

Lignes directrices pour les dentistes du Nouveau-Brunswick

visant les renseignements personnels sur la santé



**New Brunswick
Dental Society**
**Société Dentaire du
Nouveau-Brunswick**

520 rue King Street, HSBC Place #820
P.O./C.P. Box 488, Station "A"
Fredericton, N.B. E3B 4Z9
Tél.: (506) 452-8575 Fax: (506) 452-1872

Juin 2015

TABLE DES MATIÈRES

Introduction	1
Objet de la Loi.....	2
Que sont les « renseignements personnels sur la santé »?	2
Collecte, utilisation et communication de renseignements personnels sur la santé	3
Si le patient veut voir ou corriger les renseignements à son dossier, que doit-on faire?	5
Quelles sont mes responsabilités?	6
Notification obligatoire des violations de la sécurité	8
Pour combien de temps dois-je garder mes dossiers?	9
Retraite et déménagement.....	10
Droits pour fournir une copie du dossier au patient	11
Annexe A – Coordonnées et ressources.....	12
Annexe B – Règle 7 : Dépositaire désigné des dossiers dentaires des patients	13
Annexe C – Liste de contrôle – Sécurité et protection de la vie privée	14
Annexe D – Liste de vérification pour la protection des renseignements personnels sur la santé au Nouveau-Brunswick.....	16

I. INTRODUCTION

Les dentistes du Nouveau-Brunswick sont des « dépositaires » de renseignements personnels sur la santé confidentiels et ils ont des obligations juridiques en vertu de la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé (la Loi).

La Société dentaire du Nouveau-Brunswick (SDNB) a préparé ces lignes directrices pour aider ses membres à comprendre leurs obligations de dépositaires et à assurer les meilleures pratiques pour :

- obtenir des renseignements personnels sur la santé;
- garder confidentiels les renseignements personnels sur la santé;
- détruire des renseignements personnels sur la santé;
- transférer des renseignements personnels sur la santé à d'autres dépositaires.

Ces lignes directrices visent à offrir des conseils avisés et pratiques aux cabinets dentaires et ne doivent pas servir à remplacer un avis juridique. Si vous avez des questions spécifiques concernant la Loi, vous devriez consulter un conseiller juridique approprié.






II. OBJET DE LA LOI

La Loi a vise de nombreux objectifs, y compris :

- d'établir des règles touchant la collecte, l'utilisation, la communication, la conservation et la destruction sécuritaire des renseignements personnels sur la santé;
- d'établir des mécanismes de responsabilisation des dépositaires ayant la garde ou la responsabilité de renseignements personnels sur la santé;
- de mettre en place des mesures permettant de protéger la sécurité et l'intégrité des renseignements personnels sur la santé;
- de donner aux personnes le droit de consulter et de recevoir une copie des renseignements personnels sur la santé qui les concernent;
- donner aux personnes le droit de demander que soit corrigés ou modifiés les renseignements personnels sur la santé qui les concernent (pour assurer l'exactitude et le caractère complet des renseignements);
- d'améliorer davantage le système de soins de santé.

III. QUE SONT LES « RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ »?

Les renseignements personnels sur la santé peuvent être oraux, écrits ou photographiés et s'appliquent à tout support d'information y compris le papier, le microfilm, la radiographie et les dossiers électroniques. Plus particulièrement, ils comprennent les renseignements suivants :

-  Nom;
-  Adresse;
-  Numéro de téléphone;
-  Adresse de courriel;
-  Date de naissance.

Les renseignements personnels sur la santé peuvent aussi inclure ce qui suit :

- État de santé physique et/ou mentale;
- Antécédents médicaux;
- Antécédents familiaux;
- Information génétique;
- Groupe sanguin;
- Fournisseurs de soins de santé;
- Mandataire spécial;
- Médicaments sur ordonnance;
- Aides, produits et programmes de soins de santé.

*** En ce qui concerne les cabinets dentaires, les renseignements personnels sur la santé incluront aussi l'information sur l'assurance dentaire, sur la carte de débit ou de crédit qui peut être obtenue aux fins de paiement.**

IV. COLLECTE, UTILISATION ET COMMUNICATION DE RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ

Voici trois principes bien établis qui guident la collecte, l'utilisation et la communication renseignements personnels sur la santé :

1: Consentement

Sauf disposition contraire de la loi, les dentistes doivent toujours obtenir le consentement du patient pour la collecte, l'utilisation et la communication de renseignements personnels sur la santé.

En termes simples, cela signifie que le patient doit comprendre :

- votre rôle et les services que vous allez fournir;
- quels renseignements personnels sont nécessaires pour vous permettre de faire votre travail et pourquoi;
- comment vous allez utiliser les renseignements personnels sur la santé;
- à qui seront communiqués les renseignements personnels sur la santé et pourquoi (comme la compagnie d'assurance pour une pré-détermination ou un paiement, ou un autre fournisseur de soins de santé).

2: Collecte seulement du nombre minimal de renseignements personnels sur la santé nécessaires

Il faut faire la collecte seulement du nombre minimal de renseignements nécessaires et prendre des mesures raisonnables pour s'assurer que les renseignements recueillis sont exacts, actuels et complets.

3: Utilisation et communication de renseignements personnels sur la santé selon le besoin de savoir

L'utilisation et la communication de renseignements personnels sur la santé se fait uniquement selon le besoin de savoir. Cela signifie que seulement les personnes (comme d'autres professionnels des soins de la santé ou de l'équipe de soins dentaires) qui ont besoin d'avoir accès aux renseignements personnels sur la santé pour faire leur travail devraient avoir accès à ces renseignements.

Exemple :

Les hygiénistes dentaires n'ont pas besoin d'avoir accès aux renseignements personnels de tous les patients du cabinet dentaire, mais seulement à ceux des patients à qui ils offrent des soins et un traitement, et uniquement l'information requise pour faire le traitement.

Exception - Communication sans le consentement

La communication de renseignements personnels sur la santé sans le consentement peut se faire seulement dans des cas précis et limités comme suit :

- pour protéger la santé mentale ou physique et la sécurité d'une personne, d'un groupe de personnes ou du public;
- dans une situation d'urgence;
- pour se conformer à une citation à comparaître, à un mandat, à une ordonnance du tribunal, etc.
- pour se conformer à la loi ou aux exigences de la loi;
- pour aviser un parent ou un être cher d'une blessure, d'une maladie ou d'une incapacité;
- pour fournir de l'information à la SDNB afin qu'elle puisse remplir son mandat.

REMARQUE :

Le dentiste doit garder par écrit toute l'information sur une telle communication de renseignements personnels sur la santé, y compris la date, la raison de la communication et à qui les renseignements personnels sur la santé ont été communiqués.



V. SI LE PATIENT VEUT VOIR OU CORRIGER LES RENSEIGNEMENTS À SON DOSSIER, QUE DOIT-ON FAIRE?

La Loi fournit le droit de consulter ses propres renseignements personnels sur la santé et de demander la correction de ces renseignements s'ils sont inexacts ou incomplets. Le droit de consulter son dossier ne s'applique pas seulement aux renseignements consignés au dossier par le dentiste, mais aussi aux documents électroniques, aux radiographies des dents, aux impressions, etc.

En vertu de la Loi, un patient peut demander :

1. de consulter son dossier en personne; ou
2. d'obtenir une copie de son dossier (mais pas l'original).

En vertu de la Loi et conformément aux règles de la SDNB, le dentiste a l'obligation :

- de répondre à cette demande dans un délai de 30 jours (peut être prolongé d'un autre 30 jours dans certaines circonstances);
- de s'assurer que le patient aura seulement accès à ses propres renseignements personnels sur la santé conformément à la Loi.

Il est recommandé que les dentistes affichent un avis sur la politique de conservation des dossiers. Voir la collecte et destruction des dossiers des patients à la Section VIII.

Le personnel du cabinet dentaire peut aider le patient à avoir accès à ses renseignements personnels ou à changer l'information en demandant au patient si le personnel a son consentement pour communiquer l'information à son conjoint ou parent. Une note placée dans le dossier à cet égard peut être confirmée de nouveau à des visites par la suite afin de s'assurer que rien n'a changé ou, s'il y a un changement, pour indiquer le nouveau consentement. Ce petit effort dans le travail quotidien peut s'avérer très efficace quand le personnel doit téléphoner à la maison du patient et laisser un message ou communiquer de l'information à un autre membre de la famille à propos du patient.

