

**LOI 25 : LOI MODERNISANT DES
DISPOSITIONS LEGISLATIVES EN
MATIERE DE PROTECTION DES
RENSEIGNEMENTS PERSONNELS**

Politiques et pratiques encadrant la gouvernance des renseignements personnels

Réseau Infirmia

725 boul. Lebourgneuf
Québec, G2J 0C4

1-877-345-7646
info@infirmia.com



infirmia

Loi 25

ADOPTION ET ENTRÉE EN VIGUEUR

En septembre 2021, la loi modernisant des dispositions législatives en matière de protection des renseignements personnels, aussi appelée Loi 25, a été adoptée. Son entrée en vigueur qui a débutée le 22 septembre 2022, s'effectuera en 3 phases, dont les deux dernières seront prévues en septembre 2023 et 2024.

PRÉAMBULE

Dans le cadre de ses activités en tant que cliniques de soins infirmiers privés de première ligne, le Réseau Infirmia et ses cliniques affiliées recueillent et utilisent des renseignements personnels. En tant qu'établissement de santé, Infirmia est responsable d'assurer la protection des renseignements personnels de ses clients et fournisseurs, selon les responsabilités légales en vigueur. La direction a nommé une personne responsable de la protection des renseignements personnels, qui veille à ce que les procédures soient mises en place dans toutes les cliniques du Réseau Infirmia, et qui s'assure de recueillir et d'adresser toutes plaintes reçues à cet effet.

OBJECTIFS DE LA LOI 25

L'adoption de cette loi vise à responsabiliser les personnes, organisations et entreprises qui détiennent des renseignements personnels, dont les infirmiers et infirmières font partie. Elle dicte de nouvelles mesures concrètes à mettre en place au sein de l'organisation.

Ainsi, tous les infirmiers et infirmières œuvrant au sein du Réseau Infirmia et de l'une ou l'autre de ses entités doivent y porter une attention particulière et s'y conformer.

CHAMPS D'APPLICATION

La présente politique s'applique à tous les membres et employés de l'ensemble du Réseau Infirmia lorsqu'ils recueillent, utilisent, communiquent, conservent ou détruisent des renseignements personnels dans le cadre de leurs fonctions. Elle s'applique à tous les renseignements, quel que soit leur format (papier, numérique, web, etc.), de leur collecte à leur destruction.

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Depuis le 22 septembre 2022, toute personne qui exploite une entreprise est **responsable de la protection des renseignements personnels** qu'elle **détient**. Pour ce faire, la personne ayant la plus haute autorité devra veiller à assurer le respect et la mise en œuvre de la Loi sur le privé.

La loi prévoit que cette personne exercera la fonction de responsable de la protection des renseignements personnels, mais qu'elle pourra déléguer cette fonction par écrit, en tout ou en partie, à toute personne.

Le titre et les coordonnées du responsable devront être publiés sur le site Internet de l'entreprise ou, si elle n'a pas de site, rendus accessibles par tout autre moyen approprié.

RÉSEAU INFIRMIA

Responsable de la protection des RP :

Nom, prénom : _Isabelle Lechasseur____

Titre : _Présidente____

Téléphone : _418-622-0660____

Courriel : _info@infirmia.com__

Personne déléguée par la responsable de la protection des RP :

Nom, prénom : __Jessica Lamontagne_

Titre : _Directrice des services professionnels et développement clinique__

Téléphone : _418-622-0660__

Courriel : __jlamontagne@infirmia.com__

Le nom du responsable ou de la personne déléguée, ainsi que ses coordonnées, sont diffusés sur le site web de l'organisation. Également, les règles encadrant la gestion des renseignements personnels y sont détaillées.

RÈGLES ENCADRANT LA GESTION DES RENSEIGNEMENTS PERSONNELS

- **Rôles et responsabilités des membres du personnel**

Le Réseau Infirmia est responsable des renseignements personnels qu'il détient, incluant ceux dont la collecte, l'utilisation, la conservation ou la destruction est assurée par un tiers. Puis, chaque membre du personnel œuvrant au sein du Réseau Infirmia ou de l'une de ses entités à l'obligation de tenir informé le responsable de la PRP ou son délégué de tout incident en matière de protection des renseignements personnel qui serait porté à sa connaissance, dans un délai de moins de 24 heures.

