PCTF Notice & Consent Conformance Profile

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, a Final Recommendation is a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document was developed by DIACC's Trust Framework Expert Committee with input from the public gathered and processed through an open peer review process. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme. Changes to this document that may affect certification and Trustmark status will be defined in the Pan-Canadian Trust Framework Assessment component.

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 PCTF 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.

Note

- PCTF conformance criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.

1.1 Keywords and Definitions

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

- **MUST:** The requirement is absolute as part of the conformance criteria.
- **MUST NOT:** The requirement is an absolute prohibition of the conformance criteria.
- **SHOULD:** While there may exist valid reasons in particular circumstances to ignore the requirement, the full implications must be understood and carefully weighed before choosing to not adhere to the conformance criteria or choosing a different option as specified by the conformance criteria.
- **SHOULD NOT:** A valid reason for an exception 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:** The requirement is discretionary but recommended.

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

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 generating a statement that describes, for the Subject, the information that will be collected.
2. **Request Consen**t – the process of presenting Notice to a Subject and, if applicable, providing the capability for the Subject to accept (i.e., give) or decline (i.e., deny) consent based on the contents of the notice statement, resulting in a meaningful consent decision.
3. **Record Consent** – the process of making a record of the notice conditions and the Subject's consent decision.
4. **Manage Consent** – the process of managing the lifecycle of consent decisions.

2.2 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").

Whether or not it is explicitly stated in any of the criteria below it should be noted that none of the PCTF conformance criteria replace or supersede existing regulations. Organizations and individuals are expected to comply with relevant legislation, policy, and regulations in their jurisdiction.

Reference	Conformance Criteria
BASE	**Baseline**
	The organizations performing the roles defined herein **MUST** comply with all the relevant baseline criteria set forth in other components of the PCTF such as the Privacy Conformance Criteria stipulated in the Privacy Conformance Profile, Authentication Conformance Criteria stipulated in the Authentication Conformance Profile, and Verified Person Conformance Criteria stipulated in the Verified Person Conformance Profile. PCTF conformance criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.
NOTI	**Formulate Notice**
1	The Notice and Consent Processor **MUST** have processes in place to ensure that appropriate notice statements concerning the collection, use, disclosure, or retention of personal information are formulated (as per **NOTI 5**) and provided to Subjects, at or before the time personal information is collected. In cases where legislation or regulation does not require consent, notice **SHOULD** still be provided unless legislation, regulation, or policy prohibit it, or circumstances justify (e.g., collection or disclosure of data for an ongoing criminal investigation).

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 conformance criteria.
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, regulatory, and contractual requirements. In a digital identity system, information in the notice statement 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 identity and 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 or justification that clarifies the legal rationale for its collection; • 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 • the identity and details of the potential sources of the requested personal information, be they Disclosing Organizations or the Subject concerned • notification that data will be stored outside of a relevant jurisdiction in cases where that will be done, as required by data residency related legislation, regulation, or policy, notification • notification that Authorized Reviewers may review the consent decision for the purpose of an audit of adherence to the Notice and Consent Conformance Profile or other laws, regulations, or policies that are applicable in the relevant jurisdiction The Notice and Consent Processor **SHOULD** inform the Subject of the identity of the Requesting and Disclosing Organizations receiving the evidence. The Notice and Consent Processor **MUST** ensure that the information to be included in a notice statement is unambiguous. In a digital identity context, this could include, for example, the specific personal information to be shared and the necessary metadata. In cases where legislation or regulation does not require consent, notice **SHOULD** still be provided unless legislation or regulation prohibit it, or circumstances justify (e.g., collection or disclosure of data for an ongoing criminal investigation).

4	The Notice and Consent Processor **MUST** ensure that a new notice statement is provided to a Subject when the organization intends to use or disclosure 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**: • be presented to the Subject in a timeframe that does not compromise a Subject's ability to provide informed and valid consent; • 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**); • where applicable, identify the legal authority for collecting the personal information or justification that clarifies the legal rationale for its collection; and • unless prohibited by legislation or regulation, request the Subject's consent to use or disclose the personal information for the new purpose(s). In cases where legislation or regulation does not require consent, notice **SHOULD** still be provided unless legislation or regulation prohibit it, or circumstances justify (e.g., collection or disclosure of data for an ongoing criminal investigation).

