PCTF Notice & Consent

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, Final Recommendations are 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.

Table of Contents

1. Introduction to the Notice & Consent Component

Content herein concerns itself with the domain specific topic for this Pan-Canadian Trust Framework (PCTF) component. The overview section provides information related to and necessary for consistent interpretation of the included conformance criteria. For a general introduction to the PCTF, please see the PCTF Overview that describes the background, purpose, scope, principles, and objectives of the framework.

1.1 Purpose and Anticipated Benefits

The objective of the Notice & Consent Component is to ensure the on-going integrity of both the Notice & Consent processes by applying standardized conformance criteria for assessment and certification. A process that has been so certified is a trusted process that can be relied on by other participants of the Pan-Canadian Trust Framework (PCTF). The PCTF conformance criteria are intended to complement existing privacy legislation and regulations; participants in the digital identity ecosystem are expected to comply with relevant privacy legislation and regulations in their jurisdictions.

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.

The Notice & Consent Component defines a set of processes used to:

- Formulate a statement about the collection, use, disclosure, and retention of personal information.
- Obtain a meaningful and informed consent decision based upon that statement from a person authorized to do so.

The notice, and the consent, processes ensure notices are accurately formulated according to conformance criteria, that the person making the consent decision has the authority to do so, that the consent is valid (i.e., freely given, specific, informed and unambiguous), and that management of that consent decision is possible.

Figure 1 provides a conceptual overview and logical organization of the Notice & Consent Component (given the scope defined for this component below).

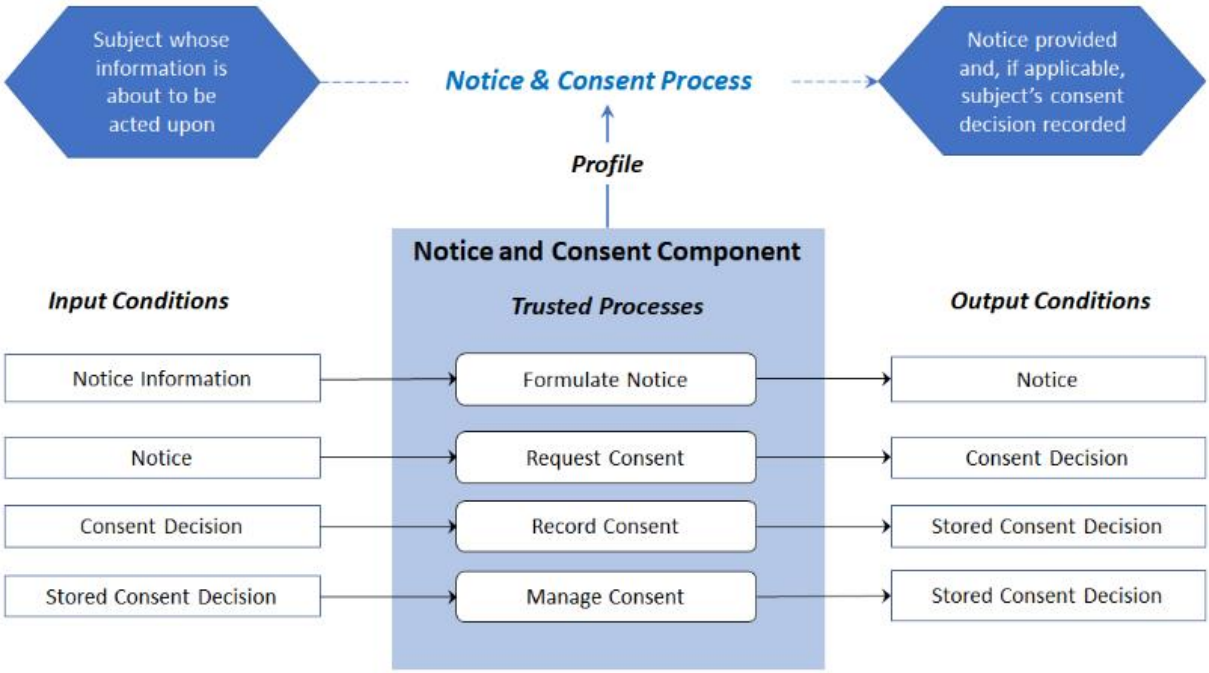

Figure 1. Notice & Consent Component

The Notice & Consent Component consists of elements that indicate:

- **Trusted Processes** – The set of processes that conform to conformance criteria (i.e., requirements) specified by the Pan-Canadian Trust Framework and which may be relied on (i.e., trusted) by others.
- **Conditions** – The particular states or circumstances relevant to making a consent decision.
- **Inputs** – Input into trusted processes, for example, a state requiring consent to proceed.
- **Outputs** – Output resulting from trusted processes, for example, a consent decision made by the subject.
- **Dependencies** – The relationship between trusted processes.
- **Profiles** – Additional criteria reflecting requirements or constraints that are relevant to a specific context (e.g., industry, public or private sector). Used to ensure consistency of implementation and facilitate the Pan-Canadian Trust Framework certification

1.2 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 2 is an illustration of the components of the Pan-Canadian Trust Framework. The Notice & Consent Component describes the processes and requirements to collect valid consent, which is integral but more specific than the general privacy requirements across the PCTF. Note that the privacy requirements for the handling of personal information by the Notice & Consent processes (and all other PCTF components) within the digital identity ecosystem are defined in the PCTF Privacy Component.

Figure 2. Components of the Pan-Canadian Trust Framework

1.3 Scope

The scope of the PCTF Notice & Consent Component and associated conformance criteria includes:

- The collection, use, disclosure, and retention of personal information for the purposes of establishing and asserting a digital identity and related verified Subject-Specific Personal Information
- Consent being obtained by a different organization than the one collecting, using or disclosing data – circumstances that could arise in a federated identity system.
- A single consent being obtained where multiple pieces of personal information are being collected, used or disclosed by multiple organizations, as part of a single transaction.
- Situations where the Subject may or may not have an explicit relationship with the information provider (e.g., where a background check is performed against a third-party source in accordance with relevant legislation); and
- Disclosure (or sharing) of data may follow either a "request" or "enquiry" mode:

  - "Request" mode retrieves personal data from another party. Example: Asking "please provide attribute X that corresponds to Y?"
  - "Enquiry" mode has personal data corroborated by another party. Example: Asking "is the combination of X and Y valid?".

For digital identity systems, Notice & Consent is expected to be characterized as follows:

- Consent will actively be sought. 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). Data protection laws allow for data to be collected without consent in certain circumstances (e.g., if disclosure is required to comply with a subpoena or legal requirement). Digital identity solutions are specifically concerned with providing visibility and control to Subjects over the collection, use, and disclosure of their personal information.
- Express consent will always be required. That is, the Subject should always perform a deliberate action to provide consent for collection and/or disclosure of some, or all, of the information requested by the Notice & Consent Provider except in cases where legislation or regulation either prohibits, or does not require, consent.
- Both notice, and consent, should take place at the time of transaction that it applies to;
- Consent can either be given only for the transaction in progress (i.e., one time); or may be given for a period of time (i.e., subscription services).
- Previously granted consent may be revoked by the Subject at any time.
- Consent will always be explicit, and in plain language
- Digital identity solutions will provide obvious and straightforward means for the Subject to manage consents, preferably in one place.
- The PCTF assumes that both Notice & Consent will be digital and online whenever possible. However, guidance from the Office of the Privacy Commissioner of Canada includes, for example, ensuring that staff are appropriately trained to provide notice and obtain consent in in-person and non-automated situations. The PCTF is focused on digital identity, namely identity services that, as far as possible, are digital. Where it is necessary to employ manual processes, it is assumed the guidance from the Office of the Privacy Commissioner of Canada or relevant legislation, regulation or policy in the appropriate jurisdiction will be followed. Additional guidance for obtaining meaningful consent in those cases can be found in the "Guidelines for obtaining meaningful consent" page of the Office of the Privacy Commissioner of Canada web site (https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/). Additional guidelines for training and accountability those cases can be found in the "Getting Accountability Right with a Privacy Management Program" area of the site (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/).

