

Ébauche de recommandations pour le profil de conformité de l'avis et du consentement

Version 1.0

Cette ébauche de recommandations a été préparée par le Comité d'experts du cadre de confiance (TFEC) du [Digital ID & Authentication Council of Canada](#) (DIACC). Le TFEC est régi par les politiques du DIACC en matière de contrôle. Les commentaires soumis par le public sont assujettis à l'[entente de contributeur du DIACC](#).

Le DIACC prévoit modifier et améliorer cette ébauche de recommandations en fonction des commentaires du public. Les commentaires ouverts ont pour but d'assurer la transparence de l'élaboration et la diversité d'un apport véritablement pancanadien. Les commentaires effectués pendant l'examen seront pris en considération en vue d'être incorporés dans la prochaine ébauche. Le DIACC va regrouper les commentaires afin de montrer d'une façon transparente comment chacun a été traité.

Les prochaines versions du cadre de confiance pancanadien vont étoffer, clarifier et peaufiner le contenu de ce document. L'auditoire ciblé inclut des décideurs qui peuvent être ou non des experts dans la technologie des domaines.

En examinant cette ébauche de recommandations, veuillez tenir compte de ce qui suit :

1. Est-ce que la liste des processus de confiance pour l'avis et le consentement cadre avec les processus en place dans votre organisation ou entreprise?
2. La description des processus de confiance est-elle claire et exacte?
3. Les critères de conformité sont-ils clairs et mesurables?
Y a-t-il des critères de conformité que vous recommanderiez d'ajouter?
4. Est-ce que les termes utilisés pour décrire l'avis et le consentement dans ce document sont censés dans le ou les contextes que vous connaissez?

Table des matières

1. [Introduction aux critères de conformité de l'avis et du consentement](#)
 - 1.1. [Relation avec le cadre de confiance pancanadien](#)
 - 1.2. [Mots clés](#)
 - 1.3. [Lois sur la protection des données et critères de conformité](#)
 - 1.4. [Rôles](#)
2. [Processus de confiance et critères de conformité](#)
 - 2.1. [Processus de confiance](#)
 - 2.2. [Niveaux d'assurance](#)
 - 2.3. [Critères de conformité de l'avis et du consentement](#)

42

43 1 Introduction aux critères de 44 conformité de l'avis et du 45 consentement

46 Ce document spécifie l'ensemble de critères de conformité pour la composante « Avis et
47 consentement » du cadre de confiance pancanadien. Les critères de conformité de l'avis et du
48 consentement spécifient les exigences que doivent remplir les participants à l'avis et au
49 consentement pour émettre des avis conformes et compréhensibles sur le plan juridique,
50 obtenir des consentements donnés en connaissance de cause et autorisés, et permettre la
51 gestion continue de ces consentements.

52 Les critères de conformité sont essentiels pour le cadre de confiance, car ils spécifient les
53 exigences essentielles convenues par les participants au cadre de confiance afin d'assurer
54 l'intégrité de leurs processus. Cette intégrité est fondamentale, étant donné que beaucoup de
55 participants se fient à l'extrant ou au résultat d'un processus de confiance – à la longue et par-
56 delà les frontières organisationnelles, juridictionnelles et sectorielles.