- **Processus de traitement des plaintes en matière de PRP**

Toute plainte en matière de PRP, qu'elle provienne d'une ressource interne ou externe, fera l'objet d'une analyse sérieuse par le délégué à la protection des renseignements personnels ou par le plus haut responsable. Elle sera traitée et communiquée à qui de droit, tel que cela est décrit dans la Loi 25. Également, l'analyse d'une plainte visera l'élaboration d'un plan correctif immédiat afin de permettre une protection des renseignements personnels sans faille au sein de l'organisation.

- **Description des activités de formation que l'organisme offre à son personnel en matière de PRP**

La personne déléguée par le responsable en matière de protection des renseignements personnels a suivi la formation intitulée *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, offert par la Commission d'accès à l'information du Québec. Également, tous les membres du personnel sont formés par ces responsables ci-haut nommés. Finalement, tous les infirmiers et infirmières, membres de l'OIIQ, et les infirmiers et infirmières auxiliaires, membres de l'OIIAQ, sont tenus de se conformer et d'appliquer le code de déontologie de leur ordre professionnel respectif dans le cadre de leur pratique. Ce code de déontologie de l'OIIQ, selon le Code des professions du Québec, énonce ce qui suit :

« **31.** L'infirmière ou l'infirmier doit respecter les règles prévues au Code des professions (chapitre C-26) relativement au secret qu'il doit préserver quant aux renseignements de nature confidentielle qui viennent à sa connaissance dans l'exercice de sa profession et des cas où il peut être relevé de ce secret. »¹

¹ *Legis Québec, Code de déontologie des infirmières et infirmiers du Québec, Code des professions, Article 31.*

- **Les mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage ou d'une cueillette de données, ou à des fins d'études, de recherches ou de production statistiques**

Dans le cadre de tout sondage effectué dans l'entreprise, les énoncés suivants s'appliquent :

- Toutes les informations recueillies seront soumises à des mesures de sécurité afin d'assurer la conservation de leur caractère confidentiel
- Les mesures seront prises afin que les renseignements ne soient accessibles qu'aux seules personnes qui en ont besoin dans le cadre de leurs fonctions
- Les renseignements ne seront utilisés qu'aux seules fins pour lesquels ils ont été recueillis, soit à des fins de recherches, d'évaluation, de dossier médicaux.
- Toutes les informations recueillies seront détruites tel que requis à la fin du sondage.

RENSEIGNEMENTS PERSONNELS ET PROTECTION

- **Qu'est-ce qu'un renseignement personnel**

Les **renseignements personnels** sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exceptions, ils ne peuvent être communiqués sans le consentement de la personne concernée.

Les renseignements personnels doivent être protégés peu importe la nature de leur support et quelle que soit leur forme : écrite, graphique, audio, visuelle, informatisée ou autre.

- **Responsabilités**

Une entreprise qui recueille, utilise, communique à des tiers, conserve ou détruit des renseignements personnels a plusieurs obligations à respecter en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé).

VOS RENSEIGNEMENTS PERSONNELS : LE PROCESSUS

❖ La collecte

Première étape du cycle de vie du renseignement personnel, la collecte est le moment où le renseignement personnel est :

- Recueilli (ex. : formulaire d'abonnement, sondage, outils analytiques Web) ;
- Créé (ex. : n° de membre ou de permis de conduire) ;
- Inféré (ex. : profil de consommateur), c'est-à-dire déduit à partir d'autres renseignements.

Le fait de visualiser un renseignement personnel, comme ceux contenus sur une pièce d'identité, constitue également une collecte, même s'il n'y a pas de conservation par la suite.