The scope of Notice & Consent Component does not include**:**

- The subsequent use of personal information by the organizations in the delivery of their services. The handling of Subject-Specific Personal Information by a Requesting Organization is subject to relevant legislation, policy, and/or regulations and is not generally deemed to fall within the scope of the requirements of the Digital Identity

Ecosystem once that data has been shared outside the Digital Identity Ecosystem. An exception to this is when a Disclosing Organization has specific requirements on the handling of personal information by its destination (the Requesting Organization). These requirements will thus form part of the digital identity ecosystem's governance and constitute "downstream" requirements with which any Requesting Organization receiving data from that Disclosing Organization must comply.

Similarly, the handling of Subject-Specific Personal Information by a Disclosing Organization is subject to relevant privacy legislation and regulations and is not generally deemed to fall within the scope of the requirements of the digital identity ecosystem until that data is processed for the purpose of sharing via the digital identity ecosystem. An exception to this is when a Disclosing Organization has specific requirements on the handling of personal information by its destination (the Requesting Organization). These requirements will thus form part of the digital identity ecosystem's governance and constitute "downstream" requirements that must be complied with by any Requesting Organization receiving data from that Disclosing Organization. For example, a healthcare agency that is a Disclosing Organization and has obligations that must be conveyed to a healthcare provider, which is a Requesting Organization (e.g., this identity can *only* be used for billing our agency), shall convey those obligations when the digital identity information is being exchanged.

- Use cases where another person acts on behalf of the Subject (e.g., power of attorney, a parent acting on behalf of a child). This version of the Notice & Consent Component only considers Subjects providing consent for the collection, usage, disclosure, and retention of personal information about themselves. Those use cases will be added in a future version.

1.4 Data Protection Laws and Notice & Consent

Digital identity is, by definition, concerned with providing entities with the digital means to collect, use and disclose verified personal information. Digital identity systems must, therefore, comply with data protection legislation, which includes requirements for Notice & Consent. The Notice & 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 must handle personal information in those provinces.

Given these considerations, PIPEDA Schedule 1- 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 & Consent Component. If conflicts arise between the Notice & Consent Component and any data protection law applicable to an organization, then the applicable law takes precedence. Future versions of this component may incorporate conformance criteria relevant

to other privacy guidance (e.g. Privacy by Design, PIPEDA modernization) and regulatory frameworks (e.g. federal and provincial privacy acts).

2. Conventions

2.1 Terms and Definitions

For purposes of the Notice & Consent component, terms and definitions listed in the PCTF Glossary, as well as the following terms and definitions apply.

Subject

In the context of the Notice & Consent component, Subject always refers to a Person. Also, note that Delegated Authority, where a person is acting on behalf of a Subject is not addressed in this version.

Notice

A statement that is formulated to describe the collection, use, disclosure, and retention of Personal Information and inform a User. Notice requirements for each jurisdiction's legislation must be adhered to. May also be referred to as: **consent form**; **notice statement**.

Consent

Permission, given from a User authorized to do so, to share Identity and/or Personal Information about a Subject as per the terms defined in a Notice. In the context of the PCTF, consent is equated to "Meaningful Consent" as described by the Office of the Privacy Commissioner of Canada and PIPEDA. Consent requirements for each jurisdiction's legislation must be adhered to. May also be referred to as: **consent decision**.

In the context of the PCTF, express consent will always be required (i.e., the Subject must perform an action to provide consent); also referred to as express or explicit consent.

Personal Information

In general, Personal Information is defined as "Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual." For the purpose of the PCTF Privacy, we define two types of Personal Information:

- **Service-Specific Information –** information collected or generated by the participants (Disclosing Organization, Requesting Organization, Notice & Consent Processor(s), or Network Facilitator) for purposes of operating and maintaining the service (e.g., service specific pseudonymous identifiers, transaction records, proofs of transactions including consent). In some cases, service-specific information may be shared, with Subject's consent.

- **Subject-Specific Personal Information –** information a Subject consents to share from a Disclosing Organization to a Requesting Organization (e.g., name, email address, phone number, mailing address, date of birth, account information).

