

Cadre de référence
en matière de protection
des renseignements détenus
par une communauté ou une organisation
des Premières Nations du Québec



[COMMUNAUTÉ]

[LOI / RÈGLEMENT / POLITIQUE]

sur la protection des renseignements
détenus par

[COMMUNAUTÉ]

Mars 2014



Ce document constitue la version 1.0 du cadre de référence.

Document rédigé conjointement par :

M. Michel Deschênes, CSSSPNQL
M. Yvon Gauthier, Yvon Gauthier Info
Mme Nancy Gros-Louis McHugh, CSSSPNQL
M^e Elisabeth Patterson, Dionne Schulze S.E.N.C.
Mme Marjolaine Sioui, CSSSPNQL

Graphisme et mise en page :
Code jaune
Patricia Mathias, CSSSPNQL

Nous tenons à remercier le Conseil Mohawk d'Akwesasne pour avoir autorisé la consultation du document intitulé : *Access to Information and Protection of Personal Privacy Regulation*.

L'emploi du masculin dans ce document vise uniquement à alléger le texte, et ce, sans préjudice envers les femmes.

Ce document est disponible en version anglaise.

Ce document est accessible en version intégrale sur le site Internet de la CSSSPNQL : http://centredoc.cssspnql.com/opac/notice_view.php?id=754.

Reproduction autorisée à des fins non commerciales à la condition d'en mentionner la source.

ISBN : 978-1-926553-48-1

© 2014 CSSSPNQL. Tous droits réservés.

Ce document propose un cadre de référence adopté par l'Assemblée des Premières Nations du Québec et du Labrador (APNQL) dans sa résolution n° 07/2012¹. Il a été rédigé à l'intention des communautés, mais il peut très bien servir aux organisations des Premières Nations, notamment aux organisations régionales. Celles-ci devront cependant apporter les adaptations nécessaires au texte afin que le document reflète les particularités de leur structure organisationnelle et la nature de leurs pouvoirs.

Comme le révèle le rapport préliminaire² qui a précédé la réalisation de ce cadre de référence, la protection des renseignements personnels et confidentiels dans les communautés des Premières Nations ne repose pas sur des règles légales claires. Nous proposons librement ce cadre de référence aux communautés et aux organisations pour combler ce vide et répondre à un besoin manifesté par plusieurs communautés qui désirent améliorer leurs pratiques administratives. Il s'agit d'un document de base qui regroupe un ensemble de définitions, de principes et de règles respectant les lois et les règlements en vigueur, ainsi que les codes de pratique utilisés dans les administrations publiques au Canada et au Québec. Il couvre principalement les règles de protection des renseignements personnels, mais comprend aussi des dispositions relatives à la protection des données collectives et de toute autre information considérée comme confidentielle par un conseil de bande ou la direction d'un service ou d'une organisation.

Le contenu du cadre est rédigé de façon formelle, de sorte qu'une communauté puisse l'utiliser tel quel, simplement en décidant, au moment de son adoption, s'il s'agit d'un règlement administratif du conseil de bande (en vertu de la *Loi sur les Indiens*), d'un règlement interne ou d'une politique du conseil. On pourra aussi décider de le désigner comme loi au moment de son adoption, affirmant ainsi davantage une volonté d'autonomie gouvernementale. Pour leur part, les organisations régionales des Premières Nations pourront en faire un règlement ou une politique interne. Ce choix revêt de l'importance en regard de la portée conférée au cadre de référence envers les employés, les tiers ou, le cas échéant, la population³.

Idéalement, l'adoption de ce cadre de référence par une communauté ou une organisation devrait être accompagnée de séances d'information et de formation destinées au leadership, aux gestionnaires, aux directeurs et aux employés. La population d'une communauté devrait en outre être bien informée de ses droits et des mesures mises en place pour les protéger.

¹ Résolution n° 07/2012 — *Cadre de référence en matière de protection des renseignements détenus par une communauté ou une organisation Première Nation du Québec*. (Voir en annexe A de la présente.)

² CSSSPNQL, *Comité d'analyse sur l'élaboration d'une loi ou d'une politique en matière de protection des renseignements personnels et d'accès à l'information pour les Premières Nations du Québec — Rapport préliminaire des options*, déposé à l'Assemblée des Premières Nations du Québec et du Labrador, Hôtel Delta, Montréal, juin 2011. (Voir en annexe C de la présente.)

³ *Id.* voir les pages 7 et suivantes.

Table des matières

Avis au lecteur.....	iii
Table des matières.....	v
Préambule.....	1
Chapitre 1 - Interprétation et définitions	1
Chapitre 2 - Dispositions générales.....	3
1. Autorité relative à l'adoption de [ce Règlement/cette Politique/ Loi]	3
2. Entrée en vigueur de [ce Règlement/cette Politique/Loi]	3
3. Principes directeurs	3
4. Objet	3
5. Application	4
6. Modification à [ce Règlement/cette Politique/Loi]	4
7. Infractions	4
8. Responsable, plainte et révision	4
Chapitre 3 - Règles en matière de collecte et de protection des renseignements personnels.....	6
9. Collecte de renseignements personnels	6
10. Exactitude et conservation des renseignements personnels	7
11. Usage et communication des renseignements personnels.....	8
12. Renseignements personnels concernant les employés.....	11
Chapitre 4 – Droit d'accès et de correction	13
13. Droit d'accès et de correction	13
14. Exceptions au droit d'accès	13
Chapitre 5 – Protection des données collectives et de l'information confidentielle.....	15
15. Données collectives	15
16. Information confidentielle	15
17. Mesures de protection générales.....	16
18. Accès d'un tiers	17
Chapitre 6 – Mesures de sécurité	18
19. Mesures de sécurité.....	18
Annexe A – Résolution n° 07/2012 de l'APNQL	19
Annexe B – Les principes PCAP	20

Préambule

Le Conseil⁴ de [COMMUNAUTÉ]⁵ prend acte que ses services administratifs détiennent et utilisent un grand nombre de renseignements personnels et confidentiels;

Le Conseil de [COMMUNAUTÉ] reconnaît que les personnes qui acceptent de fournir leurs données personnelles à des fins administratives ont le droit de voir l'utilisation de celles-ci limitée aux seules fins pour lesquelles elles ont été recueillies et que l'information détenue par ses services administratifs doit être protégée;