Ainsi, dans le Réseau Infirmia, les obligations suivantes sont respectées afin de protéger les renseignements personnels :

- **Déterminer les fins de la collecte** : un intérêt sérieux et légitime doit motiver la constitution d'un dossier sur une personne ;
- **Limitier la collecte de renseignements personnels** : la collecte doit se limiter aux renseignements nécessaires aux fins déterminées. En cas de doute, un renseignement personnel est réputé non nécessaire ;
- **Recueillir les renseignements personnels** par des **moyens légaux et légitimes** : sauf exception, la collecte doit se faire **auprès de la personne concernée** ;
- **Informier la personne concernée**, avant de constituer un dossier :
 - De l'objet du dossier ;
 - De l'utilisation qui sera faite des renseignements personnels ;
 - Des catégories de personnes qui y auront accès au sein de l'entreprise ;
 - De l'endroit où ils seront détenus ;
 - De ses droits d'accès et de rectification.
- **Obtenir le consentement des personnes concernées** avant de collecter leurs renseignements personnels auprès d'un tiers, à moins d'une exception prévue par la loi.

*MINEURS : À compter du 22 septembre 2023, les renseignements personnels concernant un **mineur de moins de 14 ans** ne pourront plus être recueillis auprès de celui-ci sans le consentement du titulaire de l'autorité parentale ou du tuteur, sauf lorsque cette collecte sera manifestement au bénéfice de ce mineur.

❖ L'objectif de la collecte de données

Dans nos cliniques, la collecte de vos données est principalement de nature démographique. Elle a pour but unique de constituer un dossier de santé, strictement confidentiel, dans lequel des informations concernant vos

consultations, vos prélèvements et votre état de santé y sont consignées. Cette collecte permet la tenue de dossier et ainsi, facilite la continuité des soins qui vous sont offerts.

❖ Le consentement

Lorsque nous obtenons de l'information vous concernant, nous demandons en premier lieu votre consentement par écrit à la collecte, à l'utilisation ou à la divulgation de vos renseignements recueillis pour les fins indiquées, lors de votre première visite en clinique. Ce consentement est valide ensuite pour toute la durée où vos données et votre dossier seront conservés. Vous pouvez toutefois retirer votre consentement à tout moment. Nous solliciterons votre consentement lors de toute autre utilisation, divulgation ou collecte de vos renseignements personnels (transfert de clinique, envoi de résultats à un tiers, etc.)

Le Réseau Infirmia s'engage à utiliser les renseignements fournis uniquement aux fins pour lesquelles ils ont été recueillis.

❖ L'utilisation

L'utilisation est la période où le renseignement personnel est utilisé par les personnes autorisées au sein de l'entreprise. À cette étape, les membres du Réseau Infirmia doivent respecter les obligations suivantes :

- **Limitier l'accès aux renseignements personnels** aux seules personnes ayant la qualité pour les recevoir au sein de l'entreprise lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions ;
- **Limitier l'utilisation des renseignements personnels** : à moins d'une exception prévue par la loi, l'entreprise doit **obtenir le consentement de la personne concernée** pour utiliser ses renseignements une fois l'objet du dossier accompli.

Également, le Réseau Infirmia **s'assure** que les renseignements personnels qu'il détient sont à jour, exacts et complets tant qu'ils sont utilisés.

❖ La communication

La communication est la période où le renseignement personnel est communiqué, par exemple dans un système de prestation électronique de services, par courriel, au service à la clientèle, par le biais de sites Web ou à un tiers.

À cette étape, l'entreprise respecte les obligations suivantes :

- **Obtenir le consentement des personnes concernées** pour communiquer leurs renseignements à un tiers (ex. : prestataire de services, autre professionnel de la santé, etc.), à moins d'une exception prévue par la loi;
- **Respecter** les obligations prévues par la loi lorsqu'elle communique des renseignements personnels sans le consentement de la personne concernée;
- **Respecter** les obligations particulières applicables à la communication de renseignements personnels à l'extérieur du Québec. Ainsi, un consentement doit être signé, identifiant les risques associés à la confidentialité lors d'une communication de renseignements personnels à l'extérieur du Québec.