Refus de l'accès aux renseignements personnels sur la santé

Dans des circonstances extrêmement rares, il est possible de refuser la demande du patient de consulter ses renseignements personnels sur la santé, c'est-à-dire si :

- la communication des renseignements personnels sur la santé pose un risque pour la santé ou la sécurité de cette personne ou d'une autre personne;
- la communication permettrait d'identifier la personne qui a fourni les renseignements en toute confiance;
- la communication révélerait de l'information préparée pour une procédure judiciaire (secret professionnel entre l'avocat et son client); ou si
- **(situation fréquente en dentisterie) la communication de l'information peut révéler des renseignements personnels sur la santé d'une autre personne (à moins qu'il ne soit possible de l'enlever ou que le praticien ait donné son consentement exprès pour la divulgation de ces renseignements).**

VI. QUELLES SONT MES RESPONSABILITÉS?

Les dentistes ont l'obligation de protéger les renseignements sur la santé du patient afin d'assurer leur confidentialité, leur intégrité et leur disponibilité. Voici les trois grandes catégories de précautions applicables pour protéger l'information :



Les précautions physiques :

- 🔒 Veiller à la garde (l'entreposage) des dossiers dans un bâtiment physiquement sécuritaire.
- 🔒 Placer les écrans des ordinateurs et télécopieurs en dehors du champ de vision du public afin de prévenir l'accès à l'information par des personnes non autorisées (comme d'autres patients au comptoir de la réception).
- 🔒 Ne jamais placer des télécopieurs dans un endroit du bureau auquel des personnes non autorisées peuvent avoir accès.
- 🔒 Toujours verrouiller les classeurs (qui contiennent les dossiers des patients) et toute autre zone d'entreposage.
- 🔒 Adopter la politique de ne rien laisser traîner sur le bureau en fin de journée, car il ne faut jamais laisser sans surveillance des documents qui contiennent des renseignements personnels sur les patients.

Les précautions administratives :

- 🔒 Demander à vos employée de signer un serment de confidentialité au moment de l'embauche et passer ce serment en revue chaque année;
- 🔒 S'assurer que le personnel connaisse les politiques et procédures de protection de la vie privée du cabinet dentaire et qu'il a reçu la formation pour les suivre.
- 🔒 Les dentistes et le personnel doivent éviter de discuter des patients sur un cellulaire, dans un endroit public ou dans une zone à laquelle le public a accès (cafés, restaurants, corridors, ascenseurs, etc.).
- 🔒 Dire au personnel de ne pas parler de l'information dans les dossiers des patients surtout quand des renseignements personnels sont discutés.
- 🔒 Confirmer régulièrement les coordonnées des patients (surtout leur numéro de téléphone et leur adresse de courriel).
- 🔒 Chaque cabinet dentaire devrait nommer un membre du personnel comme responsable de maintenir les protocoles de protection de la vie privée dans le bureau. Chaque cabinet dentaire devrait nommer un membre du personnel comme responsable de maintenir les protocoles de protection de la vie privée dans le bureau.

Les précautions techniques :

- 🔒 Voir à de forts mots de passe et au cryptage pour les ordinateurs, les réseaux sans fil et les appareils mobiles sans fil.
- 🔒 Communiquer avec votre fournisseur de logiciel de gestion pour vous assurer que toute transmission électronique de données est cryptée et protégée.
- 🔒 Organiser la fermeture de session et le verrouillage automatiques des ordinateurs quand ils ne sont pas en usage.
- 🔒 Tenir un journal d'audit pour montrer qui a eu accès au dossier électronique du patient.
- 🔒 Assurer un bon contrôle de l'accès afin de permettre seulement aux personnes autorisées du cabinet dentaire d'avoir accès seulement aux renseignements personnels sur le patient qui leur sont nécessaires pour faire leur travail.
- 🔒 Protéger le système de données électroniques contre les maliciels et organiser la mise à jour et la sauvegarde des données à intervalles réguliers.
- 🔒 Garder uniquement un nombre minimal de renseignements personnels sur le patient sur un appareil mobile sans fil (CD, lecteur d'appoint, portable, clé USB, Smartphone).

REMARQUE :

Les dentistes doivent s'assurer que les membres du personnel qui téléphonent aux patients et laissent un message sur leur répondeur ont appris à laisser seulement le nombre minimal de renseignements nécessaires (comme « Ce message s'adresse à M. Jean Untel. Veuillez téléphoner au bureau de votre dentiste au numéro xxx. »). Il importe de ne pas laisser sur le répondeur de l'information qui peut laisser entendre ou deviner la nature des renseignements personnels sur la santé ayant trait au patient et faisant l'objet de l'appel téléphonique.



Avertissement : Médias sociaux

Le cabinet dentaire peut utiliser les médias sociaux pour faire de la promotion, mais les dentistes doivent connaître les risques de l'utilisation des médias sociaux pour communiquer avec les patients. La protection des patients, de la sécurité et de la confidentialité des renseignements personnels sur la santé doit être assurée dans un environnement en ligne. Les dentistes ne doivent pas afficher des renseignements sur un patient identifiable.

VII. NOTIFICATION OBLIGATOIRE DES VIOLATIONS DE LA SÉCURITÉ

Il peut y avoir une violation de la sécurité quand des renseignements personnels sur la santé :

- sont perdus;
- sont volés;
- sont recueillis, utilisés, divulgués ou détruits d'une manière non autorisée ou sans consentement;
- sont consultés par une personne non autorisée.

La meilleure manière de prévenir toute violation de la sécurité est de réviser régulièrement les précautions physiques, administratives et techniques visant à protéger les renseignements personnels sur la santé.

S'il y a eu une violation de la sécurité, le but ultime sera de réduire les effets néfastes possibles et de prévenir toute violation future.

Voici les mesures à prendre en considération :

1. Limiter la divulgation de renseignements personnels

- ✓ Il peut être nécessaire de communiquer avec la police si des renseignements personnels sur le patient ont été volés; ou
- ✓ Il peut être nécessaire de communiquer avec un expert en technologie de l'information pour une vérification judiciaire de votre système si, par exemple, il semble que quelqu'un a « piraté » votre système électronique.

2. Dès que possible :

- ✓ Aviser toutes les personnes touchées (celles dont les renseignements personnels font l'objet de la violation de sécurité).
- ✓ Aviser le commissaire à l'accès aux renseignements personnels (obligatoire en vertu de la Loi).
- ✓ Aviser la Société dentaire du Nouveau-Brunswick.

3. Prendre des mesures correctives pour empêcher que cela ne se reproduise :



- ✓ Il est important de déterminer la cause de la violation afin de prendre les mesures nécessaires pour s'assurer que cela ne se reproduise pas et que les renseignements personnels sur la santé sont bien protégés de façon continue.

VIII. POUR COMBIEN DE TEMPS DOIS-JE GARDER MES DOSSIERS?

Conformément à la Loi, les dépositaires (les dentistes) doivent avoir une politique écrite sur la collecte, l'utilisation, la communication et la destruction sécuritaire des renseignements personnels sur la santé. Bien entendu, vous devriez communiquer cette politique à vos patients.

En vertu de la Loi sur la prescription du Nouveau-Brunswick, la Société dentaire du Nouveau-Brunswick recommande de garder les dossiers des patients pour un minimum de 15 ans, car une procédure judiciaire peut être entamée 15 ans après une action ou omission qui est visée par cette procédure. La SDNB fait cette recommandation pour s'assurer que les dentistes pourront fournir les documents pour se défendre en cas de procédure judiciaire.

REMARQUE :

En vertu de la Loi, le délai de prescription ne commence pas avant que le demandeur ait atteint l'âge de 19 ans. Le dentiste doit prendre en considération l'âge de son patient avant de prendre toute décision concernant la destruction de son dossier.

Par ailleurs, la SDNB vous recommande de consulter un conseiller juridique pour l'élaboration d'une politique de conservation des dossiers pendant moins que 15 ans.