Le Conseil de [COMMUNAUTÉ] prend acte du fait que divers systèmes de gestion de l'information sont ou seront implantés en collaboration avec les commissions et les organisations régionales (COR) des Premières Nations ainsi que d'autres partenaires;

Le Conseil de [COMMUNAUTÉ] prend acte que le droit à la protection des renseignements personnels et confidentiels détenus dans les services administratifs relevant d'un conseil de bande et des organisations des Premières Nations repose sur une base législative imprécise;

Le Conseil de [COMMUNAUTÉ] déclare qu'il a le droit, la volonté ainsi que la capacité de mettre en place ses propres mécanismes administratifs en matière de protection des renseignements personnels et d'accès à l'information dans l'organisation qu'il gère et sur le territoire qu'il administre;

Le Conseil adopte [ce Règlement/cette Politique/ Loi]⁶ pour répondre aux besoins de la population en matière de protection des renseignements personnels et d'accès à l'information, tel qu'il est exprimé dans la résolution n° 02/2011 adoptée le 27 janvier 2011 par l'assemblée des chefs des Premières Nations du Québec et du Labrador (APNQL);

Le Conseil adopte également [ce Règlement/cette Politique/Loi] pour tenir compte des préoccupations de [COMMUNAUTÉ] en ce qui a trait à la protection de ses données collectives et de son information confidentielle. Ces préoccupations ont notamment été soulevées dans la résolution n° 03/2011, adoptée par les chefs de l'APNQL le même jour;

[Ce Règlement/cette Politique/Loi] vise le Conseil de bande et les services administratifs qui en relèvent et s'applique sur l'ensemble du territoire de [COMMUNAUTÉ].

⁴ Conseil de bande ou Conseil d'administration.

⁵ Insérez le nom de votre communauté ou le nom de votre organisation. Si la politique s'applique à une organisation, il faut l'adapter.

⁶ Il revient à la communauté ou à l'organisation de choisir la forme que prendra le document.

Chapitre 1 - Interprétation et définitions

Dans [ce Règlement/cette Politique/ Loi], les articles qui présentent des exigences sont formulés à l'aide de termes tels que « doit » et « devra », tandis que les conseils, les lignes directrices et les exemples de pratiques recommandées sont présentés par l'utilisation de termes tels que « peut », « pourra » et « devrait ».

L'utilisation de la forme masculine inclut le féminin.

Signification des termes et des expressions utilisés dans [ce Règlement/cette Politique/Loi] :

- « **[COMMUNAUTÉ]** » : englobe toutes les entités de [COMMUNAUTÉ], y compris le Conseil, les services et l'administration générale.
- « **Conseil** » : entité composée de personnes élues aux fins de la gouvernance de [COMMUNAUTÉ], selon les règles en vigueur au sein de celle-ci.
- « **Directeur** » : personne nommée comme responsable d'un service (administration générale, éducation, santé, services sociaux, police, logement, etc., du gouvernement de [COMMUNAUTÉ] ou un directeur d'une entité (telle qu'une corporation de développement économique appartenant à la communauté) qui relève du gouvernement de [COMMUNAUTÉ]. Comprend également toute autre personne autorisée par [COMMUNAUTÉ].
- « **Données collectives** » : ensemble de données détenues par [COMMUNAUTÉ], tel qu'il est défini à l'article 15;
- « **Employé** » : toute personne qui agit pour [COMMUNAUTÉ] ou les organismes qui relèvent de [COMMUNAUTÉ], peu importe son statut à titre d'employé permanent ou à durée déterminée ou de bénévole.
- « **Individu** » : toute personne au sujet de laquelle [COMMUNAUTÉ] recueille des renseignements personnels.
- « **Information confidentielle** » : renseignements détenus par [COMMUNAUTÉ] que [COMMUNAUTÉ] souhaite garder confidentiels, comme décrit plus amplement à l'article 16;
- « **Principes PCAP** » : Les principes de propriété, de contrôle, d'accès et de possession cristallisent des thèmes que les Premières Nations du Canada préconisent depuis longtemps. Les principales notions véhiculées se rapportent à la propriété collective de l'information par un groupe, au contrôle de la recherche et de l'information par les Premières Nations, à la gestion par ces dernières de l'accès aux données et à la possession physique des données. Les principes PCAP sont plus amplement décrits à l'**Annexe B**.
- « **Renseignement personnel** » : tout renseignement concernant une personne physique et qui permet de l'identifier, à l'exclusion du nom et du titre d'un employé d'une organisation et de l'adresse et du numéro de téléphone de son lieu de travail;

[COMMUNAUTÉ]

Cadre de référence — [Loi/ Règlement/Politique] sur la protection des renseignements détenus par [COMMUNAUTÉ]

- « **Responsable** » : membre de la direction de [COMMUNAUTÉ] qui agit à titre de personne chargée de la protection des renseignements personnels, des données collectives et de l'information confidentielle pour [COMMUNAUTÉ].
- « **Service** » : toute composante (par exemple, l'administration générale, l'éducation, la santé, les services sociaux, la police, le logement, etc.) du gouvernement de [COMMUNAUTÉ] ou toute entité (telle qu'une corporation de développement économique) qui relève du gouvernement de [COMMUNAUTÉ].
- « **Système** » : groupes d'éléments et d'appareils électroniques qui sont utilisés à des fins de collecte, d'utilisation, de traitement, d'entreposage ou de transmission de renseignements personnels. Cela comprend les systèmes de communication et de gestion des renseignements et leurs composantes, dont les services d'accès à l'Internet, à l'Intranet, aux courriels, de même que les systèmes téléphoniques et les appareils électroniques portatifs d'entreposage et de communication.

Chapitre 2

Dispositions générales

1. Autorité relative à l'adoption de [ce Règlement/cette Politique/ Loi]

[Ce Règlement/cette Politique/ Loi] est adopté(e) au moyen de [RÉSOLUTION, RÉFÉRENDUM, ETC.], conformément aux règles en vigueur au sein de [COMMUNAUTÉ].

2. Entrée en vigueur de [ce Règlement/cette Politique/Loi]

[Ce Règlement/cette Politique/Loi] entre en vigueur le [DATE]. [Il/elle] s'applique à tous les renseignements personnels, aux données collectives et à l'information confidentielle qui sont en possession du Conseil ainsi que des services et des organismes qui relèvent du Conseil au moment de l'entrée en vigueur de [ce Règlement/cette Politique/Loi], peu importe la date de leur collecte par [COMMUNAUTÉ].