❖ La conservation

La conservation est la période durant laquelle une entreprise garde des renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

À cette étape, le Réseau Infirmia s'assure de respecter les obligations suivantes :

- **Assurer la qualité des renseignements personnels** en veillant à ce que les renseignements personnels qu'elle détient soient **à jour et exacts** au moment où elle les utilise.
- **Prendre des mesures de sécurité propres à assurer la sécurité des renseignements personnels.** En effet, toutes informations recueillies sont conservées de manière confidentielle en format papier ou électronique. Nous avons mis en place et continuons à élaborer des mesures de sécurité rigoureuses afin que vos renseignements personnels demeurent strictement confidentiels et soient protégés contre la perte ou le vol et contre tout accès, communication, copie, utilisation ou modification non autorisée. Ces mesures de sécurité sont, par exemple, l'utilisation de mots de passe uniques à chaque professionnel, le changement fréquent de mots de passe, l'utilisation d'un service anti-virus mis à jour régulièrement, etc.
- **Seuls les professionnels habilités et qui en ont l'autorisation peuvent accéder aux renseignements personnels.** Ils sont tenus d'accéder seulement aux informations requises dans le cadre de leur travail, et de ne jamais partager ces informations sans le consentement préalable de la personne.

❖ La destruction

Le cycle de vie d'un renseignement personnel se termine lors de sa destruction.

À cette étape, l'entreprise doit **détruire les renseignements personnels de manière sécuritaire** dès que la finalité pour laquelle ils ont été collectés est accomplie. Tous les documents en format papier contenant des renseignements personnels sont détruits à l'aide d'une déchiqueteuse à découpe transversale. Tous les dossiers de santé de clients, conservés électroniquement sur un serveur, peuvent être détruits sur demande de l'entreprise, si aucune activité n'y a été rapporté dans les dix dernières années.

INCIDENTS DE CONFIDENTIALITÉ

○ Qu'est-ce qu'un incident de confidentialité?

Pour l'application des lois, un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

Par exemple, un incident de confidentialité pourrait se produire lorsque :

- Un membre du personnel consulte un renseignement personnel sans autorisation;
- Un membre du personnel communique des renseignements personnels au mauvais destinataire;
- L'organisation est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

Si l'entreprise a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel qu'elle détient s'est produit, elle doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Plainte

Le Réseau Infirmia, ainsi que toutes les entités qui le composent, répond avec diligence à toute plainte concernant sa gestion des renseignements qu'elle détient.

○ **Que faire lors d'un incident de confidentialité?**

1) Prendre des mesures pour diminuer les risques et éviter de nouveaux incidents

Si l'entreprise a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient, elle prendra des **mesures raisonnables** pour **diminuer les risques** qu'un préjudice soit causé et **éviter que de nouveaux incidents de même nature ne se produisent**.

2) Évaluer si l'incident présente un risque de préjudice sérieux

Pour tout incident de confidentialité, le Réseau Infirmia évaluera la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, notamment :

- La sensibilité des renseignements concernés ;
- Les conséquences appréhendées de leur utilisation ;
- La probabilité qu'ils soient utilisés à des fins préjudiciables.

Ensuite, l'entreprise consultera son responsable de la protection des renseignements personnels. Elle peut également impliquer d'autres acteurs, comme le responsable de la sécurité de l'information ou des experts externes.

Si l'analyse fait ressortir un risque de préjudice sérieux, l'organisation doit aviser la Commission et les personnes concernées de l'incident.

Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu'un incident de même nature se produise à nouveau dans le futur.

3) Aviser la Commission et les personnes dont les renseignements sont concernés

Lorsque l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes dont les renseignements sont concernés, l'entreprise doit aviser la Commission avec diligence.

L'entreprise avisera également toute personne dont les renseignements personnels sont concernés par l'incident. Dans le cas où l'organisation n'informe pas les personnes concernées, la Commission peut lui ordonner de le faire.

GESTION DES DONNÉES BIOMÉTRIQUES

Au sein du Réseau Infirmia, aucune donnée biométrique n'est utilisée ou conservée. Cette section ne s'applique donc pas à l'entreprise.

RÉVISION DE LA POLITIQUE

La présente politique est sous la responsabilité de la responsable de la protection des renseignements personnels, ainsi que de l'équipe de direction. Elle est révisée au besoin, mais au minimum tous les trois ans à compter de sa date d'adoption.

ENTRÉE EN VIGUEUR

La présente politique entre en vigueur lors de son adoption par l'équipe responsable.

Date : __22 septembre 2023__

SOURCES

Commission de l'accès à l'information

<https://www.cai.gouv.qc.ca/>

Loi 25 : Loi sur la protection des renseignements personnels dans le secteur privé.