Destruction

La Loi exige que le dépositaire (dentiste) garde un résumé du contenu avant la destruction indiquant :

- ✓ Le nom du patient dont les renseignements personnels sur la santé seront détruits.
- ✓ Un résumé du contenu du dossier qui sera détruit.
- ✓ La période visée par les dossiers qui seront détruits (par exemple de 2004 à 2014).
- ✓ La méthode de destruction (déchetage sécurisé, effacement du disque).
- ✓ Le nom de la personne qui a supervisé la destruction.

IX. RETRAITE ET DÉMÉNAGEMENT

Je prends ma retraite ou je ferme mon cabinet dentaire. Que dois-je faire maintenant?

La responsabilité juridique du dentiste à titre de dépositaire des renseignements personnels sur ses patients ne prend pas fin quand il déménage ou prend sa retraite.

Quand le dentiste ferme son cabinet, il doit s'assurer que le dossier du patient ne devienne pas « orphelin ». Les patients doivent pouvoir avoir accès à des copies de leurs renseignements personnels sur la santé. Si le dentiste cesse de pratiquer la dentisterie (parce qu'il n'a plus son permis ou qu'il est décédé), les dossiers doivent être conservés pendant les périodes susmentionnées à moins que :

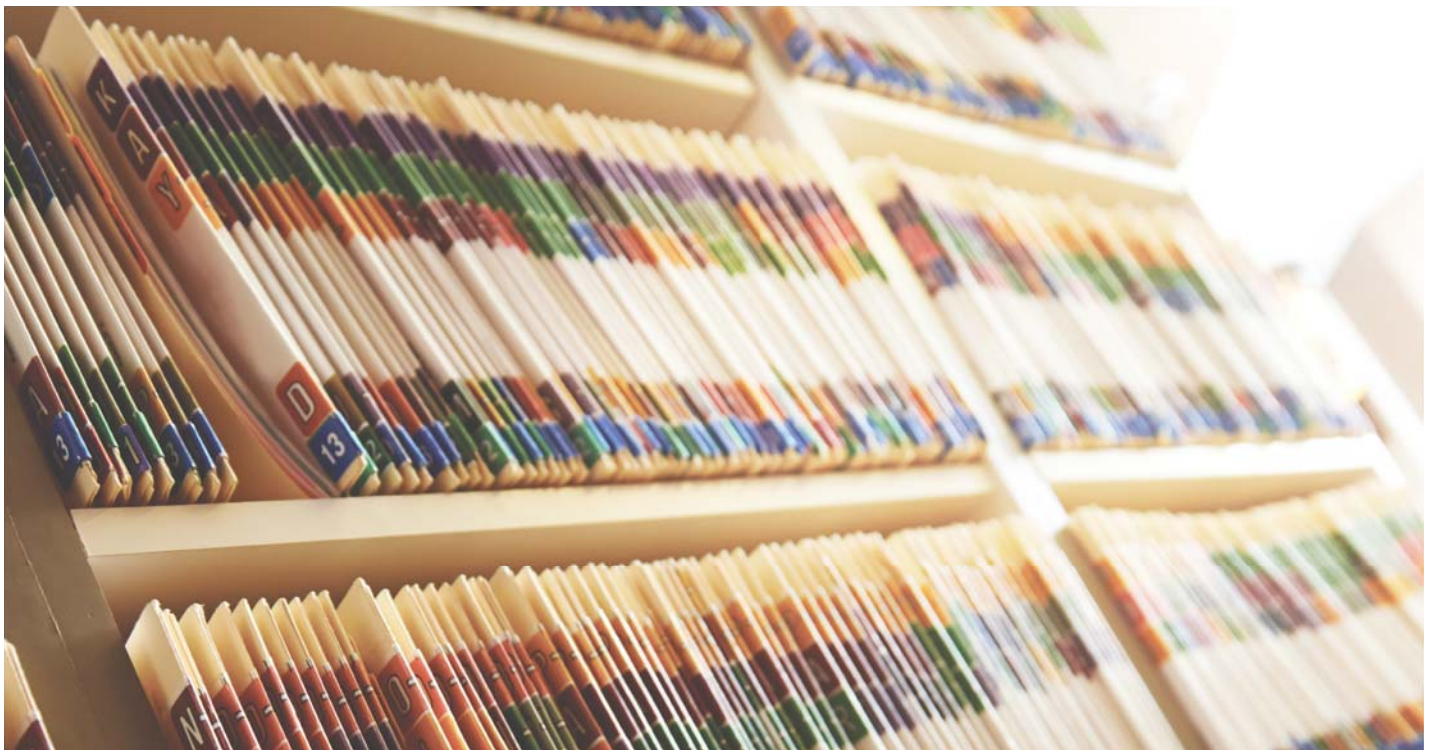
- 1) La garde et le contrôle complets des dossiers ont été transférés à un autre dépositaire (dentiste) et chaque patient a été avisé du transfert, ou
- 2) Chaque patient a été avisé de l'endroit où se trouve son dossier et de la date à laquelle son dossier sera détruit après cet avis conformément à la période de conservation recommandée par la SDNB.

Il faut fournir la chance aux patients d'obtenir leurs dossiers. Voir l'Annexe D – Liste de contrôle des dépositaires en cas de changements dans la pratique.

REMARQUE :

La SDNB recommande fortement que tout dentiste qui déménage ou prend sa retraite communique avec la SDNB et précise l'emplacement des dossiers afin que le personnel puisse répondre aux demandes de renseignements des patients.

Il est recommandé de garder les dossiers le plus longtemps possible non seulement pour répondre aux besoins des patients, mais aussi pour permettre aux dentistes d'avoir accès aux renseignements pertinents advenant une action au civil dans le délai prescrit par la Loi.



X. DROITS POUR FOURNIR UNE COPIE DU DOSSIER AU PATIENT

La Loi sur l'accès et la protection en matière de renseignements personnels sur la santé du Nouveau-Brunswick contient des dispositions sur les droits à payer par le patient pour obtenir les renseignements personnels sur la santé demandés. Le patient peut consulter le dossier sur place gratuitement OU payer des droits pour obtenir une copie du dossier comme suit :

Recherche et préparation	Copies	Traitement des données	Poste et livraison
<i>Imposer des droits seulement si cela prend plus de 2 heures.</i>	<i>Demander des droits de 25 cents par page.</i>	<i>Demander des droits de 10 \$ pour chaque 15 minutes de traitement des données.</i>	<i>Aucun droit pour l'envoi des copies par la poste ordinaire.</i>
<i>Demander des droits de 15 \$ pour chaque 30 minutes additionnelles.</i>	<i>Ou facturer le coût réel pour le service.</i>	<i>Ou facturer le coût réel pour le service.</i>	<i>Ou facturer le coût réel pour le service de livraison.</i>

Chaque dentiste peut décider de ne pas imposer une partie des droits si cela peut entraîner une difficulté au patient sur le plan financier.

REMARQUE :

Les dentistes peuvent voir le Guide des tarifs suggérés de la SDNB (codes 93211 et 02911-02919 du système de codage normalisé et de la liste des services) en ce qui concerne la reproduction des dossiers et des radiographies; (code 04912) pour la reproduction des modèles. La SDNB n'approuve pas des « frais d'administration » parce que le patient ne devrait pas avoir à payer en plus des coûts réels pour faire des copies, reproduire et transférer son dossier.

ANNEXE A

Pour de plus amples renseignements, veuillez communiquer avec :

Société dentaire du Nouveau-Brunswick

520, rue King, Place HSBC, pièce 820

C. P. 488, Succursale A

Fredericton (N.-B.) E3B 4Z9

Téléphone : 506-452-8575

Télécopieur : 506-452-1872

Courriel : SDNB@nb.aibn.com

Site Web : www.nbdental.com

Commissariat à l'accès à l'information et à la protection de la vie privée

65, rue Regent, pièce 230

Fredericton (N.-B.) E3B 7H8

Téléphone : 506-453-5965

Sans frais : 1-877-755-2811

Télécopieur : 506-453-5963

Courriel : access.info.privacy@gnb.ca

Site Web : www.info-priv-nb.ca

La Loi sur l'accès et la protection en matière de renseignements personnels sur la santé (LAPRPS)

<http://www.gnb.ca/0051/acts/legislation-f.asp>

La Loi sur la protection des renseignements personnels et les documents électroniques du Canada

https://www.priv.gc.ca/information/pub/guide_org_f.asp

RÈGLE 7

DÉPOSITAIRE DÉSIGNÉ DES DOSSIERS DENTAIRES DES PATIENTS

Tout dentiste pratiquant qui ne garde pas son permis pour une raison quelconque, comme un congé, le départ de la province ou la retraite, doit communiquer avec la SDNB pour fournir une confirmation par écrit de la personne qui deviendra le dépositaire désigné des dossiers dentaires des patients du dentiste qui quitte la pratique.