The Notice & Consent conformance criteria only consider Subject-Specific Personal Information, which is referred to as Personal Information.

Digital Identity Ecosystem

An interconnected system for the exchange and verification of digital identity information, involving public and private sector organizations (e.g., government, commercial, non-profit, and other entities) that comply with a common Trust Framework for the management and use of digital identities, and the Subjects of those digital identities. In the context of the Privacy component, the Digital Identity Ecosystem refers to the Canadian digital identity ecosystem compliant with the PCTF.

2.2 Abbreviations

No abbreviations.

2.3 Roles

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

- **Disclosing Organization –** The organization that currently holds the personal information 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 & Consent Processor –** The organization that provides the notice to the Subject of the request for personal information (from the Requesting Organization), unless not required or permitted due to legislation or regulation, obtains and records the consent and provides the Subject with the means to manage the consent going forward, including the withdrawal of consent.
- **Authorized Reviewer –** Participants impacted by a notice statement and/or consent request or approval (i.e., Disclosing Organization, Requesting Organization, and others described in this section), as well as regulatory bodies or oversight committees requiring access to a record of notice or consent for audit.

These roles help to isolate the different functions and responsibilities that participants may perform in end-to-end Notice & 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 & 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 Organization or Requesting Organization, in which case that organization would also be the Notice & Consent Processor.

2.4 Levels of Assurance

Levels of assurance are used in certain contexts, such as those described in the PCTF Authentication Component or the PCTF Verified Person Component, to indicate the robustness of the processes employed to verify the login or the identity of an individual. Notice & Consent requirements apply across all levels of assurance; there is no equivalent to "unverified" or "low assurance" for Notice & 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 & 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 Authentication (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 & 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).

3. Trusted Processes

3.1 Trusted Processes and Conditions

A process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition; some transformations also depend on the output of another process. A business or technical process is designated as a trusted process when it is assessed and certified according to conformance criteria defined in the PCTF components and profiles.

In the Notice & Consent Component, for example, a Request Consent process transforms a "notice" input condition to a "consent decision" output condition. A trusted Notice & Consent business or technical process is assessed and certified according to conformance criteria stipulated by the Notice & Consent Conformance Profile and the Pan-Canadian Trust Framework.

3.2 Notice & Consent Trusted Processes

The Notice & Consent Component defines four trusted processes:

1. Formulate Notice
2. Request Consent
3. Record Consent
4. Manage Consent

Note: It is not expected that all trusted processes and all associated conformance criteria will apply in all circumstances or use cases, nor that they will occur in the order presented above.

3.2.1 Formulate Notice

The Formulate Notice process generates a statement that describes the information that will be collected. The information required is based on applicable legal, policy and contractual requirements and could include, but is not limited to:

1. What personal information is being collected, used or disclosed;
2. What the purpose is for the collection, use, disclosure, or retention of the information;
3. To whom the information will be disclosed (organizations, individuals, or both depending on circumstances);
4. The source of the requested personal information, be it the Disclosing Organization or the Subject;
5. How the information will be handled and/or protected;
6. The time period for which the notice is applicable;
7. Under whose jurisdiction or authority the notice is applicable;
8. Contact information for an authorized person who can answer the Subject's questions about the collection; and
9. Additional information required by relevant legislation, policy, and regulations in the relevant jurisdiction.

This statement is presented to a person in the form of a Notice.

3.2.2 Request Consent

The Request Consent process presents the Notice to a Subject and provides the capability for the Subject to accept (i.e., give) or decline (i.e., deny) consent based on the contents of the Notice, resulting in a meaningful consent decision.

The Request Consent process is intended to ensure that the Subject who is being asked to provide consent has the authority to do so. The Request Consent process will typically rely on trusted processes defined in other PCTF components (e.g., Authentication, Verified Person, Verified Relationship) to authenticate the Subject, confirm Subject identity, and confirm Subject authority to make a consent decision.