3. Principes directeurs

[Ce Règlement/cette Politique/Loi] respecte les principes directeurs suivants :

- Les Premières Nations ont le droit de bénéficier d'une protection de leurs renseignements qui est au moins comparable à celle dont bénéficient tous les Canadiens;
- Les règles de protection des renseignements personnels et des données collectives doivent être appliquées dans le respect des principes PCAP reconnus par les Premières Nations;
- Toute Première Nation est investie du pouvoir inhérent de décider des règles de protection des renseignements personnels et des données collectives sur son territoire;
- En tant que gouvernement autonome, le Conseil peut exercer ses pouvoirs inhérents sur le territoire de la communauté par l'entremise d'une politique, d'un règlement ou d'une loi;
- Les règles de protection des renseignements personnels et des données collectives doivent être appliquées dans le respect des conventions internationales, notamment : la *Déclaration universelle des droits de l'homme*; le *Pacte international relatif aux droits civils et politiques*; la *Déclaration des Nations Unies sur les droits des peuples autochtones*; et la *Déclaration américaine des droits et devoirs de l'Homme*.

4. Objet

Dans l'esprit des principes directeurs énumérés ci-dessus et conformément aux principes de responsabilisation et de transparence à l'égard des renseignements personnels et des données collectives qui relèvent de [COMMUNAUTÉ], ce [Règlement/cette Politique/Loi] a pour but de les protéger, et plus précisément :

[COMMUNAUTÉ]

Cadre de référence — [Loi/ Règlement/Politique] sur la protection des renseignements détenus par [COMMUNAUTÉ]

- a) d'édicter les règles et les exigences en matière de collecte, d'usage, de protection, de communication, de partage, de conservation et de disposition des renseignements personnels et des données collectives;
- b) d'accorder aux individus le droit de demander l'accès à leurs propres renseignements et de demander la correction desdits renseignements;
- c) de clarifier et rendre publics les devoirs et les droits des gestionnaires, des directeurs, des intervenants, du personnel et des individus en matière de protection des renseignements personnels et des données collectives;

5. Application

[Ce Règlement/cette Politique/Loi] s'applique à toutes les composantes de [COMMUNAUTÉ] ainsi qu'à toutes les entités sous son contrôle, à ses employés et aux membres du Conseil, y compris le chef.

6. Modification à [ce Règlement/cette Politique/Loi]

Le Conseil peut, à sa discrétion, modifier [ce Règlement/cette Politique/Loi] et préciser la date à laquelle la modification entre en vigueur.

7. Infractions

Toute infraction envers [le présent Règlement/la présente Politique/Loi] peut entraîner des sanctions allant jusqu'au congédiement ainsi qu'à des recours judiciaires.

8. Responsable, plainte et révision

- a) [COMMUNAUTÉ] nomme une personne qui est membre de la direction pour être le responsable de la protection des renseignements personnels ainsi que de l'information confidentielle et des données collectives;
- b) Tout individu peut porter plainte au responsable relativement à toute infraction réelle ou présumée à l'égard [du présent Règlement/de la présente Politique/Loi];
- c) À la réception d'une plainte déposée en vertu du paragraphe 8(a), le responsable mènera une enquête et prendra les mesures visant à rectifier la situation y compris, le cas échéant, les sanctions prévues à l'article 7;

- d) Au besoin, le responsable peut faire appel au conseiller juridique de la communauté ou à la personne responsable de la protection des renseignements personnels de la CSSSSPNQL pour échanger à ce sujet ou discuter d'une situation précise.

Chapitre 3

Règles en matière de collecte et de protection des renseignements personnels

9. Collecte de renseignements personnels

9.1 Collecte en lien avec la mission de [COMMUNAUTÉ]

De manière générale, la collecte de renseignements personnels par [COMMUNAUTÉ] est limitée aux seuls renseignements qui ont un lien direct avec la mission de [COMMUNAUTÉ] et qui sont nécessaires à la poursuite de ses activités. La mission de [COMMUNAUTÉ] est d'agir comme gouvernement élu de [COMMUNAUTÉ], dans le meilleur intérêt de tous ses membres, et en particulier : [CHAQUE COMMUNAUTÉ PEUT MODIFIER, AU BESOIN].

- a) D'assurer le bien-être général de la population en lui fournissant des services dans les domaines suivants : développement socio-économique, santé et services sociaux, éducation et culture, habitation, immobilisations et infrastructures, police, gestion du territoire, etc., et;
- b) De défendre et de promouvoir les droits collectifs de ses membres [COMMUNAUTÉ PEUT COMPLÉTER EN AJOUTANT, PAR EXEMPLE : ...inscrits sur le registre de bande / peu importe leur lieu de résidence (OU LES DEUX)].

9.2 Collecte auprès de l'individu

À moins d'être obtenus de tiers en vertu de l'article 9.3, les renseignements personnels recueillis par [COMMUNAUTÉ] doivent provenir directement de l'individu qui est visé par lesdits renseignements, en obtenant son consentement éclairé implicite ou explicite, par écrit ou autrement.

Le Conseil ou un service qui procède à la collecte de renseignements personnels doit, chaque fois que cela est possible, fournir les renseignements suivants à l'individu :

- a) Les fins de la cueillette;
- b) Les tiers à qui les renseignements personnels pourraient être communiqués;
- c) Le titre, l'adresse d'affaires et le numéro de téléphone du responsable.

9.3 Collecte auprès de tiers

Le consentement éclairé de l'individu concerné doit être obtenu, par écrit ou autrement, avant d'obtenir des renseignements personnels auprès de tiers. Toutefois, [COMMUNAUTÉ] peut obtenir des renseignements personnels auprès de tiers, sans le consentement de l'individu concerné dans les cas suivants :

- a) La collecte est expressément autorisée par une loi ou un règlement du Canada ou du Québec ou un règlement ou une résolution de [COMMUNAUTÉ];
- b) La collecte est nécessaire aux fins de prestation de services;
- c) La collecte est dans le meilleur intérêt de l'individu, et son consentement ne peut être obtenu en temps opportun ou pourrait poser un risque pour sa santé physique ou mentale;
- d) Les renseignements sont recueillis aux fins d'une enquête liée à une contravention d'une loi ou d'un règlement de [COMMUNAUTÉ], du Canada ou du Québec.

