Cadre de gouvernance à l'égard des renseignements personnels, de l'accès à l'information et de la sécurité de l'information

Résumé

Ce document établit les règles de gouvernance à l'égard des renseignements personnels détenus par l'Ordre professionnel des inhalothérapeutes du Québec, de l'accès à l'information et de la sécurité de l'information.

ORDRE PROFESSIONNEL DES INHALOTHÉRAPEUTES DU QUÉBEC

Table des matières

Lorsque possible, sans trop alourdir le texte, nous recourons en alternance aux procédés de rédaction épicène (formulation neutre, féminisation syntaxique) et au masculin générique, selon une approche recommandée par l'OQLF.

Ce document a été révisé et corrigé selon l'orthographe rectifiée de 1990 (aussi appelée « nouvelle orthographe recommandée »).

Préambule

Dans le cadre de ses activités, l'Ordre professionnel des inhalothérapeutes du Québec (ci-après « l'Ordre » et « l'OPIQ ») détient un ensemble d'actifs informationnels, incluant des renseignements personnels.

À titre d'ordre professionnel, l'OPIQ est assujetti à un régime hybride en matière d'accès aux documents et de protection de renseignements personnels (PRP). Le régime applicable varie en fonction de la teneur des documents et des renseignements personnels concernés.

L'Ordre est donc soumis, selon la mesure prévue par le *Code des professions*, tant à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la *Loi sur l'accès*) qu'à la *Loi sur la protection des renseignements personnels dans le secteur privé* (la *Loi sur le privé*), ainsi qu'aux règlements découlant de ces lois. En cas de divergence entre l'une de ces deux lois et le cadre de gouvernance, la loi prévaut.

L'OPIQ doit assurer la protection des renseignements personnels qu'il détient tout au long de leur cycle de vie. Il se porte aussi garant de la protection de ceux dont la collecte, l'utilisation, la conservation ou la destruction est réalisée par un tiers en son nom.

Cycle de vie d'un renseignement personnel

Avis au lectorat : le recours à la couleur bleu clair dans le présent document indique que le terme ou l'expression a une portée particulière qui peut différer du sens commun ou faire l'objet de précisions. Un mot ou une locution de cette couleur signale qu'on doit se référer aux définitions présentées dans le lexique.

Titre préliminaire

1. Objectifs

La protection des renseignements personnels et la sécurité de l'information sont intimement liées. Ce cadre de gouvernance vise à :

- Établir les principes directeurs qui guident les pratiques de l'OPIQ quant à sa gestion documentaire des renseignements personnels et la sécurité de l'ensemble de ses actifs informationnels ;
- Renforcer la gouvernance à l'égard de la protection des renseignements personnels détenus par l'Ordre ;
- Établir les rôles et responsabilités des membres du personnel et des tiers en matière de sécurité de l'information et de protection des renseignements personnels ;
- Atténuer les risques auxquels peuvent être exposés l'ensemble des actifs informationnels détenus par l'OPIQ ;
- Assurer la disponibilité, l'intégrité et la confidentialité à l'égard de l'utilisation des réseaux informatiques, d'Internet et de l'utilisation des actifs informationnels détenus par l'Ordre ;
- Faire preuve de transparence, afin de permettre aux personnes d'exercer les droits d'accès prévu par la loi et d'exercer un contrôle éclairé sur leurs renseignements personnels.

2. Portée

Ce cadre de gouvernance s'applique aux membres du personnel de l'OPIQ ainsi qu'aux tiers (avec les adaptations nécessaires), tels que définis à la section suivante.

Il n'a pas pour effet de diminuer ou de compromettre l'exercice des fonctions et responsabilités de l'Ordre découlant de la loi, notamment celles du comité d'inspection professionnelle et du bureau du syndic.

Enfin, ce cadre de gouvernance ne concerne pas les renseignements détenus par un membre du personnel à des fins personnelles, même s'ils sont conservés au siège social ou sur une plateforme technologique de l'OPIQ.

3. Lexique

Voici la définition des termes et locutions qui figurent dans le présent document :

Actif informationnel : ensemble des ressources informationnelles ayant une valeur pour la personne physique ou morale qui en est détentrice, et dont la protection nécessite la mise en place de mesures de sécurité particulières. L'actif informationnel peut notamment être de nature textuelle, graphique ou sonore, et comprend également les supports qui le contiennent[1]. Cette notion inclut les renseignements personnels.