3.3.3 Record Consent

The Record Consent process makes a record of the notice conditions and the Subject's consent decision. This record is persistent and *may* be retained for historical reference even if the Subject subsequently revokes consent. In some cases, retention may be subject to legislation or

regulations. Examples of notice conditions that may be stored include information about the Subject, the recognized authority that provided consent (if applicable), the date and time that the notice was presented, and the version of the notice presented. Examples of consent decision information that may be stored include: the notice conditions along with the decision made by the Subject, the date and time of consent and, if applicable, the expiration date for the consent. Though records of consent should store information about the *type* of data a Subject consented to share, they should not contain the Subject's data. (e.g., such a record might indicate that a Subject consented their address *be used* but would not contain their actual address.) While consent may be revoked or changed as previously mentioned, records of consent should not be altered.

Storage and/or retention of notice conditions and consent decision information must comply with the legislation and regulations of the jurisdiction(s) where the Record Consent is being applied. Once the consent decision has been stored, the relevant parties to the consent decision are notified of the consent decision. Records of consent can, and should, be destroyed when no longer needed, provided that is compliant with relevant legislation and regulations.

3.3.4 Manage Consent

The Manage Consent process manages the lifecycle of consent decisions and includes:

- Reviewing consent, which makes the details of a stored consent decision visible to the Subject and authorized reviewers, follows proper and applicable privacy practices, and respects relevant legislation, regulation, and policy. Note: Authorized reviewers are participants impacted by the consent (i.e., Disclosing Organization, Requesting Organization) as well as regulatory bodies or oversight committees for audit.
- Renewing a consent decision, where the Subject or recognized authority establishes a revised consent decision from a previously stored consent decision based on a change in purpose or a period of time that has passed where there could be a change in circumstances since the previous consent.
- Expiring a consent decision based on a set timeframe for its validity.
- Revoking a consent, which includes the Subject actively withdrawing consent and situations where revocation results from other events (e.g., consent is found to be fraudulent).

The Manage Consent process results in an updated consent decision that can be stored via the Record Consent process.

3.3 Notice & Consent Conditions

3.3.1 Input and Output Conditions

Table 1 specifies the input and output conditions for the Notice & Consent Component.

Condition	Description
Notice Information	Information used to formulate a statement that is presented to a Subject to formulate an appropriate Notice and, if applicable, to obtain the consent necessary to continue with the service process. The information required is based on applicable legal, policy and contractual requirements.
Notice	The presentation of a statement containing the Notice Information to the Subject.
Consent Decision	The decision by the Subject to provide consent or decline consent.
Stored Consent Decision	The record of the notice conditions and consent decision to a storage medium.

Table 1. Notice & Consent Component Conditions

3.3.2 Dependencies

Trusted processes may need to depend on a condition that is the output of another trusted process. Figure 3 illustrates the dependencies between the trusted processes of the Notice & Consent Component, and trusted processes in other PCTF components.