10. Exactitude et conservation des renseignements personnels

- a) [COMMUNAUTÉ] doit prendre toutes les mesures raisonnables afin de s'assurer que les renseignements personnels qu'elle compte utiliser au sujet d'un individu sont aussi complets, à jour et exacts que possible;
- b) [COMMUNAUTÉ] doit conserver les renseignements personnels pour au moins une année après leur dernière utilisation afin de permettre à l'individu d'y avoir accès. Une fois la période de conservation initiale d'un an écoulée, [COMMUNAUTÉ] doit effacer ou détruire les renseignements personnels dès qu'il s'avère que ceux-ci ne sont plus nécessaires aux fins pour lesquelles ils ont été recueillis et qu'aucune disposition légale n'en exige la conservation pour une période prolongée. Cela dit, la destruction doit être effectuée de manière sécuritaire et dans le respect des règles légales ou autres qui sont applicables (par exemple, celles de la *Loi sur l'impôt*, tel qu'il est exigé par les ententes de contribution financière signées avec les organismes gouvernementaux);
- c) Les renseignements personnels peuvent être effacés ou détruits à l'intérieur de la période d'un an dans les cas suivants :
 - i. L'individu a consenti par écrit à leur conservation pour une période plus courte; ou
 - ii. La conservation des renseignements pour une période plus courte est régie par un règlement ou une politique de [COMMUNAUTÉ], par une loi ou un règlement du Canada ou du Québec, ou est ordonnée par une cour ou un autre organisme habilité par la loi à émettre une telle ordonnance.
- d) Les renseignements personnels doivent être conservés pour une période plus longue lorsqu'une loi ou un règlement du Canada ou du Québec impose l'obligation de les conserver plus d'un an. Certains professionnels sont tenus de conserver les dossiers de leurs patients pour une durée pouvant aller jusqu'à sept (7) ans. Si [Communauté] a conclu des ententes, par exemple, en matière de santé et de protection de la jeunesse, les lois applicables dans ces domaines indiquent des règles précises en matière de conservation de documents. À cette fin, [COMMUNAUTÉ] élabore un calendrier de conservation dans lequel les périodes d'utilisation et les supports de conservation de ses documents sont déterminés.

11. Usage et communication des renseignements personnels

11.1 Usage et usage compatible

- a) De façon générale, [COMMUNAUTÉ] utilise des renseignements personnels aux fins de sa mission décrite plus haut à l'article 9.
- b) Bien entendu, la prestation de chaque service s'appuie sur différents types de renseignements personnels. Chaque Service utilise les renseignements personnels aux mêmes fins pour lesquelles ils ont été recueillis avec le consentement des individus concernés.
- c) Un service peut aussi utiliser un renseignement personnel pour un autre usage, mais il doit être compatible avec les fins pour lesquelles il a été recueilli, compte tenu de la nature des services qu'il vise à soutenir. Un usage compatible est un usage secondaire directement et logiquement rattaché à l'usage initial des renseignements. Évidemment, l'usage compatible doit toujours être raisonnable, compte tenu des circonstances et des attentes de l'individu qui en fait l'objet.

À titre d'exemple, si un numéro de téléphone à domicile a été recueilli pour les visites d'une infirmière, utiliser ce même numéro pour la visite d'une travailleuse sociale serait un usage compatible. La communication, par un professeur ou par le directeur d'école, de renseignements personnels au sujet d'un étudiant afin de lui fournir des services d'orientation constitue un autre exemple d'usage compatible. Cependant, l'utilisation de renseignements relatifs à l'absentéisme d'un employé afin de déterminer si cet employé se qualifie pour un autre poste ne peut être associée à la notion d'usage compatible, tout comme la transmission de l'identité des locataires d'habitation subventionnées au service local de police.

11.2 Limite de l'usage aux seules personnes concernées

Un renseignement personnel ne peut être transmis qu'aux employés ainsi qu'aux membres du Conseil qui en ont besoin pour l'exercice de leurs fonctions. De plus, les employés liés par le Code des professions, notamment les infirmiers et infirmières auxiliaires, les travailleurs sociaux, les avocats, les comptables et les conseillers d'orientation sont obligés de respecter le secret professionnel.

Le titre, le statut et le rang d'un employé, gestionnaire ou membre élu du Conseil ne constituent nullement en soi une raison acceptable pour que ces personnes puissent avoir accès aux renseignements personnels d'un individu. Toute pression ou menace de la part d'un employé, gestionnaire ou membre élu doit être portée à l'attention du responsable qui prendra les mesures nécessaires, telles que décrites aux articles 7 et 8.

Cependant, il serait parfaitement acceptable pour un membre élu du Conseil d'avoir accès aux renseignements personnels pertinents d'un membre de la communauté lorsque ce membre a fait appel à ses services afin de résoudre un problème administratif avec un Service.

11.3 Usage entre Services

Un Service peut transférer un renseignement personnel à un autre Service s'il en est fait le même usage que prévu initialement ou un usage compatible. Toutefois, si le transfert est fait pour un usage non compatible, un nouveau consentement devra être obtenu.

À titre d'exemple, certains renseignements médicaux pourraient, dans certains cas (maladie mentale, tendances suicidaires d'un individu, etc.), devoir être partagés avec le Service des affaires sociales. Ces mêmes renseignements ne pourraient cependant pas être partagés sans le consentement de l'individu avec la direction générale si, par exemple, la personne postule pour un emploi.