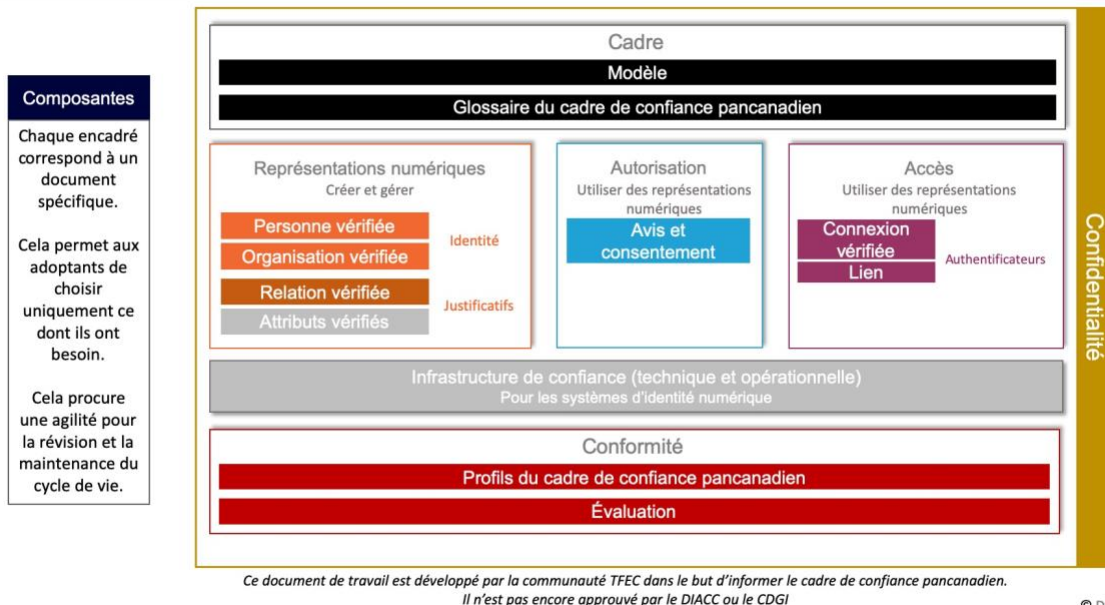
57 Les critères de conformité du cadre de confiance pancanadien visent à compléter les lois et
58 règlements existants sur le respect de la vie privée; on s'attend à ce que les participants à
59 l'écosystème de l'identité numérique remplissent les exigences de la loi et les règlements
60 applicables dans leurs territoires de compétence.

61 1.1 Relation avec le cadre de confiance pancanadien

62 Le cadre de confiance pancanadien est composé d'un ensemble de composantes modulaires
63 ou fonctionnelles qui peuvent être évaluées et certifiées d'une manière indépendante pour être
64 prises en considération en tant que composantes de confiance. Le cadre de confiance
65 pancanadien, qui adopte une approche pancanadienne, permet aux secteurs public et privé de
66 collaborer pour protéger les identités numériques en uniformisant les processus et les pratiques
67 dans tout l'écosystème numérique canadien.

68 La figure 1 donne un aperçu logique du cadre de confiance pancanadien. La composante « Avis
69 et consentement » décrit le bloc « Autorisation », qui fait partie des fonctions d'« utilisation des
70 représentations numériques ». Veuillez noter que les exigences en matière de confidentialité
71 pour le traitement des renseignements personnels par le biais des processus d'avis et de
72 consentement (et toutes les autres composantes du cadre de confiance pancanadien) à
73 l'intérieur de l'écosystème de l'identité numérique sont définies dans la composante « Respect
74 de la vie privée » du cadre de confiance pancanadien.

Schématisation des documents de travail sur le cadre de confiance pancanadien



75

76 **Figure 1. Ébauche visuelle du modèle de cadre de confiance pancanadien**

77 **1.2 Mots clés**

78 Afin d'assurer une application uniforme, les mots clés en **caractères gras** dans les critères de
79 conformité doivent être interprétés comme suit :

- 80 • **DOIT** signifie que l'exigence est impérative en ce qui concerne les critères de
81 conformité.
- 82 • **NE DOIT PAS** signifie que l'exigence est une interdiction absolue des critères de
83 conformité.
- 84 • **DEVRAIT** signifie que même s'il peut y avoir des raisons valables dans des
85 circonstances particulières pour ignorer l'exigence, toutes les implications devraient être
86 comprises et considérées avec soin avant de décider de ne pas respecter les critères de
87 conformité ou de choisir une autre option tel que spécifié par les critères de conformité.
- 88 • **NE DEVRAIT PAS** signifie qu'il peut exister une raison valable dans des circonstances
89 particulières pour que l'exigence soit acceptable ou même utile, mais que toutes les
90 implications devraient être comprises et le cas devrait être bien pris en considération
91 avant de choisir de ne pas se conformer aux exigences telles que décrites.
- 92 • **PEUT** signifie que l'exigence est discrétionnaire mais recommandée.

93 D'autres mots clés, comme des définitions normatives dans des normes et spécifications connexes,
94 seront également indiqués en **caractères gras**.

95

96 1.3 Lois sur la protection des données et critères de 97 conformité

98 L'identité numérique consiste, par définition, à fournir à des entités des moyens numériques de
99 recueillir, gérer et partager des renseignements personnels vérifiés. Les systèmes d'identité
100 numérique doivent donc se conformer aux lois sur la protection des données, ce qui inclut les
101 exigences en matière d'avis et de consentement. Le profil de conformité de l'avis et du
102 consentement ne répète pas les exigences des lois, mais il indique comment ces exigences
103 s'appliquent dans le contexte du cadre de confiance pancanadien.