Le défaut de désigner un dépositaire des dossiers dentaires des patients comme il est exigé dans cette règle fera l'objet d'une plainte par le registraire pour faute professionnelle.

ANNEXE C

Liste de contrôle – Sécurité et protection de la vie privée

A. POLITIQUES ET PROCÉDURES CLINIQUES	OUI	NON	Commentaires
Avez-vous une politique du bureau concernant la protection de la vie privée qui porte sur la confidentialité des renseignements personnels sur la santé, y compris l'impression, le transfert, l'entreposage et la destruction sécuritaire des dossiers des patients?			
Est-ce qu'il y a des procédures en place pour faire face à une violation de la vie privée réelle ou soupçonnée ou à un incident concernant la sécurité?			
Est-ce qu'il existe des processus pour une destruction sécuritaire des documents sur papier et vieux appareils électroniques (entreposage des données, ordinateurs, etc.) qui peuvent contenir des données confidentielles?			

B. PERSONNEL	OUI	NON	Commentaires
Avez-vous désigné une personne (et déléguer) responsable de la sécurité et de la protection de la vie privée? Elle sera responsable de répondre aux questions (des patients), mais aussi aux plaintes, aux enquêtes sur des incidents, aux atteintes à la vie privée et aux audits en plus de s'assurer que le personnel a reçu la formation nécessaire mise à jour sur les politiques et les procédures.			
Les membres du personnel ont-ils signé une entente sur la confidentialité?			
Les membres du personnel ont-ils reçu une formation sur la protection de la vie privée et de la confidentialité des renseignements personnels sur la santé?			
Avez-vous une activité annuelle de sensibilisation à la sécurité et à la protection de la vie privée qui inclut le besoin de protéger le nom d'utilisateur, les mots de passe, les clés et autres références d'accès?			

C. PARTENAIRES	OUI	NON	Commentaires
Est-ce que vos contrats avec de tierces parties (comme une compagnie de déchiquetage) incluent des dispositions pour la protection de la vie privée et de la confidentialité?			

D. PATIENTS	OUI	NON	Commentaires
Avez-vous une affiche sur la protection de la vie privée des patients ou d'autre matériel qui avise les patients de vos politiques sur la protection des renseignements personnels?			
Avez-vous des procédures pour répondre aux demandes des patients pour de l'information, des corrections et des plaintes?			

CONSIDÉRATIONS ADDITIONNELLES SI VOUS UTILISEZ DES ORDINATEURS, DES TÉLÉCOPIEURS ET DES APPAREILS ÉLECTRONIQUES

E. GESTION DES DOSSIERS ÉLECTRONIQUES ET CONTINUITÉ	OUI	NON	Commentaires
Avez-vous désigner une personne responsable de la gestion des dossiers électroniques (établissement de nouveaux comptes, changements des privilèges d'utilisateur, désactivation des vieux comptes d'utilisateurs)?			
Avez-vous donné un nom d'utilisateur et un bon mot de passe à chaque personne ayant accès aux dossiers électroniques?			
Avez-vous des contrôle efficaces pour vous assurer que seules les personnes autorisées dans le cabinet dentaire ont accès aux renseignements personnels des patients nécessaires pour faire leur travail et que cet accès soit caractérisé comme étant « de lire », « d'écrire » et/ou « de modifier » selon le besoin pour ces responsabilités?			
Vos systèmes ont-ils une vérification à rebours?			
Avez-vous un calendrier et des procédures qui permettent à la personne désignée de procéder à des vérifications périodiquement et à des vérifications sans préavis?			
Avez-vous un plan de poursuites des activités en cas de désastre ou d'une panne des systèmes causée par des dangers environnementaux ou autres?			

F. MATÉRIEL, LOGICIELS ET PÉRIPHÉRIQUES	OUI	NON	Commentaires
Vos politiques s'appliquent-elles à l'utilisation du télécopieur et du courrier électronique?			
Vos périphériques (imprimantes, télécopieurs) se trouvent-ils dans un endroit sécuritaire pour éviter un accès non autorisé?			
Est-ce que les écrans d'ordinateurs sont placés de manière à éviter qu'une personne non autorisée puisse les voir?			
Avez-vous prévu le cryptage des données des patients sur les ordinateurs, portables et appareils mobiles?			
Avez-vous des procédures et contrôles (verrouillage automatique) pour éviter qu'une personne non autorisée puisse voir l'écran si l'utilisateur n'est pas là?			
Avez-vous installé un programme antivirus récent sur tous les postes d'ordinateurs et ce programme est-il régulièrement activé et mis à jour?			
Avez-vous un pare-feu sur les ordinateurs ayant accès à l'internet?			
Est-ce que votre logiciel de diagnostic est conforme aux Règlements sur les instruments médicaux de Santé Canada?			

G. RÉSEAU LOCAL (LAN) ET ACCÈS SANS FIL	OUI	NON	Commentaires
Votre courrier électronique est-il sécurisé avec un bon cryptage pour satisfaire vos obligations de protéger les renseignements personnels sur la santé des patients?			
L'information communiquée aux patients ou collègues par des appareils sans fil (courriels et textes) est-elle bien codée ou rendue non identifiable?			
Les contrôles appropriés ont-ils été obtenus pour rendre le réseau local (LAN) sécuritaire?			
Les paramètres de sécurité sans fil ont-ils été établis et activés (transmission restreinte, pare-feu, cryptage)?			
Avez-vous des contrôles appropriés pour votre réseau privé virtuel si vous en avez un?			

Liste de vérification pour la protection des renseignements personnels sur la santé au Nouveau-Brunswick

À l'usage des dépositaires en cas de changement dans la pratique professionnelle

Le 1^{er} septembre 2010, la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* (« la Loi ») a été promulguée afin de donner à toute personne le droit d'accéder aux renseignements personnels sur la santé la concernant, d'établir des règles concernant l'utilisation, la collecte et la communication de ces renseignements privés et de protéger la confidentialité des renseignements personnels sur la santé et la vie privée des personnes concernées. Cette nouvelle Loi permet également au Commissariat à l'accès à l'information et à la protection de la vie privée d'exercer un rôle de surveillance afin de veiller à son respect, à tous les égards. En résumé, la Loi reflète la nouvelle approche adoptée par la Province pour l'amélioration globale du système de soins de santé public et se traduit pour de nombreux professionnels de la santé – les dépositaires – par des changements dans la manière dont les renseignements personnels sur la santé sont protégés.

Afin de faciliter la mise en œuvre des nouvelles règles prescrites par la Loi, le Commissariat à l'accès à l'information et à la protection de la vie privée a élaboré des **LISTES DE VÉRIFICATION À L'USAGE DES DÉPOSITAIRES** des plus utiles. Ces dernières sont destinées à guider les principaux intéressés à travers une série d'étapes faciles, conçues pour assurer la sécurité des dossiers médicaux des patients ou clients dans toute situation comportant un changement à la pratique professionnelle. Les dépositaires doivent continuer d'assumer la responsabilité des dossiers de leurs patients ou clients jusqu'à ce que ces dossiers soient confiés à un autre dépositaire ou à une autre personne légalement autorisée à les détenir, ou jusqu'à ce qu'ils soient détruits conformément aux dispositions prévues par la Loi. Avant de parcourir les **LISTES DE VÉRIFICATION** qui suivent, tous les dépositaires doivent être avisés d'une obligation essentielle en vertu de la Loi : celle d'établir des **DIRECTIVES ÉCRITES** concernant la conservation, l'archivage et la destruction sécuritaires des dossiers médicaux sous leur garde et l'accès à ces dossiers. Ces directives permettront d'éviter que les renseignements personnels sur la santé de vos patients soient volés, perdus, éliminés par inadvertance ou communiqués à une personne non autorisée, ou qu'une personne non autorisée puisse y accéder.