11.4 Autres usages et communication à des tiers

[COMMUNAUTÉ] ne peut pas utiliser les renseignements personnels à des fins autres que celles décrites ci-dessus à l'article 11.1, à moins : d'avoir obtenu un nouveau consentement de l'individu concerné; que l'usage ou la communication à une autre entité soit visé par l'article 11.5 ci-dessous; ou que l'usage ou la communication soit visés par l'une des exceptions suivantes :

- a) Lorsqu'il en est autrement prévu par un règlement ou une résolution de [COMMUNAUTÉ], par une loi ou un règlement du Canada ou du Québec;
- b) Lorsqu'ils sont requis par un mandataire de [COMMUNAUTÉ] qui a un absolu besoin des renseignements personnels aux fins pour lesquelles ceux-ci ont été recueillis ou pour un usage compatible, dans la poursuite de ses activités légitimes au nom de [COMMUNAUTÉ], pourvu qu'il s'engage par écrit à utiliser ces renseignements aux seules fins nécessaires et à garder l'information recueillie confidentielle;
- c) Lorsque l'usage est nécessaire aux fins de la prestation de services;
- d) Lorsqu'ils permettent de déterminer l'admissibilité de l'individu à des prestations ou à des programmes;
- e) Lorsqu'ils sont requis par des vérificateurs internes et externes ou par un avocat dont les services ont été retenus par le Conseil;
- f) Lorsqu'ils sont requis dans une enquête liée à la contravention d'une résolution ou d'un règlement de [COMMUNAUTÉ], ou d'une loi ou d'un règlement du Canada ou du Québec;
- g) Lorsqu'ils font l'objet de l'ordonnance d'une cour ou d'un organisme judiciaire ou quasi judiciaire;
- h) Lorsque les renseignements sont déjà connus du public, dans la mesure où la communication des renseignements ne risquerait pas de révéler de nouveaux faits ou renseignements qui ne sont pas connus du public;
- i) Lorsque, de l'avis du directeur ou du responsable, l'usage des renseignements ou leur communication se fait dans l'intérêt supérieur de l'individu et que son consentement ne peut être raisonnablement obtenu;

- j) Lorsque, de l'avis du directeur ou du responsable, l'usage des renseignements ou leur communication est nécessaire afin de protéger la vie, la sécurité ou la santé physique ou mentale de l'individu ou d'une autre personne;
- k) Lorsque l'utilisation ou la communication se fait en vue de la reconnaissance des droits ancestraux de [COMMUNAUTÉ] ou du règlement de ses réclamations, et dans la mesure où :
 - i. l'usage ou les recoupements à être effectués dans le cadre de la recherche ne seront pas susceptibles de causer un tort aux individus; et
 - ii. les avantages qui découleront du recoupement serviront clairement l'intérêt public ou serviront à appuyer les réclamations de [COMMUNAUTÉ].

11.5 Communication à des fins de recherche

Un service peut divulguer des renseignements personnels aux fins de recherche sans l'autorisation des personnes visées, dans la seule mesure où :

- a) L'objet de la recherche ne pourrait être atteint sans divulguer les renseignements en question;
- b) Il n'est pas raisonnablement possible d'obtenir le consentement des individus visés par les renseignements;
- c) Le directeur a obtenu un engagement écrit de la part du destinataire des renseignements qui assure :
 - i. la confidentialité des renseignements personnels;
 - ii. la sécurité des renseignements personnels, le destinataire s'engageant aussi à informer dans les plus brefs délais le directeur de tout incident de sécurité qui affecte ou risque d'affecter les renseignements personnels;
 - iii. le retour ou la destruction des données qui permettent d'identifier les individus visés par les renseignements;
 - iv. l'interdiction de publication des résultats de la recherche sous une forme qui risquerait de révéler l'identité des individus visés par ceux-ci;

11.6 Pas de communication à des fins commerciales

Les renseignements personnels des individus ne seront jamais utilisés ni transférés à des fins commerciales. Si c'était le cas, le consentement explicite des personnes concernées serait demandé.

12. Renseignements personnels concernant les employés

12.1 Application de cet article aux employés de [COMMUNAUTÉ]

- a) Cet article s'applique aux renseignements personnels recueillis ou conservés par [COMMUNAUTÉ] au sujet de ses employés. Ces renseignements personnels sont régis par la Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch. 5). Les autres articles de cette loi peuvent être utilisés de façon supplétive à cet article s'ils ne sont pas contradictoires avec celui-ci.
- b) Dans le cas où les employés de [COMMUNAUTÉ] sont issus de [COMMUNAUTÉ], leurs renseignements personnels seront aussi recueillis dans le cadre de leur relation avec [COMMUNAUTÉ] en tant que gouvernement des Premières Nations. Dans ce cas, ils sont régis par le reste de cette politique.
- c) [COMMUNAUTÉ] traite les renseignements personnels de ses employés recueillis dans le cadre de leur emploi, séparément de ceux recueillis dans le cadre de son rôle de gouvernement des Premières Nations. Par exemple, [COMMUNAUTÉ] connaît le salaire de ses employés. Elle n'utilisera pas cette information pour évaluer si un individu est éligible à un programme. L'information sera obtenue à nouveau auprès de l'individu, avec son consentement.

12.2 Collecte et utilisation des renseignements personnels

- a) Tout employé doit être informé de toute collecte, utilisation ou communication de renseignements personnels qui le concernent et y consentir, à moins que ce ne soit pas approprié (par exemple, si la collecte vise une recherche de fraude).
- b) [COMMUNAUTÉ] recueille et utilise les renseignements personnels de ses employés dans le but de gérer la relation de travail avec eux : notamment, l'embauche des employés, la paie, la retraite, les avantages, la gestion et la protection des biens de [COMMUNAUTÉ], les évaluations de rendement, les demandes de prestations et le respect des politiques et règlements de [COMMUNAUTÉ] ainsi que des lois applicables.
- c) [COMMUNAUTÉ] n'utilisera pas les renseignements personnels à d'autres fins, à moins que cela ne soit permis par la loi, qu'elle ait obtenu le consentement de l'employé ou que l'employé s'attende raisonnablement à ce que cette nouvelle utilisation soit faite. À titre d'exemple, la loi permet que les renseignements personnels soient utilisés sans consentement pour répondre à une situation d'urgence mettant en danger la vie, la santé ou la sécurité d'un individu.
- d) Les renseignements recueillis peuvent inclure, par exemple, l'adresse personnelle d'un employé, sa date de naissance, son salaire, son état de santé, son évaluation de rendement, des informations relatives à ses retards ou son taux d'absentéisme, tout avis concernant des mesures disciplinaires ainsi que des informations enregistrées sur l'ordinateur utilisé par l'employé, ses communications électroniques ou son utilisation d'Internet.

12.3 Communication des renseignements personnels

[COMMUNAUTÉ] ne transmet pas de renseignements personnels reçus de ses employés dans le cadre de la relation de travail à des tiers, sauf si cela est requis pour l'administration de la relation de travail (tel qu'au gouvernement aux fins des déductions de l'employé), si c'est permis par la loi ou si le consentement préalable de l'employé a été obtenu.