104 De nombreuses lois sur la protection des données couvrent les opérations des organisations
105 lorsque des renseignements personnels sont traités. Au niveau fédéral, la *Loi sur la protection
106 des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les
107 documents électroniques* (LPRPDE) s'appliquent au gouvernement fédéral et aux organisations
108 commerciales, respectivement. Chaque province et territoire a ses propres lois qui régissent le
109 traitement des renseignements personnels par des organismes gouvernementaux provinciaux
110 et territoriaux. Plusieurs lois provinciales ont aussi été jugées « particulièrement similaires » à la
111 LPRPDE et concernent la façon dont les organisations du secteur privé traitent les
112 renseignements personnels dans ces provinces.

113 Étant donné cela, le principe 3 de LPRPDE relatif à l'équité dans le traitement de l'information
114 (Consentement), ainsi que les conseils du Commissariat à la protection de la vie privée du
115 Canada, fournit un cadre qui peut être appliqué à une série d'organisations et de cas
116 d'utilisation, et qui sert de base à la composante « Avis et consentement » du cadre de
117 confiance pancanadien. Advenant des conflits entre la composante « Avis et consentement » et
118 une loi applicable à la protection des données, la loi applicable a alors préséance.

119 1.4 Rôles

120 Les rôles qui suivent sont définis pour couvrir la portée des critères de conformité de l'avis et du
121 consentement. Selon le cas d'utilisation, différentes organisations peuvent jouer un ou plusieurs
122 rôles :

- 123 • **Sujet** – la personne naturelle à qui s'appliquent les données personnelles en question.
124 Remarque : cette version des critères de conformité ne traite pas de l'autorité déléguée.
125
- 126 • **Organisation divulgatrice** – l'organisation qui détient actuellement les données
127 personnelles, que le sujet consent à divulguer à une organisation requérante. Dans un
128 contexte d'identité numérique, ce sera souvent un fournisseur d'identité ou d'attributs.
129 Les renseignements personnels vérifiés par une organisation divulgatrice et représentés
130 dans un appareil du sujet sont considérés comme faisant partie de l'organisation
131 divulgatrice.
132
- 133 • **Organisation requérante** – l'organisation à laquelle le sujet consent à divulguer des
134 renseignements personnels. Dans un contexte d'identité numérique, ce sera souvent un
135 fournisseur de services ou une partie utilisatrice
136

- 137 • **Responsable du traitement de l'avis et du consentement** – organisation qui avise le
138 sujet de la demande de renseignements personnels (émanant de l'organisation
139 requérante), obtient et enregistre le consentement, et fournit au sujet le moyen de gérer
140 le consentement à l'avenir, y compris le retrait du consentement.

141 Ces rôles aident à isoler les différentes fonctions et responsabilités que les participants peuvent
142 exécuter dans les processus d'avis et de consentement de bout en bout. Ils n'impliquent pas
143 une solution, architecture ou mise en œuvre en particulier. Dans certains cas, par exemple,
144 l'avis peut être présenté et le consentement obtenu d'un exploitant de réseau (agissant comme
145 responsable du traitement de l'avis et du consentement) qui facilite l'échange de
146 renseignements personnels entre un patient (le sujet), un laboratoire médical (organisation
147 divulgateur) et un hôpital (organisation requérante). Dans d'autres cas, l'avis peut être présenté
148 et le consentement obtenu directement par l'organisation divulgateur ou requérante, auquel cas
149 cette organisation serait aussi responsable du traitement de l'avis et du consentement.

150 **2 Processus de confiance et critères de** 151 **conformité**

152 **2.1 Processus de confiance**

153 Le profil de conformité de l'avis et du consentement définit les critères de conformité en tant
154 qu'exigences essentielles pour les processus de confiance définis dans l'aperçu de la
155 composante « Avis et consentement », à savoir :

- 156 1. **Formulation de l'avis** – processus consistant à déterminer quels renseignements
157 personnels doivent être recueillis, utilisés ou divulgués, par qui et à qui, et à quelles fins
158 (c.-à-d., les conditions de l'avis). Ce processus formule l'avis qui sera présenté au sujet.
159
- 160 2. **Demande de consentement** – processus consistant à déterminer que le sujet à qui on
161 demande de donner son consentement est autorisé à le faire, à présenter l'avis au sujet,
162 puis à obtenir du sujet sa décision relative au consentement (c.-à-d. acceptation ou
163 refus).
164
- 165 3. **Enregistrement du consentement** – processus consistant à enregistrer les conditions
166 de l'avis et la décision du sujet relative au consentement, et à aviser les parties
167 pertinentes de la décision.
168
- 169 4. **Gestion du consentement** – processus consistant à soutenir la gestion permanente
170 autorisée des décisions relatives aux consentements, notamment l'examen, le
171 renouvellement, l'expiration et la révocation de ces décisions.

