Centre de l'ostéoporose et de rhumatologie de Québec

Politique de protection des renseignements personnels du Centre de l'ostéoporose et de rhumatologie de Québec

Objectif

L'objectif principal de cette politique de protection des renseignements personnels est de garantir la confidentialité et la sécurité des informations sensibles de la patientèle du Centre de l'Ostéoporose et rhumatologie de Québec (CORQ). Elle établit des lignes directrices claires afin de minimiser les risques de fuite ou de mauvaise utilisation des informations sensibles.

La politique décrit les différents types de renseignements personnels qui doivent être protégés, les responsabilités en matière de protection des renseignements personnels, les procédures pour garantir la protection physique et informatique des informations, les sanctions en cas de violation de la politique, etc.

En mettant en œuvre cette politique, la direction s'assure que les renseignements personnels sensibles de la patientèle sont protégés contre les fuites, les pertes, les atteintes à la sécurité et les abus. Cela renforce leur confiance envers la clinique et garantit que les informations sensibles sont gérées de manière responsable et sécurisée.

Champ d'application

La politique de protection des renseignements personnels est applicable au personnel administratif et aux spécialistes de la santé, sans exception. Chacune et chacun a une responsabilité importante en matière de protection des informations sensibles de la clientèle selon leur rôle.

Les médecins prescrivent des médicaments de spécialité pour lesquels un service spécial, le Programme de soutien aux patients (PSP), est offert à la patientèle pour l'accompagner dans les processus liés à ce nouveau traitement et pour réduire les délais d'accès au médicament. Le PSP est géré par une entreprise privée indépendante et financé par une compagnie pharmaceutique. Le personnel du PSP est un spécialiste de la santé qui obtient également un accès privilégié aux dossiers de la patientèle du CORQ en raison de son rôle de prestataire de soins de santé envers celle-ci.

Les responsabilités de chacun des rôles sont décrites dans la section Responsabilités de la présente politique.

Un dossier médical électronique au Québec est un registre électronique qui contient des informations sur la santé et la médicale de chaque patiente et patient. Il peut contenir des

informations telles que les antécédents médicaux, les diagnostics, les prescriptions, les résultats de tests, les comptes rendus de consultations et les images médicales. Le but du dossier médical électronique est de fournir une source centralisée et accessible de l'historique médical pour améliorer la qualité et la sécurité des soins de santé. La confidentialité et la protection des renseignements personnels sont des considérations importantes pour les dossiers médicaux électroniques au Québec et ceux-ci sont réglementées par les lois sur la protection de la vie privée.

Au Québec, la Loi sur la protection des renseignements personnels dans le secteur privé et la Loi sur les fichiers de santé sont les deux lois principales qui régissent la protection des renseignements personnels, y compris les dossiers médicaux électroniques. La Loi sur la protection des renseignements personnels dans le secteur privé établit les obligations des entreprises en matière de protection de la confidentialité des renseignements personnels et de la transparence quant à leur utilisation. La Loi sur les fichiers de santé énonce les règles pour la collecte, l'utilisation, la conservation et la divulgation des renseignements médicaux. Les entreprises qui exploitent des dossiers médicaux électroniques doivent se conformer à ces deux lois pour assurer la protection des renseignements personnels de leurs clients.

MYLE de MEDFAR Solutions Cliniques est le dossier médical électronique utilisé au CORQ**.** Veuillez-vous référer auprès du prestataire pour tout ce qui concerne la protection et la sécurité des données de leur plateforme.

En résumé, cette politique s'applique au personnel administratif et aux spécialistes de la santé de la clinique ainsi qu'au personnel d'un PSP. Chaque personne doit comprendre et respecter sa responsabilité en matière de protection des informations sensibles de la patientèle.

Définitions

Les renseignements personnels sensibles sont des informations qui peuvent être très personnelles et peuvent avoir une grande valeur pour quiconque les utilisent ou les manipulent. Dans le cas d'une clinique médicale, ces informations comprennent les informations sur la santé, la vie privée et les finances de la patientèle. Il est important que ces informations soient protégées contre l'accès non autorisé, l'utilisation abusive, la divulgation illégale et tout autre risque qui pourrait les rendre vulnérables à des abus ou à une exploitation.

