



Politique de gestion des renseignements personnels

Table des matières

1.	Définition	2
2.	Responsabilité et imputabilité	2
2.1.	Le conseil d'administration de la Société	2
2.2.	Le comité de décision	2
2.3.	Le responsable de la protection des renseignements personnels	3
3.	Constitution des dossiers des assurés et des tiers	3
4.	Constitution des dossiers des employés et des administrateurs de la Société.....	3
5.	La collecte, la détention, l'utilisation et la confidentialité des renseignements personnels ..	3
6.	Accès aux renseignements	4
7.	L'accès aux renseignements personnels.....	4
8.	Échange d'informations avec l'Ordre	4
9.	Traitement des plaintes relatives à la protection des renseignements personnels	4
10.	Procédure pour une demande d'accès ou de rectification au dossier	5
11.	Motifs de refus.....	5
12.	Personne responsable	5
13.	Réponse à une demande d'accès ou de rectification au dossier	6
13.1.	Demande de renseignements visant un tiers	6
14.	Frais exigibles du requérant	6
15.	Conservation et destruction des documents renfermant des renseignements personnels..	6
16.	Avis au président du conseil d'administration	7
17.	Gestion des incidents de sécurité.....	7
18.	Audit et révision.....	7

Préambule

La Société de gestion FARPOPQ (ci-après la « **Société** ») est l'organisme constitué par l'Ordre des pharmaciens du Québec (ci-après l' « **Ordre** ») afin d'assurer le traitement de ses opérations d'assurance.

La Société adopte la présente *Politique de gestion des renseignements personnels et de la sécurité des actifs informationnels* (ci-après la « **Politique** ») dans le cadre de l'application de la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1) et le *Code des professions* (L.R.Q., c.C-26) (ces lois étant collectivement désignées la « **Loi** »).

1. Définition

Les mots « renseignement personnel » s'entendent de tout renseignement qui concerne une personne physique et permet directement ou indirectement de l'identifier, notamment le nom, le numéro de membre, l'âge, le sexe, l'adresse, le numéro de téléphone et l'identité de son employeur ainsi que tout renseignement sensible tel que les données médicales, biométriques ou autres renseignements de même nature.

Les mots « renseignement confidentiel » englobent les renseignements personnels. Ils s'étendent également aux éléments suivants :

- i. Les actifs, produits, services ou technologies développées par la Société ou qui sont sa propriété;
- ii. Aux opérations de la Société, ses finances, sa gouvernance, ses stratégies, ses fournisseurs et contrats;
- iii. Aux renseignements contenus dans les dossiers constitués par la Société en regard du traitement des déclarations de sinistre ou des opérations liées à la souscription des risques.

Les renseignements personnels et les renseignements confidentiels sont parfois globalement désignés sous le nom de « les actifs informationnels ».

2. Responsabilité et imputabilité

2.1. Le conseil d'administration de la Société

Le conseil d'administration doit notamment :

- Adopter la présente Politique;
- Veiller de façon périodique à ce que le cadre de gestion créé par la Politique soit efficace et approprié;
- Obtenir les renseignements permettant d'acquérir l'assurance raisonnable que la Société préserve adéquatement ses actifs informationnels;
- Prendre avis du comité de décision en matière d'assurance responsabilité professionnelle en regard d'enjeux associés à la présente Politique, dont sa révision périodique.

2.2. Le comité de décision

Le comité de décision doit notamment :

- Obtenir l'assurance raisonnable que les opérations de la Société sont conduites conformément à son environnement normatif; et
- Prévoir les processus de reddition de comptes appropriés.

2.3. Le responsable de la protection des renseignements personnels

La directrice générale de la Société est responsable de l'application de la présente Politique. Elle doit notamment :

- Mettre en œuvre le cadre de gestion et veiller à ce qu'il soit connu et respecté;
- Identifier les risques associés aux actifs informationnels et proposer les mesures de contrôle adéquates;
- Documenter les mécanismes de contrôle;
- Rendre compte au conseil d'administration de la Société et, le cas échéant, celui de l'Ordre.