Comité : à moins que le contexte n'indique un autre sens, fait référence au comité sur l'accès à l'information et à la protection des renseignements personnels de l'OPIQ.

Consentement : l'autorisation de la personne titulaire des renseignements personnels à recueillir, utiliser ou communiquer ses renseignements personnels. Le consentement ne se présume pas. Il doit être manifeste, libre, éclairé, transmis en termes simples et clairs, être donné à des fins spécifiques, et ne viser que la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé[2].

Évaluation des facteurs relatifs à la vie privée (EFVP) : démarche préventive pour mieux protéger les renseignements personnels et mieux respecter la vie privée des personnes physiques. Elle permet de considérer tous les facteurs qui auront un impact positif ou négatif sur le respect de la vie privée des personnes concernées. Ce processus vise d'abord à protéger les personnes physiques concernées par ces renseignements. Il vise aussi la mise en place de mesures adéquates pour respecter les obligations en matière de protection des renseignements personnels. Ainsi, l'EFVP permet d'éviter des problèmes que causerait une gestion inadéquate (plaintes, incidents de sécurité, poursuites judiciaires, atteinte à l'image, etc.)[3].

Membre du personnel : employé(e)s de la permanence de l'OPIQ, employé(e)s contractuels (membres de l'équipe d'inspection professionnelle et syndic[-que]s adjoint[e]s), membres du conseil d'administration, membres des comités.

Loi : l'ensemble des lois applicables aux ordres professionnels en matière de protection des renseignements personnels, soit : le *Code des professions*, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la *Loi sur l'accès*), la *Loi sur la protection des*

---

[1] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. (Màj 2022). *Entrée «actif informationnel»*. Grand dictionnaire terminologique, dans la Vitrine linguistique.
[2] Art. 53.1, LAI ; art. 14 LP.
[3] COMMISSION D'ACCÈS À L'INFORMATION. (MàJ 2023, 1er aout). *Évaluation des facteurs relatifs à la vie privée*.

renseignements personnels dans le secteur privé (la *Loi sur le privé*), de même que les règlements qui en découlent, le *Code civil du Québec* et la *Charte des droits et libertés de la personne*[4].

Personne responsable de l'accès et de la PRP : responsable de l'accès aux documents et de la protection des renseignements personnels au sein de l'OPIQ.

Renseignement personnel : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier[5].

Sécurité de l'information : ensemble de mesures mises en place pour assurer la protection des informations selon le niveau de confidentialité, d'intégrité et de disponibilité jugé nécessaire[6].

Tiers : une personne physique ou morale qui, en vertu d'un contrat ou d'un mandat, recueille, utilise, accède, conserve, communique ou détruit des renseignements personnels au nom de l'OPIQ ou qui assure autrement la gestion des renseignements personnels détenus par l'OPIQ.

Titre I – Nos engagements et responsabilités

Les pratiques de l'OPIQ en matière de protection des renseignements personnels reposent sur les engagements ci-après.

1. Consentement

Lorsque requis, un formulaire de consentement à la collecte, à l'utilisation ou à la divulgation des renseignements personnels est transmis aux personnes concernées. Si la demande de consentement est faite par écrit, elle est présentée distinctement de toute autre information communiquée à la personne concernée.

Même lorsqu'il est écrit, le consentement peut être retiré à tout moment en informant par écrit la personne responsable du projet ou responsable de l'accès et de la PRP. L'impact du retrait de son consentement est alors expliqué à la personne concernée afin de l'aider dans sa prise de décision.

---

[4] *Code des professions*, RLRQ c. C -26, art. 108.1 à 108,11 ; *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A -2.1 ; *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c. P -39.1 ; *Code civil du Québec*, RLRQ c. CCQ-1991 ; Charte des droits et libertés de la personne, RLRQ c. C -12, art. 5.

[5] Art. 54 et 55, LAI ; art. 2, LP.

[6] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. (MàJ 2021). *Entrée « sécurité de l'information ».* Grand dictionnaire terminologique, dans la Vitrine linguistique.

Communications sans le consentement de la personne concernée

Il pourrait arriver que l'Ordre communique des renseignements sans le consentement des personnes concernées. Toutefois, il ne le fera que lorsque la loi l'y autorise et seuls les renseignements nécessaires seront transmis.