172 **2.2 Niveaux d'assurance**

173 Les niveaux d'assurance sont utilisés dans certains contextes, comme ceux décrits dans la
174 composante « Connexion vérifiée » ou « Personne vérifiée » du cadre de confiance
175 pancanadien, pour indiquer la robustesse de la technologie et des processus employés pour
176 vérifier l'accès ou l'identité d'une personne. Les exigences concernant l'avis et le consentement

177 s'appliquent à tous les niveaux d'assurance; il n'y a pas d'équivalent au niveau « non vérifié »
178 ou « assurance faible » pour les processus de confiance en ce qui concerne l'avis et le
179 consentement.

180 L'obtention du consentement devrait se faire à peu près de la même manière, que le niveau
181 d'assurance soit faible ou plus élevé. Par conséquent, les critères de conformité de la
182 composante « Avis et consentement » devraient refléter ce qui suit :

- 183 • La divulgation des données sensibles (p. ex., attributs liés à la santé) ne devrait être
184 faite qu'avec un niveau d'assurance approprié à la personne vérifiée et à la connexion
185 vérifiée qui lui sont associées (voir CONS 3) et conformément aux lois pertinentes;
- 186 • Le consentement peut être enregistré de différentes façons avec différents niveaux de
187 robustesse. Par exemple, un drapeau dans une base de données pourrait indiquer que
188 l'utilisateur a coché une case. Pour le consentement donné, une signature numérique
189 peut fournir un niveau de non-répudiation plus élevé que le fait de cliquer dans une
190 case. Cette version des critères de conformité de l'avis et du consentement ne fait pas la
191 distinction entre de telles approches, mais elle exige que le processus de consentement
192 ait un niveau minimal de robustesse pour satisfaire aux exigences réglementaires (voir
193 RECO 1).

194 **2.3 Critères de conformité de l'avis et du** 195 **consentement**

196 Les critères de conformité sont organisés par les processus de confiance définis dans la
197 composante « Avis et consentement ». Pour faciliter la référence, un critère de conformité
198 spécifique peut être désigné par son numéro de catégorie et de référence (p. ex., « **NOTI 1** »
199 correspond à la « référence n° 1 de la formulation des critères de conformité de l'avis »).

179	Référence	Critères de conformité
180	BASE	Base
181		Les organisations qui jouent les rôles définis dans le présent document doivent se conformer à tous les critères de base concernant la conformité au respect de la vie privée stipulés dans le profil de conformité au respect de la vie privée.
182	NOTI	Formulation de l'avis
183	1	Le responsable du traitement de l'avis et du consentement DOIT avoir des processus en place pour s'assurer que les avis appropriés concernant la collecte, l'utilisation ou la divulgation des renseignements personnels sont formulés (conformément à NOTI 5) et fournis aux sujets au moment où les renseignements personnels sont recueillis ou avant cela.
184	2	Le responsable du traitement de l'avis et du consentement DOIT avoir en place des processus, des ressources et une supervision appropriés pour s'assurer que les avis sont conformes au processus de confiance « Formulation de l'avis », incluent tous les renseignements exigés et sont mis à jour en temps opportun lorsque les exigences ou la raison pour recueillir, utiliser ou divulguer les renseignements personnels changent.