Les présentes **LISTES DE VÉRIFICATION À L'USAGE DES DÉPOSITAIRES** sont destinées à être utilisées chaque fois que les dépositaires envisagent un changement à leur pratique professionnelle impliquant :

- A) la fermeture TEMPORAIRE du bureau (congé sabbatique, maladie, etc.);
- B) la fermeture PERMANENTE du bureau ou du cabinet : sa vente, le transfert de la clientèle à un autre dépositaire ou le déménagement du dépositaire concerné ailleurs au Nouveau-Brunswick ou à l'extérieur de la province, par exemple.

Selon la nature du changement envisagé, veuillez-vous reporter à la LISTE DE VÉRIFICATION A pour une FERMETURE TEMPORAIRE du bureau ou du cabinet et à la LISTE DE VÉRIFICATION B pour une FERMETURE PERMANENTE.



Liste de vérification A : Fermeture temporaire du bureau ou du cabinet

- ÉTAPE 1 : Connaître l'existence de TOUS les dossiers (actifs et inactifs) dont vous avez la garde et la responsabilité.
- ÉTAPE 2 : Créer une liste de tous les dossiers inventoriés à l'étape 1.
- ÉTAPE 3 : Décider d'un endroit sûr où les dossiers à conserver seront entreposés. Rappelez-vous que vous demeurez responsable, en tant que dépositaire, des dossiers de vos patients ou clients, même lorsqu'ils sont entreposés. Un endroit sûr dispose, par définition, de garanties appropriées.
- ÉTAPE 4 : Informer toutes les personnes dont vous détenez les dossiers (patients et clients) de la fermeture temporaire de votre bureau ou cabinet et de la durée anticipée de la fermeture.

Ceux qui ont besoin d'une copie de leur dossier seront ainsi en mesure d'en demander une. L'avis envoyé aux patients ou clients doit indiquer à qui ils peuvent présenter une demande écrite pour avoir accès à leur dossier et stipuler que le dossier en question sera conservé jusqu'à la réouverture du bureau ou jusqu'à ce qu'ils reçoivent un autre avis de votre part.

- ÉTAPE 5 : Déterminer quels dossiers doivent être conservés et lesquels peuvent être détruits. Informez-vous auprès de votre association professionnelle pour connaître le calendrier de conservation suggéré pour les dossiers se trouvant sous votre garde (durée pendant laquelle ils doivent être conservés).

Les lignes directrices du Collège des médecins et chirurgiens du Nouveau-Brunswick prévoient, par exemple, le calendrier suivant :

- *dossiers de patients : 10 ans après la dernière consultation;*
- *dossiers de mineurs : 10 ans après la dernière consultation, ou après que le mineur a atteint l'âge de 21 ans, la date la plus tardive l'emportant;*
- *dossiers de patients décédés : 2 ans après la date de décès.*

- ÉTAPE 6 : Détruire les dossiers qui n'ont plus à être conservés, et ce, de manière sécuritaire (déchetage sécuritaire, nettoyage du disque, etc.). Lorsque vous procédez à la destruction de dossiers, vous devez consigner par écrit les renseignements suivants :

- a) noms des personnes dont les dossiers seront détruits;
- b) résumé du contenu de chaque dossier détruit;
- c) période concernée par chacun de ces dossiers;
- d) méthode de destruction employée (p. ex. déchetage sécuritaire ou incinération par l'entreprise X);
- e) nom de la personne ayant supervisé la destruction.

Veillez utiliser l'**annexe ci-jointe**, intitulée **Modèle de tableau pour les dossiers détruits de manière sécuritaire**, pour vous aider à assurer le suivi des renseignements obtenus à l'ÉTAPE 6.

Liste de vérification B : Fermeture permanente du bureau ou du cabinet

- ÉTAPE 1 : Connaître l'existence de TOUS les dossiers (actifs et inactifs) dont vous avez la garde et la responsabilité.
- ÉTAPE 2 : Créer une liste de tous les dossiers inventoriés à l'étape 1.
- ÉTAPE 3 : Déterminer quels dossiers doivent être conservés et lesquels peuvent être détruits. Informez-vous auprès de votre association professionnelle pour connaître le calendrier de conservation suggéré pour les dossiers se trouvant sous votre garde (durée pendant laquelle ils doivent être conservés).

Les lignes directrices du Collège des médecins et chirurgiens du Nouveau-Brunswick prévoient, par exemple, le calendrier suivant :

- *dossiers de patients : 10 ans après la dernière consultation;*
 - *dossiers de mineurs : 10 ans après la dernière consultation, ou après que le mineur a atteint l'âge de 21 ans, la date la plus tardive l'emportant;*
 - *dossiers de patients décédés : 2 ans après la date de décès.*
- ÉTAPE 4 : Détruire les dossiers qui n'ont plus à être conservés, et ce, de manière sécuritaire (déchetage sécuritaire, nettoyage du disque, etc.). Lorsque vous procédez à la destruction de dossiers, vous devez consigner par écrit les renseignements suivants :
 - a) noms des personnes dont les dossiers seront détruits;
 - b) résumé du contenu de chaque dossier détruit;
 - c) période concernée par chacun de ces dossiers;
 - d) méthode de destruction employée (p. ex. déchetage sécuritaire ou incinération par l'entreprise X);
 - e) nom de la personne ayant supervisé la destruction.

Veuillez utiliser l'**annexe ci-jointe**, intitulée **Modèle de tableau pour les dossiers détruits de manière sécuritaire**, pour vous aider à assurer le suivi des renseignements obtenus à l'ÉTAPE 4.

- ÉTAPE 5 : Décider d'un endroit sûr où les dossiers à conserver seront entreposés. Rappelez-vous que vous demeurez responsable, en tant que dépositaire, des dossiers de vos patients ou clients, même lorsqu'ils sont entreposés. Un endroit sûr dispose, par définition, de garanties appropriées.
- ÉTAPE 6 : Informer toutes les personnes dont vous détenez les dossiers (patients et clients) de la fermeture de votre bureau ou cabinet.
Ceux qui ont besoin d'une copie de leur dossier seront ainsi en mesure d'en demander une.
L'avis envoyé aux patients ou clients doit comprendre le nom d'une personne-ressource à qui ils peuvent présenter une demande écrite pour avoir accès à leur dossier, et indiquer pendant combien de temps vous conserverez le dossier en question avant qu'il ne soit détruit (selon votre calendrier de conservation).

Directives destinées aux dépositaires

– pour évaluer leur conformité avec la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé (LAPRPS)*

Le présent document vise à aider les dépositaires à évaluer s'ils sont prêts à se conformer à la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* et pour faciliter l'identification des cas où des politiques ou des pratiques doivent être élaborées ou modifiées pour garantir la conformité. Il vise à compléter le document intitulé : *Préparation à la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé (LAPRPS) : une liste de contrôle pour les dépositaires*.

NOTA : Le présent document est un guide uniquement; il ne prétend pas fournir un énoncé complet des obligations légales de votre organisme et, à ce titre, il ne doit pas être considéré comme un avis juridique. Il faut toujours se reporter au texte officiel de la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé et de ses règlements pour un énoncé complet de la loi et pour obtenir davantage d'information sur les points dont il est question dans le présent document. Les articles pertinents de la Loi sont indiqués entre parenthèses tout au long du document afin de vous aider.

1. Êtes-vous un « dépositaire » selon la définition de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*? (Article 1)

La Loi sur l'accès et la protection en matière de renseignements personnels sur la santé s'applique aux renseignements personnels sur la santé qui sont recueillis, utilisés ou communiqués par un dépositaire ou qui sont sous la garde ou le contrôle du dépositaire. Le terme « dépositaire » désigne une personne ou un organisme qui recueille, conserve ou utilise des renseignements personnels sur la santé à des fins soit de prestation ou d'aide à la prestation de soins de santé ou de traitement, soit de planification et de gestion du système de soins de santé ou de prestation d'un programme ou d'un service gouvernemental, et notamment :

- (a) les organismes publics;
- (b) les fournisseurs de soins de santé;
- (c) le ministre;
- (d) les organismes suivants :
 - (i) *Ambulance Nouveau-Brunswick inc.*,
 - (ii) *le Conseil du Nouveau-Brunswick en matière de santé*,
 - (iii) *FacilicorpNB Ltée*,
 - (iv) *les régies régionales de la santé*,
 - (v) *Travail sécuritaire NB*,
 - (vi) *la Société canadienne du sang*;
- (e) les gestionnaires de l'information;
- (f) les personnes qui dirigent des projets de recherche approuvés en conformité avec la présente *Loi*;
- (g) les établissements de soins de santé;
- (h) les laboratoires ou les centres de prélèvement;
- (i) les foyers de soins et les exploitants selon la définition que donne de ces termes la *Loi sur les foyers de soins*;
- (j) les personnes que les règlements désignent à titre de dépositaires.

