Politique de protection des renseignements personnels

La présente politique de protection des renseignements personnels :
(ci-après la « Politique ») énonce que **MAclinique Lebourgneuf** recueille, utilise, communique, conserve et détruit vos renseignements personnels.

Pour faciliter la lecture, nous utiliserons les expressions « nous » ou « la clinique » de temps à autre dans la Politique. Nous pouvons également obtenir votre consentement spécifique dans certains cas relatifs à la collecte, l'utilisation, la communication et la conservation de vos renseignements personnels. La Politique s'applique aux renseignements personnels que nous recueillons, peu importe la manière, que ce soit, par exemple en personne, par téléphone ou via notre site Web.

En acceptant cette Politique ou en nous fournissant des renseignements personnels après avoir eu l'opportunité de consulter la Politique ou tout autre avis complémentaire, vous acceptez que vos renseignements personnels soient traités conformément à la Politique et l'avis complémentaire.

1. À propos de nous

Voici nos informations d'identification complètes :

GMF MAclinique Lebourgneuf
725 boulevard Lebourgneuf, suite 220
Québec, QC, G2J 0C4

N'hésitez pas à communiquer avec notre responsable de la protection des renseignements personnels pour toute question ou commentaire que vous pourriez avoir concernant la Politique, la manière dont nous traitons vos renseignements personnels ou pour exercer vos droits concernant vos renseignements personnels. Vous pouvez joindre notre responsable de la protection des renseignements personnels par courriel :
Nom du responsable : Philippe Bédard
[pbedard@reseaumaclinique.com **]** ou par la poste à l'adresse mentionnée plus haut.

Au sein du GMF **MAclinique Lebourgneuf,** nous avons attribué les rôles et responsabilités comme suit :
À cet effet, voici ce que prévoit la Loi 3
- Les rôles et les responsabilités des membres du personnel de l'organisme et des professionnels qui y exercent leur profession, y compris les étudiants et les stagiaires, à l'égard de ces renseignements ;
Nous formons et sensibilisons les membres de notre personnel et nos professionnels (y compris nos étudiants et nos stagiaires) par le biais des activités suivantes :
À cet effet, voici ce que prévoit la Loi 3

- Une description des activités de formation et de sensibilisation en matière de protection de ces renseignements qu'il offre aux membres du personnel de l'organisme et aux professionnels qui y exercent leur profession, y compris aux étudiants et aux stagiaires.

2. Définitions importantes dans la Politique, on entend par : « Incident de confidentialité » (i) l'accès non autorisé par la loi à un renseignement personnel ; (ii) l'utilisation non autorisée par la loi d'un renseignement personnel ; (iii) la communication non autorisée par la loi d'un renseignement personnel ; ou (iv) la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement. « Renseignement personnel » tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier.

3. Comment allons-nous traiter vos Renseignements Personnels.

3.1 Quels sont les renseignements personnels que nous collectons ;
-Nom complet /numéro d'assurance maladie, adresse domiciliaire ainsi que votre adresse courriel.

3.2 Auprès de qui collectons-nous vos renseignements personnels ;
-Auprès du patient, son tuteur légal, centre hospitalier avec autorisation et autre professionnel de la santé avec votre autorisation.

3.3 Pourquoi collectons-nous vos renseignements personnels ?
-Afin de pouvoir communiquer adéquatement avec vous, en lien avec vos problématiques médicales.

3.4 Qu'arrive-t-il si vous ne consentez pas à la collecte de vos renseignements personnels ?
-Nous pourrions ne pas être en mesure de communiquer avec vous pour vos résultats médicaux, vos rendez-vous médicaux et vos prescriptions.

3.5 Qui aura accès à vos renseignements personnels ?
-Seulement les professionnels de la santé qui sont impliqués dans votre dossier incluent la secrétaire qui procède à votre inscription.

3.6 Comment allons-nous partager vos renseignements personnels avec des tiers ?
-Avec votre consentement, par courriel, par fax et par la poste, le cas échéant.

3.7 Pendant combien de temps allons-nous conserver vos renseignements personnels ?
-Selon la loi, nous devons conserver vos informations sur une période de 10 ans.

3.8 Quels sont les risques liés au traitement de vos renseignements personnels ?
Malgré l'optimisation des serveurs sécurisés de l'entreprise, il n'est pas impossible qu'une fuite de données survienne.

3.9 Où allons-nous conserver vos renseignements personnels ?
-Directement dans le dossier médical électronique.

4. Quels produits technologiques utilisons -nous.

Nom du logiciel	Nom du fournisseur	Utilités	Calendrier de mises à jour
OMNIMED	OMNIMED	Dossier médicale électronique	OMNIMED

5. Mesures de sécurité et risques inhérents

Nous suivons les standards de sécurité dans notre secteur d'activités pour protéger les renseignements que nous recueillons et que nous recevons. Plus particulièrement, nous avons en place des mesures de protection physiques, techniques, informatiques et administratives appropriées afin de protéger vos renseignements personnels contre un incident de confidentialité.

Malgré ces mesures, compte tenu des risques inhérents à l'utilisation de systèmes informatiques, nous ne pouvons toutefois pas assurer ou garantir la sécurité et la confidentialité des renseignements que vous nous transmettez ou nous fournissez, et vous le faites à vos propres risques. Si vous avez des raisons de croire que des renseignements personnels ont été compromis, veuillez communiquer avec nous aux coordonnées indiquées à l'article 1 de la Politique.

6. Comment et sous quelles conditions allons-nous communiquer vos renseignements personnels à des fins de sécurité publique ou de poursuite des infractions ?