185

3	<p>Le responsable du traitement de l'avis et du consentement DOIT déterminer quels renseignements doivent être inclus dans les avis compte tenu de toutes les exigences légales, contractuelles et en matière de politiques applicables. Dans un système d'identité numérique, cela pourrait inclure :</p> <ul style="list-style-type: none"> • les renseignements personnels sur le sujet qui sont demandés par l'organisation requérante; • la raison pour laquelle les renseignements personnels sont demandés; • les détails sur l'organisation ou les organisations requérantes; • les coordonnées (p. ex., titre, adresse et numéro de téléphone d'affaires) d'une personne autorisée pouvant répondre aux questions du sujet sur l'obtention des renseignements; • l'autorisation légale de recueillir les renseignements; • la période pour laquelle les renseignements personnels demandés seront enregistrés ou utilisés; • le fait que la demande est pour une seule divulgation des renseignements personnels ou pour permettre la divulgation continue (en arrière-plan) aux mêmes fins, p. ex., pour permettre au sujet de « diffuser » les mises à jour de ses renseignements personnels, comme un changement d'adresse, d'une manière efficace mais contrôlée; • la façon de reprendre le consentement (pour une divulgation continue); • les détails des sources potentielles des renseignements personnels demandés, qu'il s'agisse des organisations divulgatrices ou du sujet en question. <p>Le responsable du traitement de l'avis et du consentement DOIT s'assurer que les renseignements devant être inclus dans un avis sont définis d'une manière précise. Dans un contexte d'identité numérique, cela pourrait inclure, par exemple, les renseignements personnels spécifiques à partager et les métadonnées nécessaires.</p>
---	--

186

4	<p>Le responsable du traitement de l'avis et du consentement DOIT s'assurer qu'un nouvel avis est fourni à un sujet lorsque l'organisation décide d'utiliser ou de divulguer des renseignements personnels qu'elle a déjà recueillis auprès du sujet à de nouvelles fins (qui ne sont pas conformes à celles fournies dans l'avis original).</p> <p>Le nouvel avis DOIT :</p> <ul style="list-style-type: none"> • indiquer les nouvelles fins et les renseignements personnels spécifiques qui seront utilisés ou divulgués pour les nouvelles fins; • inclure d'autres renseignements applicables qui peuvent être nécessaires (comme le type de renseignements déterminé par NOTI 3); • demander le consentement du sujet pour utiliser ou divulguer les renseignements personnels pour les nouvelles fins.
---	--

187

5	<p>L'avis DEVRAIT être fourni par écrit et DOIT être donné de manière à permettre aux sujets de comprendre raisonnablement comment leurs renseignements personnels seront utilisés ou divulgués. Cela consiste à fournir un avis d'une manière :</p> <ul style="list-style-type: none"> • intelligible (en utilisant un langage clair et simple); • concise; • facilement visible; • transparente; • facilement accessible. <p>Si ce n'est pas pratique pour l'avis d'inclure des détails supplémentaires concernant la demande (p. ex., conditions intégrales, métadonnées détaillées), un moyen pratique DEVRAIT être fourni pour permettre au sujet d'examiner ces détails, idéalement dans le cadre du flux de travail numérique fourni. Cela NE DOIT PAS être un moyen de rendre l'avis moins visible, transparent ou accessible.</p> <p>L'établissement d'une identité numérique peut comprendre l'utilisation de canaux non numériques pour recueillir des renseignements personnels. Dans ces cas, les processus DOIVENT être employés pour s'assurer que l'avis, peu importe la façon dont il a été donné, remplit les exigences ci-dessus.</p>
188	<p>6</p> <p>Dans certains scénarios, un seul avis peut inclure des demandes de consentement de la part de multiples organisations, par exemple, pour la divulgation des attributs provenant de plusieurs sources.</p> <p>Lorsque l'avis inclut des demandes de plusieurs organisations, l'avis DOIT ÊTRE conçu de sorte qu'il puisse être divisé selon les parties s'appliquant à chaque organisation, afin d'enregistrer et d'entreposer le consentement (voir RECO 2 ci-dessous).</p>
189	<p>CONS Demande de consentement</p>
190	<p>1</p> <p>Le processus consistant à demander le consentement d'un sujet DOIT inclure la présentation de l'avis et de la vérification du sujet, comme suit :</p> <ul style="list-style-type: none"> • l'avis DOIT précéder l'intervention du sujet qui donne son consentement; • si l'avis ne divulgue pas de renseignements personnels, la vérification du sujet n'est pas requise avant l'affichage; • si l'avis divulgue des renseignements personnels, l'identité du sujet DOIT alors être vérifiée avant l'affichage; • indépendamment du moment où l'avis survient, le sujet DOIT avoir été vérifié avec succès avant de pouvoir se fier à un consentement.