3. Constitution des dossiers des assurés et des tiers

L'objet de la constitution du dossier doit être inscrit au dossier.

Seuls les renseignements personnels pertinents à l'objet du dossier pour lequel ils sont nécessaires seront recueillis.

La Société conserve un dossier pour la période nécessaire en fonction de son objet et en tenant compte de ses obligations légales.

4. Constitution des dossiers des employés et des administrateurs de la Société

Aux fins de la présente Politique, les membres du comité de décision en matière d'assurance responsabilité professionnelle sont assimilés à des administrateurs de la Société en regard des renseignements personnels qu'elle détient à leur égard.

La Société constitue des dossiers pour ses employés et ses administrateurs. Elle les conserve pendant une période de trois (3) ans suite à leur départ ou la fin de leur mandat.

Le dossier comporte les renseignements nécessaires à l'administration du contrat de travail ou au mandat de l'administrateur ainsi que les renseignements concernant leur santé et leur sécurité.

Il est à noter que les demandes de confirmation de salaire lors de vérifications de crédit ainsi que les confirmations d'emploi après le départ d'un employé ou d'un administrateur ou autres demandes de cette nature, seront traitées uniquement avec le consentement de l'employé ou de l'administrateur concerné.

5. La collecte, la détention, l'utilisation et la confidentialité des renseignements personnels

Les renseignements personnels ne sont collectés qu'avec le consentement exprès des individus, ou en raison de la constitution d'un dossier de réclamation ou en conformité avec les exceptions au consentement prévues par la Loi. Les renseignements personnels ne sont utilisés que pour les fins pour lesquelles ils ont été obtenus.

Lorsqu'il est nécessaire de le faire, la Société s'assure d'obtenir un consentement à la collecte, à l'utilisation, au traitement et à la détention des renseignements personnels conformément à la présente Politique.

Les renseignements personnels sont détenus d'une telle façon que leur caractère confidentiel soit préservé, et ce, sans égard au support sur lequel ils se trouvent.

Les renseignements détenus par la Société doivent être à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée.

En ce qui a trait aux renseignements concernant les employés ou les administrateurs, ceux-ci ont l'obligation de transmettre sans délai toute modification relative aux renseignements personnels qui les concernent.

6. Accès aux renseignements

Les rôles et responsabilités des membres du personnel et des membres du conseil d'administration de la Société tout au long du cycle de vie des renseignements personnels sont encadrés par la règle du privilège minimum.

Cette règle limite l'accès des personnes aux seuls renseignements nécessaires à l'exercice de leur fonction.

7. L'accès aux renseignements personnels

L'accès aux renseignements personnels détenus par la Société s'effectue conformément à la Loi. Les personnes suivantes ont un droit d'accès aux renseignements personnels détenus par la Société :

- la personne concernée;
- le représentant ou le mandataire de la personne concernée à la condition d'avoir eu le consentement écrit de la personne concernée. Une copie de cette autorisation doit être transmise à la personne responsable des demandes d'accès avant que les renseignements ne soient communiqués.

Cependant, à la condition que les renseignements demandés soient nécessaires à l'exercice des fonctions qu'elles occupent ou à l'exécution d'un mandat, les personnes suivantes ont droit d'accès au dossier, sans le consentement de la personne concernée :

- a) le procureur de la Société;
- b) le procureur général, si le renseignement est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec;
- c) un organisme qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois, si le renseignement requis est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;
- d) toute personne ou tout organisme, si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de services ou d'entreprise confié par la Société;
- e) toute personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée.

8. Échange d'informations avec l'Ordre

Les informations que la Société doit communiquer à l'Ordre sont celles décrites dans le contrat de mandat intervenu entre l'Ordre et la Société et au Protocole de communication de renseignements en application des articles 80, 86.6, 86.7 et 86.8 du Code des professions auquel il réfère.