Oui Non

Êtes-vous (ou votre organisme est-il) un dépositaire selon la définition donnée ci-dessus?

2. Devez-vous recueillir, utiliser, communiquer ou conserver des renseignements personnels sur la santé qui pourraient être soumis à la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé? (Articles 1 et 3)

La Loi sur l'accès et la protection en matière de renseignements personnels sur la santé s'applique aux renseignements personnels sur la santé qui sont recueillis, utilisés ou communiqués par un dépositaire ou qui sont sous la garde ou le contrôle du dépositaire. Les renseignements personnels sur la santé sont définis en partie comme les renseignements qui permettent d'identifier une personne dans le cas où ils ont trait à la santé mentale ou physique de cette personne, aux antécédents de sa famille ou à ses antécédents de soins de santé. En voici quelques exemples :

- données génétiques;
- données sur l'inscription, y compris le numéro d'Assurance-maladie;
- renseignements sur les paiements ou l'admissibilité de la personne en matière de soins de santé ou de couverture des soins de santé;
- renseignements liés au don d'organes de la part de la personne;
- données d'analyse des organes ou des substances corporelles de la personne;
- renseignements qui identifient le fournisseur de soins de santé ou le mandataire spécial de la personne.

Certains documents et renseignements comportant des renseignements personnels sur la santé peuvent ne pas être soumis à la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé. Veuillez vous reporter à la Question 3 et consulter la Loi pour en savoir davantage.

Oui Non

Avez-vous des dossiers contenant des renseignements personnels sur la santé?

3. Les exceptions définies dans la LAPRPS au sujet des renseignements personnels sur la santé qui ne sont pas concernés par l'application de la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé s'appliquent-elles aux renseignements personnels sur la santé sous votre garde ou votre contrôle? (Articles 3 et 4)

La Loi prévoit certains cas dans lesquels les renseignements personnels sur la santé ne seront pas concernés par l'application de la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé et pour lesquels la Loi ne s'appliquera pas. Par exemple, la Loi ne s'applique pas :

- à une personne ou un organisme qui recueille, conserve ou utilise des renseignements personnels sur la santé à des fins autres que des soins de santé ou de traitement, de planification ou de gestion du système de soins de santé, ou de prestation d'un programme ou d'un service gouvernemental, y compris : les employeurs (publics et privés), les compagnies d'assurance, les organismes de réglementation des professions de la santé, les personnes autorisées ou inscrites aux fins de la fourniture de soins de santé, mais qui n'en fournissent pas, et toute autre personne ou tout autre organisme défini par le règlement;
- aux renseignements personnels sur la santé contenus dans un dossier créé il y a 100 ans ou plus ou lorsqu'une période d'au moins 50 ans s'est écoulée depuis le décès de la personne concernée;
- aux renseignements contenus dans des documents juridiques, tels que des documents concernant des services de soutien fournis à un juge ou à un auxiliaire de justice;

- à un document produit ou aux renseignements détenus par une personne en vertu de certaines autres lois de l'Assemblée législative, y compris la *Loi sur les services à la famille*, la *Loi sur la santé mentale*, et toute autre loi de l'Assemblée législative définie par le règlement.

Consultez la *Loi* et les règlements pour obtenir davantage de renseignements sur les cas où la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* peut ne pas s'appliquer.

Oui **Non**

- Cochez « oui » si des exceptions peuvent exempter des renseignements personnels sur la santé sous votre garde ou votre contrôle de l'application de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*.

Vos réponses aux questions 1, 2 et 3 peuvent être utilisées pour évaluer si la LAPRPS s'appliquera à tous les renseignements personnels sur la santé sous votre garde ou votre contrôle, ou seulement à une partie d'entre eux. Pour une évaluation plus complète de l'application de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* dans votre cas particulier, consultez la *Loi* et ses règlements.

4. Droits de la personne

4.1. Obtention du consentement (Articles 17, 18, 19)

4.1.1 Considérations générales au sujet du consentement

Oui **Non**

- Avez-vous obtenu le consentement de la personne pour la collecte, l'utilisation ou la communication de renseignements personnels, sauf mention contraire dans la *Loi* ou une autre loi?
- Le consentement est-il éclairé? (Pour qu'un consentement soit éclairé, les personnes doivent être informées [par la mise à disposition d'un avis ou par un moyen semblable] en termes simples de la fin visée par la collecte, l'utilisation ou la communication de leurs renseignements au sein du cercle des soins ou en dehors et qu'elles soient informées de leur droit à refuser ou à retirer leur consentement.)
- Le consentement est-il expressément lié aux renseignements personnels sur la santé recueillis et aux fins visées par leur utilisation?
- Le consentement est-il volontaire (le consentement ne peut être obtenu sous la contrainte)?

4.1.2 Consentement explicite

Oui **Non**

- Le cas échéant, avez-vous obtenu le consentement explicite pour la collecte, l'utilisation ou la communication de renseignements personnels sur la santé? (Lorsque le consentement est requis aux termes de la *Loi*, il doit être explicite, sauf si la *Loi* permet précisément un consentement implicite – voir le point 4.1.3 ci-dessous)

De manière générale et sauf indication contraire de la *Loi*, l'obtention du consentement explicite sera nécessaire lorsque les renseignements seront communiqués :

- ✓ aux médias;
- ✓ aux collecteurs de fonds;
- ✓ à un visiteur à un établissement de soins de santé;
- ✓ à une personne à des fins autres que des soins de santé (par exemple des renseignements communiqués à une compagnie d'assurance);
- ✓ à une personne à l'extérieur du Nouveau-Brunswick (certaines exceptions s'appliquent – consultez l'article 47);
- ✓ à une personne à des fins de recherche (certaines exceptions s'appliquent – consultez l'article 43).

Oui Non

- Vous assurerez-vous que le consentement explicite est obtenu par écrit auprès de la personne ou de son mandataire spécial?
- Les considérations générales relatives au consentement présentées dans le point 4.1.1 ont-elles été respectées?

4.1.3 Consentement implicite

Oui Non

- Existe-t-il un consentement éclairé implicite de la personne pour communiquer ses renseignements personnels sur la santé au sein du cercle des soins pour la prestation de soins de santé à cette personne? *(Pour qu'un consentement éclairé implicite existe, il doit être raisonnable de présumer que la personne comprend les fins visées par la collecte, l'utilisation ou la communication de ses renseignements personnels sur la santé au sein du cercle des soins et les conséquences de l'accord ou du refus du consentement).*
- Les considérations générales relatives au consentement présentées dans le point 4.1.1 ont-elles été respectées?

4.1.4 Consentement non requis

Oui Non

- Si vous recueillez, utilisez ou communiquez des renseignements personnels sur la santé sans consentement, l'autorité d'agir de la sorte aux termes de la *Loi* a-t-elle été justifiée et confirmée?
- Avez-vous un moyen d'assurer que tous les renseignements personnels sur la santé communiqués sans consentement sont consignés conformément à l'article 46 de la *Loi*?