191

2	<p>Le responsable du traitement de l'avis et du consentement, l'organisation divulgateuse et/ou l'organisation requérante DOIVENT vérifier que la personne qui donne le consentement est le sujet en question et qu'elle est donc autorisée à effectuer l'intervention.</p> <p>Un certain nombre de scénarios peuvent se produire :</p> <ul style="list-style-type: none"> • L'organisation requérante demande des renseignements personnels précédemment recueillis auprès d'une organisation divulgateuse. Dans ce cas, le responsable du traitement de l'avis et du consentement et l'organisation divulgateuse DOIVENT prendre des mesures pour vérifier (ou authentifier) que la personne effectuant l'intervention est le sujet en question. • L'organisation requérante recueille auprès du sujet de nouveaux renseignements personnels qui sont destinés à être associés au sujet. Dans ce cas-là, l'organisation requérante et le responsable du traitement de l'avis et du consentement DOIVENT prendre des mesures pour vérifier (ou authentifier) que la personne effectuant l'intervention est le sujet en question. <p>L'organisation requérante recueille de nouveaux renseignements personnels auprès d'un nouveau sujet. Dans ce cas-là, le processus DOIT être effectué conjointement avec les processus « Personne vérifiée » et « Connexion vérifiée » pour s'assurer que le sujet est vérifié et qu'il contrôle l'accès subséquent à ses données personnelles.</p> <p>Les sujets DEVRAIENT pouvoir effectuer eux-mêmes la vérification rapidement et d'une manière sécuritaire.</p>	
192	3	<p>Le niveau d'assurance pour la vérification ou l'authentification DOIT être suffisant pour la sensibilité des données personnelles à divulguer. L'organisation divulgateuse détermine habituellement le niveau de sensibilité des données à partager en fonction du contexte (p. ex., type de renseignements, utilisation prévue).</p>
193	4	<p>L'intervention de la part du sujet pour donner son consentement DOIT être claire, explicite et directe.</p> <p>Si le sujet se voit proposer un choix dans le consentement demandé (p. ex., pour partager un sous-ensemble des renseignements personnels demandés), l'intervention requise pour effectuer le choix DOIT être claire, explicite et directe.</p>
194	5	<p>Le responsable du traitement de l'avis et du consentement DOIT s'assurer que ce consentement est affirmatif, spécifique, informé et sans ambiguïté.</p>

195	6	<p>Si le consentement du sujet est demandé dans le cadre d'une déclaration écrite qui porte sur d'autres questions, la demande de consentement DOIT être présentée d'une manière qui :</p> <ul style="list-style-type: none"> • la différencie nettement des autres questions; • est sous une forme intelligible et facilement accessible; • utilise un langage clair et simple.
196	7	<p>L'organisation divulgateuse DOIT avoir des processus en place qui lui permettent de démontrer facilement qu'un sujet a consenti à la collecte, l'utilisation ou la divulgation de ses renseignements personnels, ou qu'elle est autorisée par la loi à recueillir, utiliser ou divulguer les renseignements personnels.</p> <p>Dans le cas où le responsable du traitement de l'avis et du consentement est une organisation distincte de l'organisation divulgateuse, l'organisation divulgateuse DOIT alors s'assurer que le responsable du traitement de l'avis et du consentement a en place des processus adéquats.</p>
197	8	<p>Avant de demander le consentement d'un sujet, l'organisation requérante DOIT déterminer si le sujet peut reprendre son consentement à une date ultérieure ou si des restrictions légales ou contractuelles empêchent ou limitent le retrait du consentement.</p> <p>S'il n'existe pas un moyen clair et facile à comprendre de reprendre le consentement, cela DOIT être divulgué dans l'avis lorsque les renseignements sont demandés.</p>
198	9	<p>Si un sujet a le droit de reprendre son consentement à une date ultérieure, l'organisation requérante (ou le responsable du traitement de l'avis et du consentement agissant pour son compte) DOIT :</p> <ul style="list-style-type: none"> • informer le sujet de son droit (sous réserve d'un avis raisonnable et des conditions ou restrictions applicables) au moment où le consentement est demandé; • informer le sujet de la façon d'exercer ce droit; • s'assurer qu'il est aussi facile pour le sujet de reprendre le consentement que de le donner.
199	RECO	Enregistrement du consentement