L'Ordre peut, lorsqu'il le demande, avoir accès à des informations statistiques non nominatives visant, entre autres, à favoriser la prévention de la commission d'actes générateurs de responsabilités ou à participer à l'orientation des politiques de formation, de formation continue ou de recherche de l'Ordre ou à évaluer la performance de la Société.

9. Traitement des plaintes relatives à la protection des renseignements personnels

La Société s'assure de bénéficier des ressources nécessaires afin de répondre aux demandes concernant l'accès, la correction, le retrait ou toute autre question ou demande d'accompagnement concernant leurs renseignements personnels. De telles demandes doivent être traitées dans les 30 jours suivant leur réception.

10. Procédure pour une demande d'accès ou de rectification au dossier

La demande d'accès peut être verbale ou écrite. La demande doit être suffisamment précise pour identifier le requérant ainsi que les renseignements auxquels il veut avoir accès.

Si une demande verbale est formulée, le requérant doit être informé que seules une demande écrite et une décision rendue sur celle-ci sont susceptibles de révision en vertu des dispositions législatives applicables.

La demande doit être adressée à la personne responsable de l'accès pour la Société, à savoir la directrice générale. Si la demande concerne des renseignements détenus par l'Ordre, notamment ceux relatifs au Registre des membres, la demande sera transmise à l'Ordre et sera dès lors traitée par ce dernier.

Toute personne peut faire corriger au dossier qui la concerne, les renseignements personnels inexacts, incomplets ou équivoques, et faire supprimer les renseignements périmés ou non justifiés par l'objet du dossier.

Seuls les renseignements factuels et objectifs peuvent faire l'objet d'une demande de rectification ou de suppression. La personne concernée peut cependant formuler des observations et exiger qu'elles soient versées au dossier à l'égard des opinions, jugements ou commentaires qui s'y trouvent.

La rectification doit être notifiée sans délai à toute personne qui a reçu les renseignements inexacts, périmés ou non justifiés dans les six (6) mois précédents.

11. Motifs de refus

La Société peut refuser de donner accès à des renseignements personnels qu'elle détient si :

- Ces documents sont visés par le secret professionnel au sens de l'article 9 de la Charte des droits et libertés de la personne (L.R.Q., c. C-12) ou le privilège relatif au litige;
- la communication des renseignements qu'elle détient peut avoir effet sur une procédure judiciaire ou quasi judiciaire, qu'elle ait été déposée ou qu'elle soit potentielle;
- ces renseignements comportent une analyse ou des conclusions de nature juridique portant sur l'application d'un droit à un cas en particulier ou pour tout autre motif prévu par une loi ou par la jurisprudence.

La Société doit refuser de donner communication d'un renseignement personnel concernant une personne lorsque la divulgation révélerait vraisemblablement un renseignement personnel sur un tiers et que cette divulgation serait susceptible de nuire sérieusement à ce tiers. La Société peut cependant communiquer un tel renseignement personnel si le tiers y consent.

12. Personne responsable

Le conseil d'administration de la Société est responsable de l'application de la présente Politique.

Pour les dossiers relatifs aux administrateurs, le secrétaire du conseil d'administration est la personne responsable.

Le responsable de l'application de la Politique est la personne qui exerce les fonctions de directeur(trice) général(e). Ses coordonnées se retrouvent sur le site Web du Fonds : www.farpopq.com.

13. Réponse à une demande d'accès ou de rectification au dossier

La personne responsable de l'accès, ou toute autre personne qu'elle désigne, doit contacter le requérant afin de s'enquérir des motifs pour lesquels il fait une demande d'accès, vérifier l'identité de cette personne et déterminer si elle détient les autorisations nécessaires.

Un accusé de réception sera transmis au requérant, dans lequel la date de réception de la demande sera indiquée, ainsi que le délai dont la Société bénéficie pour y répondre.

Lorsque la demande n'est pas suffisamment précise ou lorsque le requérant le requiert, la personne responsable de l'accès doit prêter assistance au requérant pour identifier le document susceptible de contenir les renseignements recherchés.

