state change will result in a new record and past records can be recovered. Storage of evidence **MUST** also comply with applicable legislation (e.g., in certain cases, data must be stored in Canada).
203	4	Updates to conditions/statements presented to a Subject **MUST** be versioned uniquely, so that changes over time can be recovered and accessible at all times to the Subject.
204	5	Per Canadian laws related to required languages (e.g., English, French), each language variation of the notice statement **MUST** be stored.
205	6	A notice and consent record **MAY** become invalid in the event that a data breach or unauthorized access is discovered, or if it is discovered that the consent was given without the authority or capacity to give it. If any of these situations arise, the organizations affected **MUST** review the circumstances and take appropriate action (e.g., revoke the affected consent) .If there is a data breach that includes the Subject's personal information, they **MUST** notify the affected Subject. The actions taken **MUST** comply with applicable legislation.
206	7	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** employ processes and procedures to prevent the loss of notice and consent records and to limit the impact of any data security violations, and in accordance with relevant law (e.g., a public body's requirements under section 30 of FOIPPA).
207	8	Privacy-preserving practices **MUST** be followed when storing records of consent. In this context, privacy-preserving practices refer to methods, approaches, or procedures designed to maintain the privacy of consent records.
208	**MANA**	**Manage consent**
209	1	If a Requesting Organization wishes to obtain a revised consent from a Subject, then the requirements set out above relating to notice, consent and record (**NOTI 1-6**, **CONS 1-9**, **RECO 1-8**) apply to the new consent. This **WILL** result in an updated consent decision, which **MUST** be stored as per **RECO 3**.

2	A consent **MUST** expire when the expiration date captured in the consent process (**RECO 1**) is passed. After that date, the Requesting Organization **MUST** (unless applicable law requires or authorizes its on-going use and storage) cease to use the personal data concerned for the specified purpose and, if required, delete it in a way that protects the privacy of the Subject.
3	Revocation of the consent decision **MUST** occur when either: • the Subject withdraws the consent; • an interval of time (determined by legislative, business, or other applicable considerations) has passed where there could be a significant change in circumstances under which consent was originally obtained; or • the Disclosing Organization, Requesting Organization or Notice and Consent Processor determines that the consent was not legitimate, for example, if a fraudulent activity, data breach, or unauthorised access is confirmed.
4	Where a Subject notifies the Notice and Consent Processor that they wish to withdraw the consent given and there are no legal or contractual restrictions preventing the Subject from withdrawing consent, the Notice and Consent Processor: • **MUST** inform the Subject of the implications of such withdrawal; but • **MUST NOT** prohibit the Subject from withdrawing consent; and • the action required to withdraw the consent **MUST** be clear, explicit and straightforward.
5	Where it is determined that the consent was not legitimate or lawful, the Notice and Consent Processor **MUST** revoke the consent as per **MANA 3**. The Notice and Consent Processor **MUST** also inform the Subject (if appropriate), Disclosing Organization and Requesting Organization. In the case of identity theft where the Subject itself is compromised it may not be appropriate to inform the Subject of the consent withdrawal. In the interest of protecting identity information from abuse and privacy breaches, withdrawing consent in such circumstances **MUST** be done with great care. The Notice and Consent Processor **MUST** ensure that it has processes in place to prevent the erroneous or malicious withdrawal of consent.
6	When consent is withdrawn (for any reason), the Notice and Consent Processor **MUST** notify the Requesting Organization. The Requesting Organization **MUST** then stop collecting, using or disclosing the personal information specified in the consent unless the collection, use or disclosure is permitted without consent. When consent is withdrawn (for any reason), the Notice and Consent Processor SHOULD inform third-party providers (this may not be possible in all cases if the identity of the third-parties is not known to the Notice and Consent Processor).

7	The Notice and Consent Processor **SHOULD** provide Subjects with the ability to manage all consent decisions made. These features **SHOULD** be easy to use, providing an efficient and optimal means for Subjects to manage consent decisions. This should include: • the ability to review, update or revoke the consent decisions for a particular organization; • search facilities so that consent decisions can be easily found; • notifications of expired consent decisions, which could indicate loss of service from a Requesting Organization; • descriptions of the consequences of the Subject revoking their consent (e.g., impact on applications or payments in process); and • when necessary, the ability to review, update or revoke individual consent decisions at a granular level.
8	The Notice and Consent Processor **SHOULD** provide the Subject and authorized reviewers with the ability to review consent decisions made. These features **SHOULD** be easy to use, providing an efficient and optimal means for the Subject and authorized reviewers to manage consent decisions. Authorized reviewers are participants impacted by the consent (i.e., Disclosing Organization, Requesting Organization) as well as regulatory bodies or oversight committees for audit. This could include, for example: • the ability to review the consent decisions for a particular organization; and • search facilities so that consent decisions can be easily found.

Table 1. Notice and Consent Conformance Criteria