2. Transparence

2.1. Collecte

L'OPIQ recueille uniquement les renseignements personnels nécessaires à la réalisation des fins poursuivies.

Au plus tard au moment où il recueille des renseignements personnels, l'OPIQ informe la personne concernée de ce qui suit :

- L'objectif de cette collecte de renseignements ;
- Les moyens utilisés pour les recueillir (p. ex. formulaire, captation vidéo)
- Le caractère obligatoire ou facultatif de la demande[7] ;
- Les conséquences pour la personne concernée (ou pour le tiers) d'un refus de répondre ou de consentir à la demande ou, si cela s'applique, d'un retrait de son consentement à la communication ou à l'utilisation des renseignements recueillis suivant une demande facultative ;
- Les droits d'accès et de rectification prévus par la loi ;
- La possibilité que les renseignements personnels soient communiqués à l'extérieur du Québec ou à des tiers, le cas échéant.

Si applicables, les informations suivantes seront aussi fournies :

- Nom du **tiers qui recueille les renseignements au nom de l'OPIQ :** par exemple, si une firme externe a été mandatée pour effectuer un sondage pour l'OPIQ, celle-ci doit s'identifier au moment de la collecte ;
- Nom du tiers ou des catégories de **tiers à qui il est nécessaire de communiquer les renseignements pour atteindre les objectifs justifiant la collecte :** par exemple, si une entreprise assiste l'OPIQ dans l'évaluation d'un programme et qu'elle doit recevoir certains renseignements, l'OPIQ la nommera. Si le contrat n'est pas encore signé, une catégorie plus générale sera indiquée ;
- **Possibilité** que les **renseignements soient communiqués à l'extérieur du Québec** :

[7] Une demande est obligatoire quand elle est directement liée à une attribution de l'OPIQ et qu'il ne pourrait offrir le service ou remplir ses fonctions sans recueillir le renseignement personnel.

par exemple, si l'OPIQ héberge les renseignements chez un fournisseur infonuagique en Ontario, l'OPIQ le mentionnera.

Sur demande, la personne concernée est également informée des renseignements personnels recueillis à son sujet, des catégories de personnes qui y ont accès au sein de l'OPIQ, de la durée de conservation de ces renseignements ainsi que des coordonnées de la personne responsable de l'accès et de la PRP.

À moins d'une exception prévue par la loi, l'OPIQ ne recueillera pas de renseignements personnels auprès d'un tiers sans le consentement de la personne concernée.

La collecte de renseignements à l'aide de certaines technologies

Le site web de l'OPIQ utilise des fichiers témoins et d'autres outils d'analyse (Google Analytic) qui enregistrent des données sur vos interactions avec le site. Les données restent complètement anonymes et n'ont pour but que d'améliorer le site en fonction des besoins de ses utilisateurs.

Un bandeau de notification avise la personne utilisatrice de l'utilisation de fichiers témoins et la réfère aux conditions d'utilisation et politique de confidentialité (site Web). Toutes les fonctions non-essentielles des outils d'analyse (ex. identification, localisation ou profilage) sont désactivées par défaut.

Quant aux médias sociaux, même si la personne utilisatrice consent à ces fonctions en acceptant d'utiliser ces plateformes, l'OPIQ l'informe de l'usage qu'il fait de ces données par l'entremise des règles d'utilisation des médias sociaux de l'OPIQ.

2.2. Utilisation

L'OPIQ fait usage des renseignements personnels recueillis aux seules fins précisées lors de la collecte, à moins que la personne concernée y consente ou que la loi autorise un usage différent.

Ainsi, en règle générale, l'OPIQ n'utilisera pas un renseignement pour un autre usage que celui pour lequel la personne concernée a consenti. Si une autre utilisation de ce même renseignement personnel s'avère nécessaire, un nouveau consentement sera sollicité.

2.3. Divulgation et communication

En principe, l'OPIQ obtient le consentement de la personne concernée pour communiquer ses renseignements personnels.

La loi prévoit cependant des exceptions, entre autres :

- L'OPIQ peut, sans le consentement de la personne concernée, communiquer un renseignement personnel lorsque cela est nécessaire pour l'exercice d'un mandat ou pour l'exécution d'un contrat de service ou d'entreprise — par exemple à des fournisseurs de services informatiques.