6.1 En cas de risque sérieux de mort ou de blessures graves
Nous pourrons communiquer un renseignement personnel que nous détenons en vue de protéger une personne ou un groupe de personnes lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves, lié notamment à une disparition ou à un acte de violence, dont une tentative de suicide, menace cette personne ou ce groupe et que la nature de la menace inspire un sentiment d'urgence.
Les renseignements peuvent alors être communiqués à la ou aux personnes exposées à ce risque, à leur représentant ou à toute personne susceptible de leur porter secours. Seuls les renseignements nécessaires aux fins poursuivies par la communication seront communiqués.

6.2 Forces de l'ordre
Nous pourrons également communiquer un renseignement au Directeur des poursuites criminelles et pénales ou à une personne ou à un groupement chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois lorsque le renseignement est nécessaire aux fins d'une poursuite pour une infraction à une loi applicable au Québec.

Finalement, nous pourrons communiquer un renseignement à un corps de police lorsqu'il est nécessaire à la planification ou à l'exécution d'une intervention adaptée aux caractéristiques d'une personne ou de la situation, dans l'un ou l'autre des cas suivants : 1° le corps de police intervient, à notre demande, pour nous apporter de l'aide ou du soutien dans le cadre des services que nous fournissons à une personne; 2° nous agissons en concertation ou en partenariat avec le corps de police dans le cadre de pratiques mixtes d'interventions psychosociales et policières.

7. Vos renseignements personnels sont-ils transférés à l'extérieur du Québec ?
Il se peut que vos renseignements personnels soient transférés à l'extérieur du Québec.

8. Quels sont vos droits à l'égard de vos renseignements personnels ?

8.1 Accès : le droit de demander si nous détenons des renseignements personnels sur vous et, le cas échéant, de demander d'avoir accès à ces renseignements personnels.
8.2 Rectification : le droit de demander de faire rectifier tout renseignement personnel incomplet ou inexact que nous détenons.
8.3 Retrait du consentement : le droit de retirer votre consentement à la communication ou à l'utilisation des renseignements personnels détenus.
8.4 Restriction ou refus d'accès : le droit de demander qu'un intervenant particulier ou qui appartient à une catégorie d'intervenants indiquée ne puisse avoir accès à un ou à plusieurs renseignements que vous aurez identifiés.
8.5 Plainte : le droit de formuler une plainte adressée à notre responsable de la protection des renseignements personnels tel qu'identifié à l'article 1 en lien avec cette Politique ou de déposer une plainte auprès de la Commission de l'accès à l'information du Québec si vous croyez qu'une infraction aux lois sur la protection des renseignements personnels a été commise. Pour porter plainte auprès de la Commission d'accès à l'information (Québec), veuillez utiliser le formulaire approprié disponible à l'adresse suivante : Pour les citoyens | Commission d'accès à l'information du Québec (gouv.qc.ca)
8.6 Portabilité : Vous avez le droit de demander que vos renseignements personnels vous soient communiqués ou qu'ils soient transférés à une autre organisation dans un format technologique structuré et couramment utilisé.

Pour exercer l'un ou l'autre de ces droits, veuillez communiquer avec notre responsable de la protection des renseignements personnels de la manière indiquée à l'article 1 de la présente Politique.

9. Comment utilisons-nous les témoins de navigation ?
Au moment d'inspecter un fichier ou une URL, avant toute analyse, nos produits consultent la mémoire cache locale à la recherche d'objets malveillants ou d'objets bénins figurant sur la liste blanche. Ceci améliore la performance de l'analyseur.
Ensuite, notre Système de réputation LiveGrid® d'ESET reçoit des requêtes sur la réputation de l'objet afin de savoir s'il a déjà été détecté ailleurs et classé comme malveillant. Ceci améliore la performance de l'analyse et permet la transmission plus rapide de renseignements sur les logiciels malveillants à nos clients.
L'application de listes noires d'URL et la vérification de la réputation empêchent les utilisateurs d'accéder à des sites renfermant du contenu malveillant ou à des sites d'hameçonnage.

10. Sites de tiers
Cette Politique ne s'applique pas aux sites web, aux pages ou aux applications de tiers auxquels il est possible d'accéder via nos services et nous ne sommes pas responsables à l'égard de tels services tiers. Si vous suivez de tels liens, ces sites ou services tiers auront probablement leurs propres politiques sur la protection des renseignements personnels que vous devrez examiner avant de soumettre vos renseignements personnels.

11. Décisions entièrement automatisées
Cette section doit être complétée si vous avez recours à une technologie qui prend des décisions de manière automatisée basée sur des renseignements personnels.
-Nous n'avons pas recours à une technologie qui prend des décisions de manière automatisée.

12. Technologies d'identification, de profilage, ou localisation.
Cette section doit être complétée si vous avez recours à une technologie qui utilise des renseignements personnels pour analyser le comportement de vos clients.
-Nous n'avons pas recours à une technologie qui prend des décisions de manière automatisée.

13. Comment mettons-nous à jour la présente Politique sur la protection des renseignements personnels ?
Nous pourrons, de temps à autre, modifier la Politique afin de refléter les changements dans nos processus d'affaires ou dans la loi. Il serait pertinent de prévoir un mécanisme pour aviser les individus que votre politique a été mise à jour. Idéalement, vous fournissez un sommaire des changements afin de faciliter l'identification de ce qui a été ajouté.

[1]

[1] *Ce document a été préparé par AMOQ et la FMOQ. L'adaptation du document en lien avec la clinique a été réalisée par l'équipe de gestion Réseau MAclinique.*