200	1	<p>Une fois que le sujet a donné son consentement, le responsable du traitement de l'avis et du consentement DOIT obtenir les preuves suivantes :</p> <ul style="list-style-type: none"> • assez de renseignements pour déterminer qui a donné le consentement. Lorsque c'est possible, cela DOIT être relié à une personne vérifiée; • la date, l'heure ou tout autre renseignement contextuel sur le moment et la façon dont le consentement a été donné; • la version de l'avis fourni et les renseignements personnels demandés (c.-à-d., le type de renseignements, pas le contenu ou les renseignements comme tels); • la décision relative au consentement, qui DOIT être l'acceptation ou le refus, pour chaque consentement proposé; • le cas échéant, la date ou l'heure d'expiration du consentement.
201	2	<p>Le responsable du traitement de l'avis et du consentement DOIT fournir les preuves (décrites en RECO 1) aux organisations requérantes et divulgatrices pertinentes.</p> <p>Le responsable du traitement de l'avis et du consentement DEVRAIT informer le sujet de l'identité des organisations requérantes et divulgatrices qui reçoivent les preuves.</p> <p>Si l'avis inclut des demandes de consentement de plusieurs organisations, l'avis DOIT être divisé de façon à ce que chaque organisation ne reçoive que les preuves qui s'appliquent à elle.</p> <p>Les preuves concernant une organisation NE DOIVENT PAS être fournies à une autre organisation.</p>
202	3	<p>Les organisations divulgatrices et requérantes DOIVENT enregistrer les preuves d'une manière unique (c.-à-d., enregistrer les preuves une seule fois pour chaque consentement accordé) et immuable, de sorte que toute mise à jour ou tout changement d'état entraînera un nouveau dossier et les anciens dossiers peuvent être récupérés. L'entreposage des preuves DOIT aussi se conformer aux lois applicables (p. ex., dans certains cas, les données doivent être entreposées au Canada).</p>
203	4	<p>Les mises à jour des conditions et déclarations présentées au sujet DOIVENT comporter un numéro de version unique de façon à ce que les changements ultérieurs puissent être récupérés et soient accessibles en tout temps au sujet.</p>
204	5	<p>Conformément aux lois canadiennes sur les exigences linguistiques (français et anglais), chaque variation linguistique de l'avis DOIT être enregistrée.</p>

205	6	<p>Un dossier d'avis et de consentement PEUT devenir invalide si une infraction aux données personnelles ou un accès non autorisé sont découverts ou si l'on constate que le consentement a été donné sans avoir l'autorisation ou la capacité de le faire.</p> <p>Si l'une ou l'autre de ces situations se présente, les organisations touchées DOIVENT examiner les circonstances et prendre les mesures appropriées (p. ex., révoquer le consentement visé). En cas de vol de données incluant les renseignements personnels du sujet, elles DOIVENT aviser le sujet touché. Les mesures prises DOIVENT être conformes aux lois applicables.</p>
206	7	<p>Les organisations divulgatrices, les organisations requérantes et les responsables du traitement de l'avis et du consentement DOIVENT recourir à des processus et des procédures pour empêcher la perte des dossiers d'avis et de consentement et pour limiter l'impact des infractions à la sécurité des données, conformément aux lois pertinentes (p. ex., exigences d'un organe public en vertu de l'article 30 de la <i>Loi sur l'accès à l'information et la protection de la vie privée</i>).</p>
207	8	<p>Des pratiques visant à préserver la confidentialité des renseignements personnels DOIVENT être suivies pour l'enregistrement des dossiers de consentement. Dans ce contexte, les pratiques visant à préserver la confidentialité des renseignements personnels font référence à des méthodes, approches ou procédures conçues pour préserver la confidentialité des dossiers de consentement.</p>
208	MANA	Gestion du consentement
209	1	<p>Si une organisation requérante souhaite obtenir un consentement révisé d'un sujet, les exigences établies plus haut relativement à l'avis, au consentement et à l'enregistrement (NOTI1-6, CONS1-11, RECO1-8) s'appliquent au nouveau consentement. Cela VA entraîner un consentement à jour, qui DOIT être enregistré conformément à RECO 3.</p>
210	2	<p>Un consentement DOIT expirer quand la date d'expiration saisie dans le processus de consentement (RECO 1) est passée. Après cette date, l'organisation requérante DOIT (à moins que la loi applicable n'exige ou n'autorise leur utilisation et leur entreposage permanents) cesser d'utiliser les données personnelles en question pour les fins spécifiées et, au besoin, les supprimer d'une manière qui protège la vie privée du sujet.</p>
211	3	<p>La révocation du consentement DOIT survenir si :</p> <ul style="list-style-type: none"> • le sujet reprend son consentement; • il s'est écoulé un intervalle (déterminé par des considérations législatives, commerciales ou autres applicables) pendant lequel les circonstances dans lesquelles le consentement a été initialement obtenu auraient pu changer considérablement; • l'organisation divulgatrice, l'organisation requérante ou le responsable du traitement de l'avis et du consentement détermine que le consentement n'était pas légitime, par exemple, si une activité frauduleuse, un vol de données ou un accès non autorisé sont confirmés.