  Dans ce cas, le contrat est confié par écrit et prévoit des mesures de protection, notamment l'obligation pour le tiers de garder les renseignements personnels confidentiels, les utiliser uniquement aux fins pour lesquelles ils ont été divulgués et en assurer la destruction à la suite de l'exécution du contrat.

- L'OPIQ peut transmettre certains renseignements personnels à des fins d'étude, de recherche ou de production de statistiques, sous réserve des conditions prévues par la loi.

Dans certaines situations, la personne responsable de l'accès et de la PRP doit inscrire la communication dans le registre de communication des renseignements personnels.

2.4. Conservation et destruction

L'Ordre conserve les renseignements personnels qu'il détient aussi longtemps qu'il est nécessaire pour atteindre les fins pour lesquelles il les a collectés et selon son calendrier de conservation. Le tout, dans les limites autorisées par la loi ou pour se conformer aux exigences légales.

En règle générale, lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont terminées, l'Ordre le détruit de manière irréversible. Il pourrait également l'anonymiser pour l'employer à des fins d'intérêt public.

Cependant, ce sont les modalités de conservation et les destructions prévues au calendrier de conservation de l'Ordre qui s'appliquent lorsque le renseignement personnel est inclus dans un document visé par ce calendrier.

Lors de la destruction de documents, l'Ordre prend les mesures de protection nécessaires pour assurer la confidentialité des renseignements personnels. Il choisit la méthode de destruction adaptée à leur support et au niveau de confidentialité.

3. Sécurité

L'OPIQ met en place des mesures de protection appropriées et raisonnables afin de protéger les renseignements personnels collectés, utilisés, communiqués, conservés ou détruits.

L'Ordre s'assure du maintien des infrastructures technologiques et prend les mesures de protection pour assurer la sécurité des données, en tenant compte des risques liés aux technologies de l'information et à la cybersécurité.

Les mesures suivantes sont notamment instaurées :

- Protection des appareils électroniques par des mots de passe complexes et du réseau Internet par un pare-feu ;
- Accès à distance via un réseau privé virtuel (RPV/VPN) avec un système de double identification des usagers ;
- Signature d'ententes de confidentialité avec les membres du personnel et avec les tiers mandataires ;
- Politique de sécurité de l'information à laquelle tous les membres du personnel de l'OPIQ doivent se conformer ;
- La sécurité de l'information est intégrée et appliquée tout au long du processus qui mène à l'acquisition, au développement, à l'utilisation, à l'entretien, au remplacement ou à la destruction d'un actif informationnel ;
- Accès restreints aux actifs informationnels. L'attribution d'un accès aux membres du personnel s'effectue selon ce qui leur est strictement nécessaire pour l'exécution de leurs tâches.

Un plan de reprise permet à l'Ordre de reprendre ses activités lors d'un sinistre ou d'une défaillance majeure affectant les actifs informationnels jugés essentiels.

De plus, lorsque l'OPIQ partage des renseignements personnels avec un tiers, il prend les mesures de protection appropriées.

Activités de formation et de sensibilisation offertes aux membres du personnel

L'individu constitue un facteur crucial dans la protection de l'information puisqu'il la génère, la traite, la sauvegarde et doit, ultimement, en assurer la sécurité. Il importe donc de sensibiliser les membres du personnel ayant accès à des renseignements personnels[8] aux menaces et conséquences d'une atteinte à la sécurité.

[8]Les activités de formation sont offertes aux membres du personnel en fonction du type et des modalités de leur accès aux actifs informationnels. Par exemple, les membres de comités, qui n'ont qu'un accès limité et en lecture seule à des documents précis, ne sont pas tenus de suivre les programmes de formation en cybersécurité.

Par conséquent, ces personnes suivent, sur une base continue, des formations théoriques et pratiques pour les conscientiser aux enjeux de cybersécurité. Des activités de formation et de sensibilisation en matière de protection des renseignements personnels et plus spécifiquement, quant aux processus internes, sont aussi offertes aux membres du personnel.

4. Sondages

Dans le cadre de ses activités, l'OPIQ peut être appelé à effectuer des sondages à caractère facultatif. Ces derniers peuvent, par exemple, s'adresser aux inhalothérapeutes qui occupent un certain type d'emploi, afin d'obtenir un portrait contemporain des pratiques cliniques.