4.2. Directives en matière de consentement (Article 22)

Oui Non

- Lorsque le consentement a été obtenu, des procédures sont-elles en place pour répondre à la demande d'une personne de retirer son consentement pour la collecte, l'utilisation ou la communication de ses renseignements personnels sur la santé?
- Des procédures sont-elles en place pour contrôler et surveiller les situations dans lesquelles un dépositaire peut avoir à outrepasser la directive en matière de consentement d'une personne conformément à la *Loi* (par exemple pour des raisons de santé et de sécurité)? *(Ces procédures doivent inclure, sans y être limitées : l'enregistrement, le contrôle et la vérification des dérogations relatives aux directives en matière de consentement consignées et autorisées par la Loi).*

- Si des réseaux d'information sont utilisés, un processus est-il en place pour informer les personnes sur la manière dont elles peuvent exercer leur droit afin d'empêcher l'accès à leurs renseignements personnels sur la santé contenus dans un réseau d'information ou d'en empêcher la communication? *(Remarquez toutefois qu'une personne ne peut pas retirer son consentement pour la collecte de renseignements personnels sur la santé par un dépositaire aux fins de création ou de maintien d'un réseau d'information.)*

4.3 Droit d'être informé (Article 31)

Oui Non

- Avez-vous pris des mesures raisonnables pour informer directement les personnes auprès desquelles les renseignements personnels sur la santé sont directement recueillis de la fin visée (y compris des utilisations et des communications prévues) par la collecte des renseignements, et ce, avant la collecte ou dès que possible? *(Les « mesures raisonnables » peuvent comprendre, par exemple, la création d'une affiche ou d'un avis sur la protection des renseignements personnels et la mise à disposition de ces éléments sur le site Web du dépositaire ou sous forme de document à distribuer; la notification verbale ou écrite des personnes sur la manière dont elles peuvent obtenir une copie de l'avis de l'organisme; et la description de la fin visée par la collecte sur les formulaires utilisés pour recueillir les renseignements personnels sur la santé.)*

4.4. Collecte du numéro d'Assurance-maladie (Article 48)

Oui Non

- Les personnes sont-elles uniquement tenues de présenter leur numéro d'Assurance-maladie pour des raisons liées aux services de santé?
- Si vous avez besoin du numéro d'Assurance-maladie pour des raisons qui ne sont pas liées à la santé, la collecte est-elle autorisée par une loi ou son règlement? *(Si non, la collecte peut être volontaire, mais elle ne peut pas devenir une condition pour l'obtention d'un service. Les personnes doivent avoir la possibilité d'utiliser un autre moyen d'identification.)*

4.5. Le droit d'une personne de déposer une plainte auprès du Commissaire à l'accès à l'information et à la protection de la vie privée au sujet d'une action ou d'une décision d'un dépositaire (Partie 6)

Oui Non

- Les personnes sont-elles informées de leur droit de communiquer avec le Commissaire à l'accès à l'information et à la protection de la vie privée pour demander l'examen d'une action effectuée ou d'une décision prise, dans le cas où vous ne pourriez résoudre une préoccupation concernant leurs renseignements personnels sur la santé?

4.6. Possibilité pour une personne de désigner une autre personne (Articles 25,26)

Oui Non

- Disposez-vous de procédures pour traiter la demande écrite d'une personne pour désigner une autre personne qui agira en son nom au sujet de ses droits relatifs à ses renseignements personnels sur la santé?

- Si une personne n'est pas capable d'agir en son nom, vous assurez-vous que la personne désignée entre dans le cadre de l'un des cas déterminés dans l'article 25 de la *Loi*?

4.7 Demandes d'accès aux renseignements personnels sur la santé (Partie 2, Section A)

Oui Non

- Avez-vous mis en place des procédures pour recevoir les demandes d'accès et accorder l'accès aux documents comportant des renseignements personnels sur la santé?
- Facturerez-vous des frais pour accorder l'accès? Si oui, sont-ils cohérents avec les règlements visés par la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*?
- Lorsque vous répondez aux demandes de communication de renseignements personnels sur la santé, disposez-vous de procédures visant à identifier uniquement la personne concernée par ces renseignements avant d'en accorder l'accès?

4.8. Demandes de correction des renseignements personnels sur la santé

Oui Non

- Avez-vous mis en place des procédures visant à corriger les dossiers de renseignements personnels sur la santé lorsque cela est exigé par la personne concernée par ces renseignements; ou visant à inclure une mention de désaccord aux dossiers comportant les renseignements personnels sur la santé de la personne?

5. Protection des renseignements personnels sur la santé

5.1. Devoir de protection (Article 50)

Oui Non

- Avez-vous élaboré une politique de sécurité et des procédures connexes qui définissent de quelle manière votre organisme garantira que des mesures de sécurité raisonnables sont en place pour protéger la confidentialité, la sécurité, l'exactitude et l'intégrité des renseignements personnels sur la santé dont vous avez la garde ou le contrôle?
- Un examen a-t-il été effectué pour garantir que les politiques et les pratiques relatives aux renseignements personnels sont conformes à la norme de l'industrie (nationale ou régionale), ainsi qu'aux normes et processus de sécurité des technologies de l'information adéquats pour le niveau de sensibilité des renseignements personnels sur la santé à protéger?
- Avez-vous mis en place des garanties physiques raisonnables, telles que des armoires fermées à clé et l'utilisation de cartes d'accès pour contrôler l'entrée aux zones d'entreposage qui contiennent des renseignements personnels sur la santé?
- Avez-vous mis en place des garanties administratives raisonnables, telles que des contrôles de références, des formations obligatoires pour les employés et des politiques de protection de la vie privée et de sécurité appropriées afin de protéger les renseignements personnels sur la santé contre les risques tels l'accès non autorisé, l'utilisation, la communication, ou la modification?

- Avez-vous mis en place des garanties techniques raisonnables, telles que le cryptage approprié des renseignements personnels sur la santé, des mots de passe difficiles à identifier, une protection antivirus et des pare-feu afin d'empêcher l'accès non autorisé aux renseignements personnels sur la santé, leur utilisation, leur communication ou leur modification?
- Les politiques et les procédures décrites ci-dessus sont-elles conçues pour protéger les renseignements sous toutes leurs formes, y compris, sans s'y limiter, les documents papier; les dossiers électroniques, y compris les bases de données, les courriels, les formulaires électroniques; et les microfilms ou les microfiches?

5.2. Conservation, entreposage et destruction sécuritaire (Article 55)

Oui **Non**

- Disposez-vous de politiques écrites relatives à l'accès aux renseignements personnels sur la santé sous votre garde ou votre contrôle, ainsi qu'à leur conservation, leur archivage et leur destruction sécuritaire?
- Vos procédures existantes permettent-elles la conformité avec ces politiques?
- Les politiques de conservation se conforment-elles à des prescriptions de la loi?
- Les politiques ci-dessus s'appliquent-elles à tous les formats de document (par exemple, aux documents papier, aux bases de données électroniques, aux courriels et aux microfilms ou aux microfiches), quel que soit le support?
- Existe-t-il des politiques ou des procédures qui garantissent que les renseignements personnels sur la santé sont détruits de façon sécuritaire lorsqu'ils ne sont plus requis? *(Les politiques doivent réduire les risques, tels que le rejet de dossiers contenant des renseignements personnels sur la santé dans une poubelle ou des dossiers électroniques partiellement supprimés sur un disque dur vendu à des fins de récupération.)*
- Disposez-vous d'un système et d'un processus officiels/sûrs pour sauvegarder les données électroniques contenues dans tous les systèmes informatiques qui stockent des renseignements personnels sur la santé?
- Les bandes de sauvegarde sont-elles entreposées de façon sécuritaire et correctement détruites une fois qu'elles ont atteint la fin de leur durée de vie utile?
- Vous assurez-vous que des documents papier sont entreposés de façon sécuritaire dans un endroit où ils ne seront pas endommagés en cas d'inondation ou de dégât d'eau?
- Conservez-vous un dossier officiel sur le contenu de tous les documents comportant des renseignements personnels sur la santé détruits, en conformité avec la politique de conservation ou de destruction?
- Les renseignements personnels sur la santé sous la garde ou le contrôle de l'organisme entreposés à l'extérieur du Canada le sont-ils à des fins autorisées uniquement *(l'entreposage à l'extérieur du Canada n'est pas autorisé, sauf si la personne y a consenti ou si ce type d'entreposage est expressément autorisé aux termes de la Loi)?*

5.3. Information Management Service Provider agreements (Article 52)

Oui **Non**

- Avez-vous identifié tous les « gestionnaires de l'information » (par exemple les services de déchiquetage et les fournisseurs de services des TI) embauchés par votre organisme pour fournir des programmes et des services?

Avez-vous conclu avec tous les gestionnaires de l'information des accords par écrit comportant des clauses de protection de la vie privée et de sécurité appropriées, dont :

- une description de la manière dont les renseignements personnels sur la santé seront protégés contre les risques tels l'accès non autorisé aux renseignements ou l'utilisation, la communication, l'élimination ou la modification non sécuritaires de ces renseignements;
- l'obligation du gestionnaire de l'information à se conformer à la *LAPRPS* et ses règlements;
- l'exigence pour les gestionnaires de l'information de ne pas entreposer des renseignements personnels sur la santé à l'extérieur du Canada, sauf s'ils fournissent l'entretien et le soutien technique pour les systèmes de renseignements personnels sur la santé ou sauf disposition contraire de la *Loi*.