Une réponse écrite doit être transmise dans les vingt (20) jours de la réception de la demande ou, si ce délai est susceptible d'affecter les opérations de la Société, dans un délai maximal de trente (30) jours. À défaut de réponse, la Société est réputée avoir refusé d'y acquiescer.

Le refus de faire suite à la demande du requérant doit être notifié par écrit, et les motifs sur lesquels ils sont fondés doivent y être indiqués. Ce refus doit de plus comporter une indication quant au mécanisme de révision.

Le requérant peut, dans les trente (30) jours de la date de la décision ou de l'expiration du délai dont bénéficiait la Société pour répondre à la demande, s'adresser à la Commission d'accès à l'information afin de faire une demande de révision.

13.1. Demande de renseignements visant un tiers

Si la demande d'accès n'émane pas de la personne concernée ou ne découle pas de l'application d'une loi, la Société doit donner avis à cette dernière du fait qu'une personne ou un organisme demande d'avoir accès à de l'information la concernant. La Société doit informer la personne ou l'organisme qui fait la demande de l'avis donné à la personne concernée.

L'avis à la personne concernée est transmis par courrier dans les vingt (20) jours qui suivent la date de la réception de la demande d'accès. Cet avis doit fournir à cette personne l'occasion de présenter des observations écrites.

La personne concernée peut présenter ses observations dans les vingt (20) jours qui suivent la date où elle a été informée de la demande d'accès à des renseignements qui la concernent. À défaut de le faire dans ce délai, elle est réputée avoir consenti à ce que l'accès soit donné aux documents ou aux renseignements.

14. Frais exigibles du requérant

L'accès aux renseignements personnels contenus dans un dossier est gratuit sous réserve des frais raisonnables de transcription, de reproduction ou de transmission que la Société peut exiger. La Société informe le requérant de ces frais avant la communication et le requérant doit les acquitter à l'avance. L'importance des frais est déterminée par le conseil d'administration de la Société.

15. Conservation et destruction des documents renfermant des renseignements personnels

La Société conserve les renseignements personnels conformément au cadre posé par la Loi.

Lorsque la conservation d'un renseignement personnel n'est plus nécessaire en fonction de l'objet pour lequel il a été recueilli, et sous réserve de la durée de conservation prévue par la Loi, la Société assure sa destruction d'une manière qui protège le caractère confidentiel du renseignement et son importance.

En ce qui concerne les dossiers liés à une réclamation, les renseignements personnels seront anonymisés. Le dossier est conservé par la Société à des fins d'évaluation de la sinistralité.

16. Avis au président du conseil d'administration

La directrice générale doit donner avis au président du conseil d'administration de la Société de toute violation de confidentialité, de son origine et des mesures qui ont été mises en place afin d'en éviter la répétition. Elle doit également donner à l'Ordre les avis prévus par tout contrat auquel la Société est partie.

Le président du conseil d'administration de la Société doit donner à l'Ordre, sans délai, un avis similaire.

Les modalités relatives à la gestion de la violation de confidentialité sont celles prévues par l'Ordre.

17. Gestion des incidents de sécurité

La Société tient un Registre des incidents de confidentialité. Les utilisateurs doivent noter et signaler sans délai au à la personne responsable de l'application de la présente Politique tout événement, situation, ou incident susceptible de constituer une faille à la sécurité des actifs informationnels.

La personne responsable doit alors procéder aux vérifications nécessaires afin de déterminer si la sécurité d'actifs informationnels a été compromise, inventorier lesdits actifs et apporter une réponse rapide et efficace afin de pallier tout préjudice susceptible de découler de l'incident.

Elle doit également procéder aux vérifications nécessaires afin de déterminer s'il existe une vulnérabilité et une menace et, le cas échéant, procéder à une analyse du risque et à la mise en place de mesures correctives.

Le cas échéant, elle applique les sanctions disciplinaires appropriées en cas de manquement à la Politique.