212	4	<p>Si un sujet avise le responsable du traitement de l'avis et du consentement qu'il souhaite reprendre le consentement donné et il n'y a pas de restrictions légales ou contractuelles empêchant le sujet de reprendre son consentement, le responsable du traitement de l'avis et du consentement:</p> <ul style="list-style-type: none"> • DOIT informer le sujet des implications d'un tel retrait; mais • NE DOIT PAS empêcher le sujet de reprendre son consentement; • L'intervention requise pour reprendre le consentement DOIT être claire, explicite et sans ambiguïté.
213	5	<p>S'il est déterminé que le consentement n'était pas légitime ou légal, le responsable du traitement de l'avis et du consentement DOIT reprendre le consentement conformément à MANA 3.</p> <p>Le responsable du traitement de l'avis et du consentement DOIT aussi informer le sujet (le cas échéant), l'organisation divulgateur et l'organisation requérante.</p> <p>En cas de vol d'identité où le sujet lui-même est compromis, ce n'est peut-être pas approprié d'informer le sujet du retrait du consentement. Afin de protéger les renseignements sur l'identité contre les abus et atteintes à la vie privée, la reprise du consentement dans de telles circonstances DOIT être faite avec beaucoup de soin. Le responsable du traitement de l'avis et du consentement DOIT s'assurer qu'il a en place des processus pour éviter le retrait erroné ou malveillant du consentement.</p>
214	6	<p>Quand un consentement est repris (pour quelque raison que ce soit), le responsable du traitement de l'avis et du consentement DOIT aviser l'organisation requérante. L'organisation requérante DOIT ensuite arrêter de recueillir, d'utiliser ou de divulguer les renseignements personnels spécifiés dans le consentement à moins que la collecte, l'utilisation ou la divulgation ne soit permise sans consentement.</p> <p>Lorsque le consentement est repris (pour quelque raison que ce soit), le responsable du traitement de l'avis et du consentement DEVRAIT informer les fournisseurs tiers (ce qui n'est pas toujours possible si le responsable du traitement de l'avis et du consentement ne connaît pas l'identité des tierces parties).</p>

215	7	<p>Le responsable du traitement de l'avis et du consentement DEVRAIT donner aux sujets la capacité de gérer tous les consentements accordés. Ces fonctionnalités DEVRAIENT être conviviales, et fournir aux sujets un moyen efficace et optimal de gérer les consentements.</p> <p>Cela devrait inclure :</p> <ul style="list-style-type: none"> • la capacité d'examiner, de mettre à jour ou de reprendre les consentements pour une organisation en particulier; • des moyens de recherche permettant de trouver facilement les décisions relatives aux consentements; • des notifications concernant les consentements expirés, qui pourraient indiquer la perte de service de la part d'une organisation requérante; • des descriptions des conséquences qu'entraîne la révocation du consentement du sujet (p. ex., répercussion sur les demandes ou paiements en cours de traitement); • au besoin, la capacité d'examiner, de mettre à jour ou de reprendre des consentements individuels à un niveau granulaire.
216	8	<p>Le responsable du traitement de l'avis et du consentement DEVRAIT fournir au sujet et aux examinateurs autorisés la capacité d'examiner les consentements donnés. Ces fonctionnalités DEVRAIENT être conviviales, et fournir au sujet et aux examinateurs autorisés un moyen efficace et optimal de gérer les consentements. Les examinateurs autorisés sont des participants visés par le consentement (c.-à-d., organisation divulgateuse, organisation requérante), ainsi que les organes de réglementation et les comités chargés de superviser les audits.</p> <p>Cela pourrait inclure, par exemple :</p> <ul style="list-style-type: none"> • la capacité d'examiner les consentements pour une organisation en particulier; • des moyens de recherche permettant de trouver facilement les consentements.

Tableau 1. Critères de conformité de l'avis et du consentement