À titre d'exemple, la loi permet notamment que les renseignements personnels soient utilisés sans consentement si la communication est faite à un avocat qui représente l'organisation, en vue du recouvrement d'une créance, à une institution gouvernementale pour l'application de la loi ou dans une situation d'urgence mettant en danger la vie, la sécurité ou la santé d'une personne.

12.4 Responsable, droits d'accès et sécurité

- a) Le responsable doit répondre à toute question ou plainte relative aux dossiers personnels des employés et à la protection des renseignements personnels des employés. Tout changement d'adresse personnelle, de numéro de téléphone, d'état matrimonial, de personne(s) à charge, de bénéficiaire ou de personne(s) à prévenir en cas d'urgence devrait être porté à son attention dès que possible.
- b) Les droits d'accès et de correction de l'article 13 ainsi que les mesures de sécurité de l'article 19 ci-dessous s'appliquent aux renseignements personnels recueillis dans le cadre de la relation de travail, avec les adaptations nécessaires.

13. Droit d'accès et de correction

- a) Un individu a le droit de demander l'accès à ses propres renseignements qui se trouvent en possession du Conseil ou d'un Service, sous réserve de l'article 14.
- b) [COMMUNAUTÉ] peut exiger des frais raisonnables de la part du demandeur afin de couvrir ses propres coûts liés à la recherche et la reproduction des documents renfermant ses renseignements personnels. En aucun cas [COMMUNAUTÉ] ne pourra exiger un montant de frais supérieurs à ce qui lui en coûte réellement pour traiter la demande d'accès.
- c) Un individu a le droit de demander la correction de ses renseignements personnels qui se trouvent en possession de [COMMUNAUTÉ], et ce, sans frais.
- d) L'individu devra être informé dans les trente jours suivant la réception de sa demande écrite d'accès ou de correction si celle-ci a été acceptée ou non. Le cas échéant, la lettre de réponse devra en outre préciser de manière explicite la raison pour laquelle l'accès ou les corrections demandées ne seront pas effectués.
- e) Un délai additionnel de trente jours pourra être accordé, si justifié, et l'individu devra être informé de tout délai supplémentaire dans le traitement de sa demande d'accès ou de correction.

14. Exceptions au droit d'accès

Il peut être refusé à un individu l'accès à ses propres renseignements dans les circonstances suivantes :

- a) L'accès serait susceptible de mettre en danger la vie, la sécurité ou la santé de l'individu ou d'une autre personne;
- b) L'accès serait susceptible d'entraver les activités visant à faire respecter les lois ou de nuire à une enquête;
- c) L'accès est interdit par une loi du Canada ou du Québec, ou par l'ordonnance d'une cour ou d'un organisme quasi judiciaire;
- d) Les renseignements sont visés par le secret professionnel qui lie un avocat à son client;

- e) Les renseignements ont été obtenus de manière confidentielle d'un autre gouvernement, y compris le gouvernement d'une autre communauté des Premières Nations, ou d'un de ses organismes;
- f) Les renseignements contiennent des renseignements personnels d'un tiers qui refuse d'y donner accès et les renseignements ne peuvent être séparés de ceux-ci;
- g) Les renseignements font partie des délibérations à huis clos du Conseil ou de ses membres dans l'exercice de leurs fonctions de conseillers.

Les exceptions ci-dessus énumérées ne s'appliquent pas dans les cas où l'accès d'un individu à ses propres renseignements peut avoir pour effet de protéger sa vie, sa sécurité ou sa santé ou celles d'une autre personne.

Chapitre 5 – Protection des données collectives et de l'information confidentielle

15. Données collectives

En plus des renseignements personnels, [COMMUNAUTÉ] a en sa possession d'autres informations qu'elle veut protéger, notamment pour faire respecter les principes PCAP.

[COMMUNAUTÉ] détient des ensembles de données, nominales et dénominisées, créées à partir de renseignements personnels des membres de [COMMUNAUTÉ], particulièrement en matière de santé, de services sociaux et d'éducation. Ces données sont appelées des « données collectives ».

Par ailleurs, [COMMUNAUTÉ] possède des données relatives à l'utilisation et aux caractéristiques du territoire de [COMMUNAUTÉ], par exemple, concernant le sol, le sous-sol, les éléments naturels, la faune et la flore; ces données sont également considérées comme des « données collectives ».

Fait aussi partie des « données collectives » le savoir traditionnel détenu par [COMMUNAUTÉ]. Il peut se présenter sous différentes formes (compilations de données, études, livres, enregistrements musicaux ou vidéo...).

Les données collectives sont protégées, quelle que soit leur forme de support, matériel, électronique ou autre. Elles sont considérées comme de l'information confidentielle à moins que [COMMUNAUTÉ] n'ait décidé de les rendre publiques.

16. Information confidentielle

[COMMUNAUTÉ] détient des renseignements, sous forme orale, écrite ou autre, qui ne sont généralement pas facilement accessibles et pour lesquels [COMMUNAUTÉ] prend des mesures pour les garder secrets. Ils sont appelés « information confidentielle ». Ces renseignements peuvent appartenir à [COMMUNAUTÉ], à des membres individuellement, à tous les membres de la [COMMUNAUTÉ] de façon collective, ou bien appartenir à des tiers.

Tel qu'énoncé à l'article 15, l'information confidentielle inclut les données collectives, dans la mesure où [COMMUNAUTÉ] n'a pas décidé de les rendre publiques.

Par ailleurs, l'information confidentielle peut aussi inclure :

- Les stratégies de négociations de [COMMUNAUTÉ] – avec d'autres gouvernements (fédéral, provincial, municipal) ou avec des contractuels, des syndicats, des individus ou des entreprises;

- Les renseignements relatifs aux procès-verbaux, aux comptes-rendus et aux propos tenus lors de réunions, de négociations ou dans le cadre des activités de [COMMUNAUTÉ];
- Les renseignements obtenus à titre confidentiel d'autres gouvernements;
- Les renseignements relatifs à l'application de la loi, aux enquêtes ou aux vérifications, incluant les techniques et stratégies visant à mener de telles activités;
- Les renseignements dont la divulgation serait susceptible de compromettre la sécurité d'un individu ou de la communauté;
- Les renseignements visés par le secret professionnel qui lie un avocat à son client;
- Les renseignements relatifs aux avis, recommandations et analyses obtenus ou produits dans le cadre des activités de [COMMUNAUTÉ];
- Les renseignements relatifs aux affaires de nature budgétaire, financière et administrative;
- Les renseignements dont la divulgation est interdite par une entente signée entre [COMMUNAUTÉ] et une autre partie – un autre gouvernement (fédéral, provincial, municipal), un individu ou une entreprise;
- Certains renseignements portant sur la protection des infrastructures – édifices, systèmes informatiques, etc., de [COMMUNAUTÉ].

