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

La présente liste de contrôle vise à aider les dépositaires à déterminer certaines des mesures clés dont ils peuvent se prévaloir pour 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 (LAPRPS)*. Il ne s'agit que d'un guide; elle ne doit pas être considérée comme un avis juridique. On encourage les dépositaires à consulter la *LAPRPS* et ses règlements pour connaître l'énoncé complet de la *Loi*. Ils souhaiteront peut-être également avoir recours à des conseils professionnels afin d'évaluer davantage leur conformité avec la *LAPRPS*.

√ Désigner quelqu'un pour superviser la conformité avec la *LAPRPS*

Désigner une personne chargée de garantir la conformité générale avec la LAPRPS, y compris :

- √ d'assurer l'élaboration et la mise en place des politiques et des procédures appropriées relatives à la protection de la vie privée;
- √ de contrôler la conformité avec les politiques relatives à la protection de la vie privée de l'organisme;
- √ d'informer les employés et les autres mandataires sur la protection de la vie privée et la sécurité;
- √ de s'assurer que les accords écrits adéquats avec les tierces parties et les gestionnaires de l'information sont en place;
- √ de répondre aux demandes de renseignement et aux préoccupations relatives à la manière dont les renseignements personnels sur la santé (RPS) sont gérés.

√ Examiner et évaluer les pratiques de manipulation de l'information et contrer les risques

Examiner

- √ Créer un inventaire de tous les RPS recueillis, utilisés, communiqués, conservés et détruits.
- √ Déterminer les besoins en renseignements des différents programmes et fonctions au sein de l'organisme.
- √ Repérer les pratiques actuelles relatives aux renseignements (y compris pourquoi et comment les RPS sont recueillis, utilisés, conservés, communiqués et détruits).

Évaluer

- √ Examiner si les pratiques de manipulation de l'information sont conformes aux obligations posées par la *LAPRPS*.
- √ Déterminer et évaluer les risques liés à la protection de la vie privée posés par les pratiques actuelles relatives aux renseignements.

Contrer

- √ Élaborer un plan visant à combler les lacunes, en commençant par les secteurs dont le risque est le plus élevé.
- √ Examiner quelles modifications pourraient être apportées aux politiques et aux pratiques et déterminer si de nouvelles sont requises.
- √ Examiner si les mesures de sécurité (contrôles techniques, physiques ou administratifs) sont adéquates par rapport au niveau des risques d'atteinte à la protection de la vie privée.

√ Élaborer ou mettre à jour les politiques relatives aux renseignements de l'organisme, y compris :

- √ les politiques relatives à la protection de la vie privée (qui concernent la collecte, l'utilisation, la communication, l'accès et la correction, le traitement des plaintes, la gestion du consentement, les mesures de protection, la conservation, l'élimination et l'exactitude);

- √ les politiques de sécurité (qui garantissent que les normes de sécurité des TI conviennent au degré de sensibilité des renseignements protégés et qu'elles sont conformes aux normes de sécurité des meilleures pratiques);
- √ les politiques de conservation;
- √ les politiques d'accès à l'intention des utilisateurs (la manière dont l'accès des utilisateurs aux RPS sera accordé, contrôlé et retiré);
- √ les politiques et les procédures de destruction sécuritaire des RPS;
- √ les politiques et les procédures d'intervention en cas d'avis d'infraction ou d'incident;
- √ les politiques relatives à l'accès aux RPS et à leur correction.

√ Promouvoir et contrôler la conformité du personnel et des tierces parties au moyen de politiques

- √ Informer le personnel et les tierces parties de leur obligation de se conformer aux politiques relatives aux renseignements ainsi qu'à la *LAPRPS* et de la manière dont cela se concrétise dans leur travail quotidien.
- √ Exiger de tous les nouveaux employés et de toutes les nouvelles tierces parties qu'ils suivent une formation obligatoire sur la protection de la vie privée et la sécurité avant qu'ils aient accès aux RPS.
- √ Exiger des employés et des tierces parties qu'ils signent un accord de confidentialité qui les contraint à se conformer à la *LAPRPS* et aux politiques de protection de la vie privée et de sécurité de l'organisme.
- √ Exiger des employés et des tierces parties qu'ils examinent et approuvent chaque année leur conformité avec les politiques de protection de la vie privée et de sécurité de l'organisme.
- √ Mettre en place des processus assurant le contrôle régulier de la conformité du système et du programme avec la *LAPRPS*.