La réalisation — par ou pour le compte de l'OPIQ — d'un sondage, impliquant la collecte ou l'utilisation de renseignements personnels, est préalablement approuvée par la personne responsable de l'accès et de la PRP.

On effectue alors une évaluation des facteurs suivants :

1. la nécessité de recourir au sondage ;
2. l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

S'il y a lieu, on accompagne l'acceptation de la réalisation d'un sondage de recommandations quant à la gestion des renseignements recueillis, de son élaboration jusqu'à la destruction des renseignements personnels.

Situations exclues :

- Consultations obligatoires et questionnaires adressés aux inhalothérapeutes en vertu des lois professionnelles. Par exemple :
  - Questionnaire d'autoévaluation ;
  - Consultations liées à l'assemblée générale annuelle (AGA) ou à l'adoption d'un règlement portant sur l'exercice de la profession.

- Échanges courants à des fins sociales entre les membres du personnel de l'Ordre ou avec des partenaires aux fins de la planification ou de l'organisation du travail (confirmation de disponibilités, préférences pour certaines conditions ou modalités de réunions, etc.).

5. Incident de confidentialité

Un incident de confidentialité correspond à tout accès à un renseignement personnel, à son utilisation ou à une communication non autorisée par la loi, de même qu'à sa perte ou à toute autre atteinte à sa protection[9].

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

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

Lorsque l'OPIQ a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel qu'il détient s'est produit, il prend les mesures raisonnables pour réduire les risques d'éventuel préjudice et éviter que de nouveaux incidents de même nature se reproduisent.

Tout incident potentiel de confidentialité doit être immédiatement signalé au responsable de l'accès et de la PRP, qui assure sa gestion.

Si l'incident de confidentialité présente un risque de préjudice sérieux, la Commission d'accès à l'information en est informée avec diligence. Sauf les situations d'exception prévues par la loi, toute personne concernée par l'incident de confidentialité touchant un renseignement personnel est aussi informée.

Toute autre personne et tout organisme susceptible de diminuer ce risque peuvent également être avisés, sans le consentement de la personne concernée. Dans ce cas, seuls les renseignements personnels nécessaires sont communiqués et la communication est enregistrée par la personne responsable de l'accès et de la PRP.

L'OPIQ tient un registre des incidents de confidentialité, dont le contenu est déterminé par le *Règlement sur les incidents de confidentialité*.

[9] Art. 63.8, LAI ; art. 3.6 LP.

TITRE II – Rôles et responsabilités

L'efficacité des mesures de protection des renseignements personnels exige l'attribution claire de rôles et de responsabilités aux différents intervenants.

1. Direction générale

La direction générale dirige l'intégralité des activités de l'Ordre et assure une saine gestion des ressources humaines, matérielles et informationnelles. Elle s'assure que les orientations en matière de sécurité sont partagées par l'ensemble des membres du personnel.

Entre autres, elle :

- Veille à l'application du présent cadre de gouvernance;
- Informe les membres du personnel sur les obligations qui découlent des différentes politiques en vigueur au sein de l'OPIQ, obtient leur engagement quant au respect de ces politiques et prend les mesures administratives en cas de manquements;
- Planifie et assure la réalisation des activités de formation liées à la protection des renseignements personnels;
- Participe à l'évaluation des risques informationnels, la sélection du niveau de protection et l'élaboration des contrôles non informatiques;
- Détermine les règles d'accès aux actifs informationnels ;
- Approuve et assure l'application du calendrier de conservation des documents;
- Approuve les contrats liant l'OPIQ et s'assure notamment de l'inclusion des clauses de protection de renseignements personnels prévues par la loi.

2. Comité sur l'accès à l'information et à la protection des renseignements personnels (comité)

Le conseil d'administration a instauré un comité sur l'accès à l'information et à la protection des renseignements personnels afin de soutenir l'Ordre dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu des lois d'accès à l'information et de protection des renseignements personnels.

Il est composé des personnes suivantes :

- Responsable de l'accès et de la PRP;
- Responsable de la sécurité de l'information;
- Direction générale.