17. Mesures de protection générales

Afin de protéger ses données collectives et son information confidentielle, [COMMUNAUTÉ] s'assure de :

- a) Limiter leur divulgation aux personnes qui en ont légitimement besoin dans l'exercice de leur fonction;
- b) Former ses employés concernant les mesures à prendre pour protéger l'information (protéger les documents écrits et informatiques, obtenir l'autorisation du directeur ou du responsable avant de transmettre des données collectives et de l'information confidentielle, éviter de discuter ou de traiter de l'information confidentielle dans un lieu public, ne pas divulguer d'information confidentielle de [COMMUNAUTÉ] à la suite d'une fin d'emploi...);
- c) Appliquer les mesures de sécurité de l'article 19 avec les modifications nécessaires aux données collectives et à l'information confidentielle.

Il est entendu que ces mesures ne s'appliqueront pas aux données collectives que la [COMMUNAUTÉ] a décidé de rendre publiques.

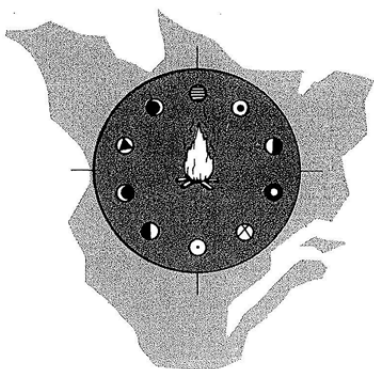
18. Accès d'un tiers

- a) Si un tiers souhaite avoir accès aux données collectives ou à l'information confidentielle, [COMMUNAUTÉ] s'assure d'appliquer les principes PCAP.
- b) [COMMUNAUTÉ] s'assurera notamment que le tiers demandant à avoir accès aux données collectives non rendues publiques ou à l'information confidentielle apporte une justification législative ou contractuelle à cette exigence ou que l'accès est dans l'intérêt de [COMMUNAUTÉ], par exemple, dans le cas d'une entente de contribution ou d'une loi fiscale.
- c) [COMMUNAUTÉ] s'assurera du respect des principes ci-dessous et, si possible, fera signer au tiers une entente de confidentialité et/ou d'utilisation des données qui :
- décrit clairement l'utilisation permise au tiers et indique que toute autre utilisation nécessite un consentement additionnel de [COMMUNAUTÉ];
 - indique quel est l'intérêt pour [COMMUNAUTÉ] de permettre l'utilisation de ses données;
 - interdit la divulgation de ses données publiquement et la transmission à des tiers;
 - exige une reddition de comptes concernant les résultats de l'utilisation des données et le respect de l'entente.

19. Mesures de sécurité

Les renseignements personnels, l'information confidentielle et les données collectives qui relèvent de [COMMUNAUTÉ] doivent être adéquatement protégés contre la collecte, l'usage, la modification, l'accès et la destruction non autorisés. Cela signifie la mise sur pied d'un programme de sécurité qui se compose des éléments suivants :

- a) La nomination d'un **responsable de la sécurité** : qui est chargé de mettre en œuvre les mesures de sécurité raisonnables afin d'assurer la protection adéquate des renseignements contre l'accès, la modification, l'utilisation et la destruction non autorisés;
- b) **La sécurité matérielle** : qui comprend la mise en place de mesures de sécurité visant à contrôler ainsi qu'à limiter l'accès aux installations de chaque service – cadenas, portes, clôtures, etc.;
- c) **La sécurité des technologies de l'information** : qui comprend la mise en place de mesures visant à protéger les systèmes informatiques ainsi que les autres appareils électroniques (télécopieurs, téléphones et agendas portatifs, ordinateurs, serveurs et leurs périphériques, etc.) qui sont utilisés pour la collecte, le traitement, l'entreposage et la transmission des renseignements personnels et non personnels de nature délicate;
- d) **La sécurité en matière de contrats** : qui vise à s'assurer que les tiers mandataires adhèrent scrupuleusement à toutes les exigences de [COMMUNAUTÉ] en matière de sécurité et de protection de la vie privée;
- e) **La sécurité en matière de personnel** : qui vise à s'assurer que les employés ainsi que les membres du Conseil adhèrent scrupuleusement à toutes les exigences de [COMMUNAUTÉ] en matière de sécurité et de protection de la vie privée. Les employés doivent respecter la présente politique;
- f) **La conduite d'évaluations de la menace et des risques ainsi que de vérifications et d'enquêtes** : qui vise l'identification, sur une base régulière, des situations qui pourraient affecter la confidentialité, l'intégrité, la disponibilité ainsi que la valeur stratégique des renseignements et la réaction efficace aux incidents de sécurité;
- g) **L'élaboration de plans de mesures d'urgence et de continuité des opérations** : qui vise à assurer la prestation en continu des services aux membres de la communauté ainsi que des renseignements qui sont essentiels à ces activités.