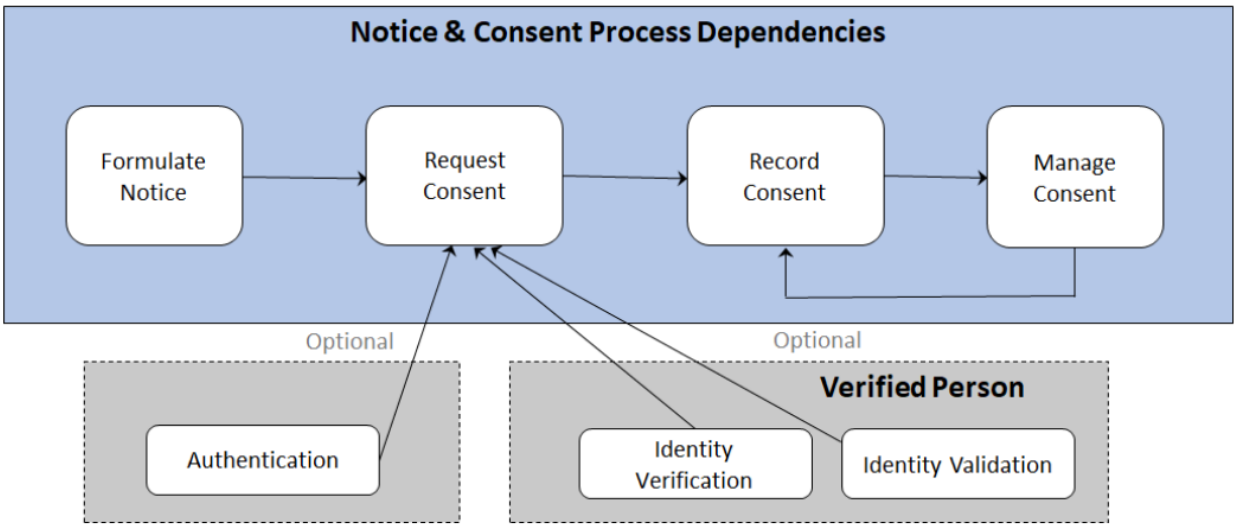

Figure 3. Trusted Process Dependencies

4. Introduction to Notice & Consent Conformance Criteria

This section specifies the set of conformance criteria for the Notice & Consent Component, a component of the Pan-Canadian Trust Framework (PCTF). The Notice & 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.

4.1 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**.

5. Trusted Processes and Conformance Criteria

5.1 Trusted Processes

The Notice & Consent Conformance Profile defines conformance criteria as essential requirements for the trusted processes defined in the Notice & 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.

5.2 Notice & Consent Conformance Criteria

Conformance criteria are organized by the Trust Processes defined in the Notice & 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 & 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 & 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 & 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 & Consent Conformance Profile or other laws, regulations, or policies that are applicable in the relevant jurisdiction The Notice & Consent Processor **SHOULD** inform the Subject of the identity of the Requesting and Disclosing Organizations receiving the evidence. The Notice & 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 & 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 & 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 & 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 & 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 & 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 & 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 & 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 & Consent Processor.
8	Where a Subject has the right to withdraw their consent at a later date, the Requesting Organization (or the Notice & 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 & 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 & 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 & 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 & 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 & Consent Processors **MUST** employ processes and procedures to prevent the loss of Notice & 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 & 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 & Consent Processor **MUST** revoke the consent as per **MANA 3**. The Notice & 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 & 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 & 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 & Consent Processor **SHOULD** inform third-party providers.
7	The Notice & 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 & 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 & 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 & 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.

6. Notes

- More than one organization may be responsible for carrying out the Notice & Consent trusted processes from end-to-end.

  For example, the Request Consent process may be the responsibility of one organization, and the Record Consent process may be the responsibility of a different organization. While the involvement of multiple organizations may introduce complexity in the assessment and certification process, the PCTF does not impose specific implementation approaches. However, all approaches must respect relevant legislation, policy, and regulations.

  To help isolate the different functions and responsibilities within the end-to-end process, the Notice & Consent Conformance Profile defines, in the **Roles section**, three organizational roles (Disclosing Organization, Requesting Organization, and Notice & Consent Processor). These delineations do not imply any particular solution, architecture or implementation.

- Notice and/or consent may be required multiple times in a single digital identity flow. For example, a Subject may consent to share specific, limited information at the beginning of a transaction. Subsequently a Requesting Organization may discover that additional information is required in order to complete the transaction and that they must issue an additional request for consent to share that additional information. Additional notices and/or consent requests can also occur when a downstream process requires services from an additional party (not involved in the initial consent process) and consent to share information with that new party is required.

7. References

1. Government of Canada, Department of Justice. *Personal Information Protection and Electronic Documents Act (Canada). Schedule 1, Section 5*. <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-11.html>
2. Government of Canada, Department of Justice. *Official Languages Act (Canada).* <https://laws-lois.justice.gc.ca/eng/acts/o-3.01/>

8. Revision History

Version Number	Date of Issue	Author(s)	Description
0.01	2017-01-30	SECUREKEY	Initial working draft
0.02	2018-04-19	Consult Hyperion	First full draft
0.03	2018-04-26	Consult Hyperion	Addressed review comments
0.04	2019-03-25	PCTF Editor	Updated for discussion draft
0.05	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, 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	Approved as Final Recommendation V1.0 through DIACC Sustaining Member Ballot