√ Établir ou réviser les avis sur la protection des renseignements personnels, les formulaires et les documents de communication

- √ Préparer un avis sur la protection de la vie privée afin d'informer les patients ou les clients de vos pratiques en matière de protection de la vie privée.
- √ Rendre l'avis disponible ou visible pour toutes les personnes au moment de la collecte de leurs renseignements. Par exemple sur le site Web de l'organisation, sur des affiches, des brochures, des dépliants, etc.
- √ Réviser les formulaires utilisés pour recueillir des RPS pour garantir que les personnes sont bien informées des pratiques relatives aux renseignements de l'organisme ou orientées vers l'avis sur la protection de la vie privée.

√ Examiner et réviser les contrats et les accords pour se conformer à la *LAPRPS*

- √ Identifier les « gestionnaires de l'information » (par exemple les services de déchiquetage, les fournisseurs de services des TI, les organismes de services gouvernementaux) qui traitent les RPS en votre nom.
- √ Mettre à jour ou créer avec les gestionnaires de l'information des accords ou des contrats écrits qui décrivent :
  - √ l'objectif pour lequel ils sont autorisés à utiliser des RPS et qui interdisent d'autres utilisations ou communications;
  - √ la manière dont les RPS doivent être protégés lorsqu'ils sont sous leur garde ou leur contrôle;
  - √ le cas échéant, comment sont détruits les RPS de manière sécuritaire et sans compromettre la confidentialité des renseignements;
  - √ l'obligation du gestionnaire de l'information à se conformer à la *Loi* et ses règlements;
  - √ les restrictions relatives au stockage de RPS en dehors du Canada (sous réserve de certaines exceptions).

√ Créer un processus efficace pour le traitement des incidents et des atteintes à la protection de la vie privée

- √ Élaborer des procédures pour recevoir les plaintes relatives aux pratiques de protection de la vie privée et pour y répondre.
- √ Élaborer des procédures pour enquêter sur les préoccupations concernant la protection de la vie privée et sur les incidents au sein de votre organisation et pour répondre aux atteintes à la protection de la vie privée et les déclarer de manière appropriée.

- √ Élaborer des procédures visant à informer les personnes dont la privée a été transgressée, y compris les échéanciers et la méthodologie.
- √ Élaborer des moyens de suivre de près les atteintes à la protection de la vie privé, graves ou non, afin d'améliorer de façon soutenue les mesures de sécurité mises en place dans le but de prévenir d'autres violations.

√ Être prêt à répondre aux demandes d'accès et de correction par des personnes

- √ Définir et publier, dans l'avis sur la protection de la vie privée de l'organisme et dans ses politiques, la manière dont les personnes peuvent obtenir l'accès à leurs RPS et demander qu'on les corrige.
- √ Créer des procédures pour accorder l'accès aux dossiers ou autoriser les corrections, qui définissent notamment les personnes à qui les demandes sont adressées, le moment du transfert des demandes, les frais qui s'appliquent, la vérification de l'identité et la manière dont les mentions de désaccord seront obtenues et consignées.

√ Élaborer et documenter un processus de gestion du consentement

- √ Déterminer les modèles de consentement qui s'appliquent. Documenter à quel moment le consentement éclairé s'appliquera, quand il faudra obtenir un consentement explicite, et les circonstances, s'il y en a, qui permettent de recueillir, d'utiliser ou de communiquer des renseignements sans consentement.
- √ Si des renseignements sont communiqués sans consentement, s'assurer que la nature des renseignements communiqués est documentée de façon adéquate, comme le prescrit la *Loi*.
- √ Concevoir des procédures visant à permettre aux personnes de communiquer leurs directives en matière de consentement. Présenter de quelle manière de telles directives seront gérées, notamment quand il sera nécessaire d'outrepasser une directive en matière de consentement et de quelle manière ces cas seront documentés et surveillés.

√ Revoir la *LAPRPS* afin de repérer d'autres dispositions qui pourraient s'appliquer, comme :

- √ les restrictions en matière de collecte et d'utilisation du numéro d'Assurance-maladie;
- √ l'exigence pour les organismes publics d'effectuer une évaluation des facteurs relatifs à la vie privée (EFVP);
- √ les règles qui s'appliquent aux dépositaires qui créent un réseau d'information ou qui agissent au sein d'un tel réseau;
- √ la cessation d'activité d'un dépositaire;
- √ les mandataires spéciaux et l'exercice des droits par un représentant personnel;
- √ l'utilisation et la communication des RPS aux fins de recherche.