Secrétariat
de l'Assemblée des
Premières Nations
du Québec
et du Labrador

Secretariat of the
Assembly of the
First Nations
of Quebec
and Labrador

250, Place Chef Michel Laveau, bur. 201, Wendake, QC G0A 4V0
Tél. : (418) 842-5020 / 842-5274 Téléc. : (418) 842-2660

RÉSOLUTION NO 07/2012

CADRE DE RÉFÉRENCE EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS DÉTENUS PAR UNE COMMUNAUTÉ OU UNE ORGANISATION PREMIÈRE NATION DU QUÉBEC

ATTENDU QUE les services administratifs relevant des gouvernements de Première Nation et des organisations des Premières Nations détiennent et utilisent un grand nombre de renseignements personnels;

ATTENDU QUE les personnes qui acceptent de fournir leurs données personnelles à des fins administratives ont le droit de voir l'utilisation de celles-ci limitées aux seules fins pour lesquelles elles ont été recueillies;

ATTENDU QUE les gouvernements de Première Nation et les commissions et organisations régionales implantent actuellement ou implanteront divers systèmes de gestion de l'information;

ATTENDU QUE les informations détenues par les gouvernements de Première Nation, les intervenants et les citoyens doivent être protégées;

ATTENDU QUE les avis juridiques produits à la demande de la CSSSPNQL révèlent que le droit à la protection des renseignements détenus dans les services administratifs relevant des gouvernements de Première Nation et des organisations des Premières Nations repose sur une base législative imprécise;

ATTENDU QUE les Premières Nations du Québec et du Labrador ont le droit, la volonté politique ainsi que la capacité de mettre en place leurs propres mécanismes administratifs en matière de protection des renseignements personnels et d'accès à l'information;

LE GRAND CERCLE DE NOS PREMIÈRES NATIONS — THE GREAT CIRCLE OF OUR FIRST NATIONS

[COMMUNAUTÉ]

Cadre de référence — [Loi/ Règlement/Politique] sur la protection des renseignements détenus par [COMMUNAUTÉ]

ATTENDU QUE l'Assemblée des Premières Nations du Québec et du Labrador a adopté le 27 janvier 2011, la résolution 02/2011 appuyant la création d'un comité visant l'analyse de possibilités entourant l'élaboration d'une loi ou d'une politique en matière de protection des renseignements personnels et d'accès à l'information à l'intention des communautés et des organisations des Premières Nations du Québec;

ATTENDU QUE le 14 juin 2011, ce comité a déposé un rapport préliminaire des options à l'Assemblée des Chefs des Premières Nations du Québec et du Labrador et que celle-ci a approuvé la poursuite des travaux;

ATTENDU QUE les travaux du comité ont mené à l'élaboration d'un cadre de référence en matière de protection des renseignements détenus par une communauté ou une organisation des Premières Nations du Québec;

ATTENDU QUE le cadre de référence proposé peut être adopté tel quel par toute communauté qui le désire sous la forme d'une loi, d'un règlement ou d'une politique ou, le cas échéant, être adopté par toute organisation sous la forme d'un règlement interne ou d'une politique;

ATTENDU QUE le cadre de référence proposé est un moyen conçu spécifiquement pour soutenir les communautés et les organisations qui doivent mettre en place des règles appropriées pour protéger les renseignements personnels, les données collectives et autres informations confidentielles qu'elles détiennent,

IL EST RÉSOLU QUE l'Assemblée des Premières Nations du Québec et du Labrador adopte le cadre de référence sur la protection des renseignements détenus par une communauté ou une organisation Première Nation du Québec, afin de le proposer comme modèle aux gouvernements de Première Nation et aux organisations des Premières Nations du Québec;

IL EST RÉSOLU QUE l'Assemblée des Premières Nations du Québec et du Labrador appuie la CSSSPNQL dans le développement d'une formation et de documents d'information à l'intention des dirigeants et employés des communautés et organisations qui adopteront le cadre de référence.

PROPOSÉE PAR : Chef Terence McBride, Timiskaming

APPUYÉE PAR : Chef Raphaël Picard, Pessamit

ADOPTÉE PAR CONSENSUS À MONTRÉAL LE 12 JUIN 2012



Ghislain Picard
Chef de l'APNQL

Annexe B

LES PRINCIPES PCAP

Extrait du **Procotole de recherche des Premières Nations du Québec et du Labrador de l'APNQL (2005)**

Les principes PCAP projettent l'autodétermination à la recherche; c'est une réponse politique à une tendance coloniale tenace en matière de recherche et de gestion de l'information. Ils s'appliquent à la recherche, à la surveillance, aux enquêtes, aux statistiques, aux connaissances à caractère culturel, etc. D'une façon générale, ces principes visent tous les aspects de l'information, notamment sa création et sa gestion.

- **Propriété** : La notion de propriété se rapporte à la relation d'une communauté des Premières Nations avec les connaissances, les données et l'information relatives à sa culture. Ce principe veut qu'une communauté ou un groupe détienne collectivement la propriété de l'information de la même façon qu'une personne détient la propriété de son information personnelle. Cela diffère de la gouvernance. La gouvernance ou l'administration de données ou d'information par une institution qui doit rendre des comptes au groupe est un mécanisme au moyen duquel il devient possible de réaliser la propriété.
- **Contrôle** : Les aspirations et les droits des membres des Premières Nations concernant la reprise et le maintien du contrôle de tous les aspects de leur vie et de leurs institutions s'étendent à la recherche, à l'information et aux données. Le principe de contrôle veut que les membres des Premières Nations, leurs communautés et les groupes qui les représentent soient en droit de souhaiter obtenir le contrôle de tous les aspects du processus de gestion de la recherche et de l'information ayant des répercussions sur eux-mêmes. Le contrôle de la recherche par les Premières Nations peut inclure toutes les étapes d'un projet de recherche en particulier, de la conception à l'achèvement. Ce principe s'étend au contrôle des ressources et du processus d'examen, à la formulation des cadres conceptuels du travail, à la gestion des données, etc.
- **Accès** : Les membres des Premières Nations doivent avoir accès à l'information et aux données qui les concernent et qui concernent leurs communautés, peu importe l'endroit où l'on conserve ces données. Ce principe fait aussi référence aux droits des communautés et des organisations autochtones de gérer l'information qui les touche collectivement et de prendre des décisions en regard de l'accès à cette information. En pratique, on peut y parvenir au moyen de protocoles normalisés et officiels.
- **Possession** : Le terme propriété désigne en principe la relation entre un peuple et les données existantes à son sujet tandis que les termes possession ou gouvernance sont plus explicites. Bien que la possession ne soit pas une condition essentielle à la propriété (des données), elle constitue un mécanisme permettant d'affirmer et de protéger la propriété. Lorsqu'un parti possède des données appartenant à un autre parti, un risque de violation ou d'usage abusif existe. Cette situation mérite une vigilance attentive, particulièrement lorsque sévit un manque de confiance entre le propriétaire et le possesseur.

[COMMUNAUTÉ]

Cadre de référence — [Loi/ Règlement/Politique] sur la protection des renseignements détenus par [COMMUNAUTÉ]



www.csspnql.com