5.4. Devoir de collecte de renseignements exacts (Article 53)

Oui Non

Prenez-vous des mesures raisonnables pour garantir que les renseignements personnels sur la santé que vous recueillez sont exacts et complets?

6. Collecte, utilisation et communication

6.1. Limites relatives à la collecte (Article 29)

Oui Non

Prenez-vous des mesures pour limiter le nombre de renseignements personnels sur la santé recueillis, utilisés ou communiqués au strict nécessaire pour réaliser la fin visée par la collecte, l'utilisation ou la communication?

Utilisez-vous ou communiquez-vous des renseignements personnels sur la santé anonymisés, s'ils peuvent servir au même titre que les renseignements identifiables?

6.2. Mode de collecte (Article 28)

Oui Non

Recueillez-vous les renseignements personnels sur la santé seulement directement auprès de la personne concernée par ces renseignements?

Si des renseignements personnels sur la santé sont recueillis indirectement à partir d'autres sources, la personne a-t-elle autorisé un autre mode de collecte ou la collecte est-elle autorisée en vertu des exceptions énoncées dans l'article 28 de la *Loi*?

Lorsque vous recueillez des renseignements personnels sur la santé à partir d'autres sources, prenez-vous des mesures raisonnables pour vérifier l'exactitude des renseignements?

6.3. Restrictions quant à l'utilisation et à la communication des renseignements (Articles 32-45)

Oui Non

Disposez-vous de politiques ou de procédures visant à limiter l'utilisation et la communication de renseignements personnels sur la santé au minimum nécessaire pour réaliser la fin visée par l'utilisation ou la communication?

- Disposez-vous de politiques ou de procédures visant à restreindre l'accès aux renseignements personnels sur la santé d'une personne ou leur communication par des « mandataires », tels que des employés, des bénévoles et d'autres personnes qui n'ont pas besoin de connaître les renseignements dans le cadre de leur emploi?
- Les personnes ont-elles donné leur consentement pour chaque utilisation des renseignements personnels sur la santé qui les concernent?
- Si vous n'avez pas toujours obtenu le consentement pour l'utilisation des renseignements personnels sur la santé d'une personne, l'utilisation satisfait-elle l'un des critères présentés dans l'article 34 de la *Loi*?
- Prenez-vous des mesures pour vous assurer que le consentement est obtenu avant la communication de renseignements personnels sur la santé, sauf si cette communication est précisément autorisée par la *Loi*?
- Si vous n'avez pas obtenu le consentement pour la communication des renseignements personnels sur la santé d'une personne, la raison de la communication est-elle l'une des circonstances décrites dans l'article 37 (6) et dans les articles 38 à 45 de la *Loi*? (*Ces articles autorisent une communication limitée sans consentement.*)
- Informez-vous les non-dépositaires (comme les gestionnaires de l'information) qu'ils ne peuvent utiliser les renseignements personnels sur la santé qu'aux fins pour lesquelles vous les leur communiquez et pour aucune autre raison, sauf lorsque cela est permis par la *Loi*?
- Disposez-vous d'une politique exigeant que les renseignements personnels sur la santé soient anonymisés dans les cas où le consentement pour l'utilisation ou la communication des renseignements n'a pu être obtenu et que l'utilisation et la communication des renseignements personnels sur la santé ne sont pas autorisés par la *Loi*?
- Dans le cas où des renseignements anonymisés seront utilisés ou communiqués, des procédures sont-elles en place pour garantir que les renseignements ne pourront raisonnablement pas être utilisés seuls ou combinés à d'autres renseignements pour identifier à nouveau une personne ou des personnes dont les renseignements personnels sur la santé se trouvent dans l'ensemble de données?

6.4. Utilisation ou communication à des fins de recherche (Article 43)

Oui **Non**

- Des renseignements personnels sur la santé seront-ils utilisés ou communiqués à des fins de recherche?
- S'il est prévu d'utiliser ou de communiquer des renseignements personnels sur la santé à des fins de recherche, le projet a-t-il été approuvé par un comité d'examen de la recherche autorisé qui satisfait à toutes les exigences de la *Loi*?

7. Autres éléments à prendre en considération – pratiques générales de protection de la vie privée

7.1. Responsabilité à l'égard de la protection de la vie privée

Oui **Non**

- Avez-vous désigné une ou plusieurs personnes qui seront chargées de mettre en place et de superviser la conformité à la *LAPRPS*? (*Les personnes doivent être correctement formées et recevoir les ressources adéquates pour faire le travail.*)

7.2. Politique de protection de la vie privée – élaboration et conformité

Oui Non

- Disposez-vous au sein de votre organisation d'une politique de protection de la vie privée écrite visant à garantir la conformité avec la *Loi*?
- Les employés et les entrepreneurs connaissent-ils la politique de protection de la vie privée et leur rappelle-t-on régulièrement leurs responsabilités à l'égard du respect de cette politique?
- Les employés et les entrepreneurs sont-ils tenus de signer des accords de confidentialité qui comportent par écrit l'exigence de conformité avec la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* et les politiques de protection de la vie privée de l'organisme?
- Des procédures sont-elles en place pour contrôler et garantir le respect par les mandataires (par exemple les employés, les entrepreneurs et les bénévoles) des politiques de protection de la vie privée et de sécurité de l'organisme?

7.3 Avis sur la protection de la vie privée

Oui Non

- Avez-vous élaboré un avis sur la protection de la vie privée propre à votre organisme affiché publiquement qui fournira raisonnablement un avis aux personnes concernant les pratiques de protection de la vie privée de votre organisme?

(Un avis sur la protection de la vie privée peut être mis à disposition, par exemple sur le site Web de l'organisme ou intégré sur des affiches et des brochures, ou encore au moyen d'un enregistrement vocal). Un avis sur la protection de la vie privée est un outil de communication différent de la politique de protection de la vie privée de l'organisme (tout en étant cohérent avec cette politique). L'avis sur la protection de la vie privée est un document interne qui présente les responsabilités des employés et des mandataires à l'égard de la vie privée dans le cadre de la loi.

- Avez-vous examiné les formulaires, demandes et autres documents de l'organisme utilisés pour recueillir des renseignements personnels sur la santé afin de garantir que les personnes sont correctement informées des fins visées au moment de la collecte des renseignements? Cela peut être réalisé en intégrant une explication des objectifs directement dans les formulaires ou par un bref énoncé expliquant comment la personne peut obtenir une copie de l'avis sur la protection de la vie privée ou en savoir plus sur la fin visée par la collecte.

7.4. Formation et sensibilisation à la protection de la vie privée

Oui Non

- Avez-vous mis en place un plan pour fournir régulièrement des formations obligatoires à tous les employés et entrepreneurs, afin de renforcer leurs obligations dans le cadre de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* et des politiques de protection de la vie privée de l'organisme?
- Avez-vous mis en place un plan destiné à communiquer aux employés les politiques de protection de la vie privée de l'organisme et à aider les employés ou les directeurs à élaborer des procédures qui assurent l'harmonisation avec les politiques?

7.5. Inventaire en matière de protection de la vie privée et analyse de l'écart

Oui Non

- Avez-vous effectué un inventaire des renseignements que possède votre organisme et déterminé les différents objectifs pour lesquels vous recueillez, utilisez et communiquez des renseignements personnels sur la santé?
- Avez-vous effectué une analyse de l'écart basée sur l'inventaire afin de déterminer les domaines à risque et les domaines de non-conformité?

7.6. Enquête sur les incidents et les atteintes à la protection de la vie privée

Oui Non

- Disposez-vous d'un processus pour recevoir et enquêter en temps opportun des plaintes en matière de protection de la vie privée?
- Avez-vous élaboré une politique et des procédures d'intervention en cas d'incident relatif à la protection de la vie privée afin de gérer et de maîtriser une atteinte à la protection de la vie privée, s'il devait s'en produire une?
- Avez-vous élaboré un processus visant à signaler les atteintes à la vie privée aux personnes concernées et au Commissaire à l'accès à l'information et à la protection de la vie privée?