Le comité :

- Approuve la mise à jour de la politique de confidentialité et en assure la révision périodique;
- Approuve l'élaboration et la mise à jour du présent cadre de gouvernance et en assure la diffusion sur le site Web de l'OPIQ;
- Révise au besoin les processus de collecte, d'utilisation, de transmission, de conservation et de destruction des renseignements personnels;
- Agit comme équipe de gestion des incidents de confidentialité en appliquant le plan prévu à cet effet;
- Procède au processus d'évaluations des facteurs relatifs à la vie privée (EFVP) lorsque requis;
- Soutient les membres du personnel, incluant la direction générale et la personne responsable de l'accès et de la PRP, dans l'exercice de leurs responsabilités et dans l'exécution de leurs obligations;
- Approuve toute autre politique ou procédure liée à la protection des renseignements personnels.

3. Responsable de la protection des renseignements personnels

Par délégation de la personne titulaire de la présidence de l'OPIQ, la direction des affaires juridiques exerce les fonctions de responsable de l'accès et de la PRP à l'égard des affaires courantes de l'OPIQ[10].

La personne responsable du bureau du syndic agit aussi à titre de responsable de l'accès à l'information et de la protection des renseignements personnels à l'égard des documents et renseignements qu'elle obtient ou détient de même que de ceux qu'elle communique au sein de l'Ordre.

À cet effet, ces personnes :

- Reçoivent et traitent les demandes d'accès et de rectification en respect de la protection des renseignements personnels et de la confidentialité;
- Reçoivent les incidents de confidentialité et les transmettent au comité pour traitement;

[10]La personne titulaire de la présidence de l'OPIQ exerce les fonctions que la loi confère à la personne responsable de l'accès aux documents ou de la protection des renseignements personnels. Elle peut désigner un(e) membre du personnel de direction et lui déléguer toutes ses fonctions ou seulement une partie.

- Reçoivent les plaintes qui mettent en cause la protection des renseignements personnels et les transmettent au comité pour traitement;
- Approuvent la réalisation de sondages effectués au nom de l'OPIQ, qu'ils soient effectués à l'interne ou par une firme externe;
- Tiennent à jour le registre des communications de renseignements personnels et, en collaboration avec le comité, le registre des incidents de confidentialité.

4. Responsable des technologies de l'information (TI)

La personne responsable des technologies de l'information assure la sécurité de l'information et des services informatiques de l'OPIQ.

Plus précisément, elle :

- Assure la réalisation et la coordination des mesures informatiques de protection des renseignements personnels;
- Applique des mesures appropriées de réaction à toute menace et à tout incident de sécurité de l'information et de confidentialité lorsque les circonstances l'exigent, en vue d'assurer la sécurité de l'information et la protection des renseignements personnels en cause;
- Assure la gestion des accès aux documents sous format papier et informatique;
- Met en œuvre et assure le suivi de toute recommandation découlant d'une vérification ou d'un audit de sécurité;
- Participe à l'évaluation des risques, s'informe sur les menaces, les tendances et les options de sécurité.

5. Responsable de la gestion documentaire

La personne responsable de la gestion documentaire assure la gestion des documents et des archives de l'OPIQ.

Plus précisément, elle :

- Tient à jour la liste de classement des documents de manière à en permettre le repérage et l'inventaire des fichiers de renseignements personnels.

6. Membres du personnel

Les membres du personnel sont responsables d'appliquer et de respecter les politiques et procédures en vigueur au sein de l'OPIQ, incluant le présent cadre de gouvernance.

Ils(elle) assurent la protection des renseignements personnels et la sécurité de l'information dans ses activités professionnelles, de la collecte à la destruction.

Il(elle) doit notamment :

- Participer aux activités de formation en cybersécurité et protection des renseignements personnels offertes par l'OPIQ;
- Utiliser les ressources informationnelles en se limitant aux fins pour lesquelles elles sont destinées et à l'intérieur des accès autorisés;
- Assurer la sécurité des actifs informationnels et la protection des renseignements personnels détenus par l'Ordre conformément au cadre de gouvernance;
- Signaler immédiatement à la personne responsable des technologies de l'information toute situation susceptible de compromettre la sécurité des actifs informationnels;
- Signaler aussitôt à la personne responsable de l'accès et de la PRP tout incident de confidentialité dont il(elle) a connaissance;
- Transmettre toute demande d'accès à l'information ou de rectification des renseignements personnels ainsi que toute plainte concernant la protection des renseignements personnels au responsable de l'accès et de la PRP ;
- Restituer, s'il y a lieu, les systèmes et appareils électroniques que l'Ordre a mis à sa disposition;
- Respecter son serment ou son engagement de confidentialité;
- Faire approuver tout contrat ou entente liant l'OPIQ par la direction générale.