La Société s'assure que les contrats conclus avec ses fournisseurs comportent des mesures de confidentialité au moins équivalentes à celles prévues par la présente Politique. L'Annexe A des présentes comporte les indications appropriées.

18. Audit et révision

La société procède à un audit technologique périodique.

La Politique, pour sa part, doit être révisée au moins tous les deux (2) ans afin de tenir compte des changements survenus dans les opérations de la Société, dans son environnement réglementaire et déterminer s'il existe de nouveaux risques technologiques.

Les modalités de cette révision seront définies par le conseil d'administration de la Société qui prend alors avis du comité de décision en matière d'assurance responsabilité professionnelle.



ANNEXE A

1. INFORMATION CONFIDENTIELLE

- 1.1. L'information confidentielle concerne toute information transmise par le Client sous la forme écrite ou sous quelque forme que ce soit en vertu du Contrat ou, généralement, quoi que ce soit dont le Prestataire de services aurait eu connaissance dans l'exécution du Contrat.
- 1.2. Le Prestataire de services s'engage à ce que ni lui ni aucun membre de son personnel ne divulgue, sans y être dûment autorisé par le Client, toute information confidentielle. À cet effet, le Prestataire de services doit prendre les mesures de sécurité nécessaires pour assurer le caractère confidentiel de cette information, notamment en contrôlant les accès et en faisant signer à tout membre de son personnel qui peut avoir accès à l'information confidentielle un engagement de confidentialité.
- 1.3. À l'expiration du Contrat, le Prestataire de services doit remettre au Client tous les documents qui lui ont été fournis en lien avec l'exécution du Contrat sans en conserver de copies, ceux-ci étant confidentiels et demeurant la propriété entière et exclusive du Client.

2. RENSEIGNEMENTS PERSONNELS

- 2.1. Un renseignement personnel est un renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier. Il est confidentiel.
- 2.2. Les seuls renseignements personnels qui seront communiqués au Prestataire de services sont ceux nécessaires à l'exécution du Contrat.
- 2.3. Le Prestataire de services doit prendre les mesures de sécurité nécessaires pour assurer le caractère confidentiel des renseignements personnels qui lui sont communiqués par le Client et pour assurer que ces renseignements ne seront utilisés que dans le cadre de l'exécution du Contrat.
- 2.4. Le Prestataire de services doit informer tout son personnel des obligations stipulées aux présentes et faire signer à tout membre de son personnel qui peut avoir accès aux renseignements personnels un engagement de confidentialité.
- 2.5. Le Prestataire de services s'engage à rendre accessibles les renseignements personnels uniquement aux membres de son personnel qui en ont besoin pour l'exécution du Contrat.
- 2.6. Le Prestataire de services s'engage à ne pas communiquer à qui que ce soit les renseignements personnels, sans le consentement écrit du Client.
- 2.7. Le Prestataire de services s'engage à détruire, à l'expiration du Contrat, tous les renseignements personnels qui lui seront communiqués en se conformant à la Fiche info *Destruction des documents contenant des renseignements personnels* de la Commission d'accès à l'information du Québec et transmettre au Client, dans les 60 jours suivant la fin du Contrat, une Attestation de disposition des renseignements personnels et confidentiels.
- 2.8. Le Prestataire de services s'engage à aviser le Client sans délai de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité des renseignements personnels communiqués. Cela vise tout autant les obligations contractuelles que celles imposées par une loi.



- 2.9. Le Prestataire de services doit collaborer et permettre au Client d'effectuer, en tout temps, toute vérification relative à la confidentialité des renseignements personnels et par voie de conséquence, au respect des conditions et obligations prévues aux présentes.
- 2.10. La fin du Contrat ne dégage aucunement le Prestataire de services de ses obligations et engagements relatifs à la protection des renseignements personnels et confidentiels.

3. HÉBERGEMENT DE DONNÉES

- 3.1. Le Prestataire de services s'engage à ce que toutes les données qui lui sont transmises par le Client, notamment les renseignements personnels concernant ses membres, soient hébergées sur des serveurs situés au Canada.