5	The notice statement **SHOULD** be presented in writing and **MUST** be provided in language that enables Subjects to reasonably understand how their personal information will be used or disclosed. This includes providing notice in a manner that is: • in 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. In cases where a someone is acting on behalf of a Subject who is unable to obtain notice digitally (e.g., disabled persons, digitally disadvantaged persons), persons acting on behalf of the subject **MUST** ensure they are communicating notice to the subject in compliance with the Notice and Consent Conformance Profile, and that they are in compliance with legislation, regulation, and policy governing this type of assistive relationship in their jurisdiction. In jurisdictions where regulation, legislation, or policy states a mandatory requirement to provide physical notice for certain types of notice (e.g., for video surveillance), such notification **SHOULD** also conform to the criteria described in this document unless otherwise prohibited by the legislation, regulation, or policy.
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).

7	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. The Requesting Organization **MAY** also determine whether they will offer the option of automatic revocation of consent following the passage of an interval of time or on a specific date, which might, for example, be determined by legislative, business, or other applicable considerations. If there is no clear and easily understood way to withdraw the consent, this **MUST** be disclosed in notice statement.
CONS	**Request Consent**
1	The process of requesting the consent of a Subject **MUST** include the presentation of Notice and verification of the Subject, as follows: • the notice **MUST** precede the action of the Subject providing consent; • if the Notice itself does not disclose personal information then verification of the Subject is not required prior to its display; • if the Notice discloses personal information then the identity of the Subject **MUST** have been verified prior to its display; and • regardless of when the notice occurs, for consent to be considered valid, the Subject **MUST** have been successfully verified to an appropriate level of identity assurance.
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. 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 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 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 conformance with the Verified Person and Verified Login conformance criteria to ensure that the Subject is verified and subsequent access to the Subject's personal data is under their control.

3	The level of assurance **MUST** be sufficient for the sensitivity of the personal data to be disclosed. Thus, the *minimum* level of assurance required of a Requesting Organization must be equal to or higher than the *highest* level of assurance requirement associated with all of the data being requested. 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 specific, informed, freely given, 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: • in clear and plain language; • concise; • easily visible; • transparent; • accessible; and • is clearly distinguishable from the other matters contained in the statement.
7	The Disclosing Organization **MUST** have processes in place to show either the evidence of consent from the Subject for the collection, use, disclosure, or retention of the personal information, or that it has legislated authority for the collection, use, disclosure, or retention of the personal information without consent. 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	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.

9	In cases where a someone is acting on behalf of a Subject who is unable to provide consent digitally (e.g., disabled persons, digitally disadvantaged persons), persons acting on behalf of the Subject **MUST** ensure they providing consent only as directed by the subject and in compliance with the Notice and Consent Conformance Profile. Persons acting on behalf of such Subjects must also ensure that they are in compliance with legislation, regulation, and policy governing this type of assistive relationship in their jurisdiction.
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. 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 that was provided, and the kind of 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; • if applicable, the expiration date/time of consent; and • if no expiration is set at the time of consent that **SHOULD** be noted.
2	The Notice and Consent Processor **MUST** provide the evidence (described in **RECO 1**) to the relevant Requesting and Disclosing Organizations. Where the notice statement includes requests for consent from multiple organizations, the consent decision **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. For example, if a Subject's bank account number is required as evidence to one Disclosing Organization (i.e.: the bank from which information is being requested), that bank account number **MUST NOT** be disclosed to other Disclosing Organizations participating in the transaction.