Titre III – Accès et rectification des renseignements personnels

Sur demande et sous réserve des exceptions prévues à la loi, toute personne a le droit d'accéder et de rectifier les renseignements personnels détenus à son sujet.De plus

De plus amples informations, ainsi que la marche à suivre (incluant les coordonnées de la personne responsable de l'accès et de la PRP) pour faire une demande d'accès aux documents et de rectification des renseignements personnels, se trouvent sur le site Web de l'OPIQ à la section Accès et protection des renseignements personnels.

Ces demandes doivent être adressées par écrit à la personne responsable de l'accès et de la PRP. Elles doivent fournir des indications suffisamment précises pour lui permettre d'y répondre. La demande ne sera considérée que si elle est faite par la personne concernée ou par une personne autorisée[11].

La personne requérante reçoit un avis de réception écrit, qui l'informe de la date de réception de la demande, des délais prescrits pour y donner suite et des recours possibles.

La personne responsable de l'accès et de la PRP répond à la demande au plus tard dans les 20 jours qui suivent la date de sa réception. Dans certains cas et sur avis écrit préalable à l'expiration du délai de 20 jours, le délai de réponse peut être prolongé d'une période n'excédant pas 10 jours.

Aucuns frais ne sont exigés à la suite d'une demande de rectification. La personne demandeuse reçoit une copie de tout renseignement personnel modifié ou ajouté, ou, selon le cas, une attestation du retrait d'un renseignement personnel. Pour les autres situations, l'OPIQ pourrait exiger des frais selon le *Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements personnels*.

[11]Une personne est autorisée si elle agit à titre de représentante, d'héritière ou de successible de la personne concernée, de liquidatrice de la succession, de bénéficiaire d'une assurance vie ou d'indemnité de décès, de titulaire de l'autorité parentale.

Titre IV – Commentaires, plaintes et recours

Toute personne, qui a des motifs de croire que les lois applicables à l'OPIQ en matière de protection des renseignements personnels, que le cadre de gouvernance ou les politiques en la matière n'ont pas été respectés à son égard, peut adresser une plainte et demander que la situation soit corrigée.

Une plainte en matière de protection des renseignements personnels peut porter sur leur cueillette, leur conservation, leur utilisation, leur communication ou leur destruction.

Toute question, commentaire ou plainte concernant le présent cadre de gouvernance et les pratiques en matière de confidentialité doivent être envoyés à la personne responsable de l'accès et de la PRP. Cette personne est identifiée sur le site Web de l'OPIQ et ses coordonnées se trouvent à la section Accès et protection des renseignements personnels.

La plainte doit être formulée par écrit, décrire la situation non conforme et inclure tous les éléments documentaires ainsi que les coordonnées de la personne qui dépose la plainte. La personne responsable de l'accès et de la PRP s'assure de recueillir les informations qui sont pertinentes au traitement de la plainte. S'il y a lieu, elle effectue l'inscription de l'incident de confidentialité au registre approprié.

La personne qui fait la demande peut également s'adresser à la Commission d'accès à l'information.

Cadre juridique

- *Charte des droits et libertés de la personne*, RLRQ, c. C -12
- *Code civil du Québec*, RLRQ, c. CCQ-1991
- *Code des professions*, RLRQ c. C -26
- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ, 2021, c. 25
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1
- *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P -39.1
- *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C -1.1
- *Règlement sur les incidents de confidentialité*, RLRQ, c. A -2.1, r. 3.1
- *Règlement excluant certains organismes publics de l'obligation de former un comité sur l'accès à l'information et la protection des renseignements personnels*, D. 744-2023 (G.O. II)
- *Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements personnels*, RLRQ, c. A -2.1, r. 3

Entrée en vigueur

Approuvée par le comité le : 11/09/2023
Entrée en vigueur le : 22/09/2023
Dernière mise à jour : 22/09/2023

Un avis sera publié si ce document fait l'objet de modifications importantes.