3	Disclosing Organizations 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). Evidence **SHOULD** be retained only as long as necessary in order to fulfill the purpose for which it was collected. The Notice and Consent Processor, Requesting Organization, and Subject **MUST** have clear agreement and understanding of where the consent records will be stored. Consent records **MUST** be auditable and available to all three parties. Organizations and individuals **MUST** comply with relevant privacy legislation, policy, and regulations that govern retention of this type of data in their jurisdiction.
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, or available upon request, to the Subject and Requesting Organization.
5	Per applicable language legislation in the jurisdiction, each language (e.g., English, French) variation of the notice statement **MUST** be stored.
6	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).
7	Privacy-preserving practices, as defined in the Privacy Component Overview and Privacy Conformance Profile, **MUST** be followed when storing records of notice or records of consent. In this context, privacy-preserving practices refer to methods, approaches, or procedures designed to maintain the privacy of notice records and consent records and preventing unauthorized access to those records. Storage of records **MUST** comply with relevant privacy legislation, policy, and regulations that govern storage of this type of data in the relevant jurisdiction(s).
MANA	**Manage consent**
1	If a Requesting Organization wishes to obtain a revised consent from a Subject (e.g., to extend the duration for which consent is given), then the requirements set out above relating to notice, consent and record (**NOTI 1-7**, **CONS 1-9**, **RECO 1-7**) apply to the new consent. This **WILL** result in a new consent decision, which **MUST** be stored as a new consent record per **RECO 3**.

2	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 and in accordance with applicable legislation, regulations, and policies.
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 (e.g., if a fraudulent activity, data breach, or unauthorised access is confirmed, or consent is given by an entity without the authority to provide it).
4	A record of notice and/or consent **MUST** be considered invalid in the event that it is discovered that the consent was given by an entity without the authority or capacity to give it (e.g: when consent was given as a result of a data breach or unauthorized access). When a record of notice and/or consent is determined to be invalid 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, the affected Subject **MUST** be notified. All actions taken **MUST** comply with applicable legislation.

5	Where it is determined that the consent was not legitimate or lawful (e.g., was not conformant with the guidelines set forth in the PCTF or contravened a law, policy, or regulation in an applicable jurisdiction), 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 in accordance with applicable legislation, regulations, policies, and conformance criteria. Where permitted by regulation, legislation, and policies, the appropriate authorities (e.g., the relevant police force or anti-fraud organization) **SHOULD** be informed. 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 and Disclosing Organization(s). The Requesting Organization and Disclosing Organization(s) **MUST** then stop collecting, using or disclosing the personal information specified in the consent unless the collection, use, disclosure, or retention is permitted without consent. When consent is withdrawn (for any reason), the Notice and Consent Processor **SHOULD** inform third-party providers.
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 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 authorized reviewers to audit consent decisions. Authorized reviewers are participants impacted by the consent (e.g., Disclosing Organization, Requesting Organization) as well as regulatory bodies or oversight committees for audit.
9	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** verify that the individual withdrawing consent is the Subject in question**;** • **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.

Table 1. Notice and Consent Conformance Criteria

3 Revision History

Version Number	Date of Issue	Author(s)	Description
0.01	2017-01-30	SECUREKEY	Initial working draft
0.02	2017-03-26	DIACC	Updated to: • Incorporate notice requirements • Add first set of draft conformance criteria and definitions
0.03	2018-04-19	Consult Hyperion	First full draft
0.04	2018-04-26	Consult Hyperion	Addressed review comments
0.05	2018-05-31	Consult Hyperion	Finalized remaining comments
0.06	2018-06-06	Consult Hyperion	Refinements of scope section after Notice and Consent review meeting
0.07	2019-03-25	PCTF Editor	Updated for discussion draft
0.08	2019-05-24	PCTF Editor	Incorporated comments from discussion draft open review
1.0	2019-08-07	TFEC, PCTF Editor	Component is now in the Draft Recommendation stage
1.1	2019-12-13	PCTF Editor	Updates from Open Review of the Draft Recommendation, and apply standard PCTF component structure.
1.2	2020-02-10	PCTF Editor	Updates to incorporate feedback from the public review.
1.0	2020-05-11	PCTF Editor	Final Recommendation V1.0