Les informations sur la santé comprennent les antécédents médicaux, les informations sur les traitements et les soins médicaux, ainsi que les informations sur les diagnostics et les résultats des examens médicaux. Les informations sur la vie privée comprennent les informations personnelles, telles que le nom complet, l'adresse, le numéro de téléphone et la date de naissance. Les informations financières comprennent les informations sur les paiements, les factures et les remboursements.

En résumé, les renseignements personnels sensibles sont des informations très personnelles qui peuvent avoir une grande valeur pour quiconque les utilisent ou les manipulent. Il est donc important de prendre des mesures pour les protéger.

Responsabilités

a) Spécialistes en santé

- Les **médecins** sont responsables de la collecte, de la gestion et de la divulgation des informations sensibles de leur patientèle dans le cadre du traitement médical. Ils protègent les renseignements personnels sensibles en utilisant des formulaires d'information sécurisés, en veillant à ne pas discuter des informations confidentielles en public et en se conformant aux lois sur la protection des données.
- Le **personnel soignant** est responsable de la collecte et de la gestion des informations médicales de la patientèle. Il collecte les informations sur la santé et les stocke en toute sécurité.

b) Personnel administratif

- L'**adjointe administrative** ou l'**adjoint administratif** est responsable de la gestion des données personnelles, incluant les informations financières, de quiconque est enregistré au dossier médical électronique et effectue également la mise à jour de celles-ci. Elle ou il doit s'assurer que les informations sont stockées en toute sécurité et que seules les personnes autorisées y ont accès.
- La ou le **secrétaire réceptionniste** est responsable de la gestion des rendez-vous et de la communication avec la patientèle. Elle ou il collecte les informations personnelles et les stocke de manière sécurisée.
- La ou le **gestionnaire** est responsable de l'administration générale de la clinique. Elle ou il agit aussi à titre de responsable de la protection des informations sensibles de la patientèle. Elle ou il voit à la mise en œuvre et à la surveillance de la présente politique.
- La ou le **responsable de l'informatique** voit à la sécurité des systèmes informatiques et de la protection des renseignements personnels sensibles stockés sur les ordinateurs.

c) Le **personnel du PSP** est responsable de la collecte des informations sur la santé de la patientèle du CORQ et de la mise à jour de celles-ci, de la planification et de la coordination des soins, de la surveillance de la réponse aux traitements et de la communication avec d'autres membres de l'équipe de soins de santé. Dans le cadre de son travail, il doit respecter les normes éthiques et les lois sur la protection de la vie privée

de la patientèle, notamment en veillant à ne partager les informations sensibles quiconque est autorisé et en utilisant ces informations uniquement pour des fins de soins de santé légitimes.

Protection physique des renseignements

En outre, il est important de prendre des mesures supplémentaires pour protéger les renseignements physiques contre les risques tels que les incendies, les inondations, les dégâts causés par les intrusions et les erreurs humaines. Nous effectuons des sauvegardes régulièrement des informations sur des supports externes tels que des disques durs externes et des services de stockage en nuage sécurisés. Le personnel administratif et les spécialistes de la santé sont informés de la nécessité de protéger les renseignements physiques et de suivre les procédures établies pour garantir la sécurité des informations. Enfin, il est important de tenir des audits réguliers pour s'assurer que les renseignements personnels sensibles sont correctement protégés et pour détecter et pour corriger les lacunes potentielles dans les procédures de protection physique.

Protection informatique des renseignements

Les systèmes informatiques de la clinique sont protégés par des mots de passe sécurisés, une surveillance régulière et des mises à jour de sécurité régulières. Seules les personnes autorisées peuvent accéder aux renseignements personnels sensibles stockés sur les ordinateurs.

Les renseignements personnels sensibles stockés sur les ordinateurs et l'accès à ces informations doivent être enregistrés et surveillés de manière rigoureuse. Les ordinateurs utilisant ces informations sont protégés contre les menaces en ligne telles que les virus, les chevaux de Troie, les rançongiciels et les attaques par déni de service. En outre, les disques durs sont chiffrés pour protéger les données en cas de vol ou de perte de l'ordinateur. La clinique effectue des sauvegardes régulières des données pour minimiser les pertes en cas d'incident.

Formation

La formation sur la protection des renseignements personnels est un élément clé de la politique de la clinique. Elle vise à sensibiliser quiconque qui est concerné des enjeux de la protection des renseignements personnels sensibles et à fournir les connaissances nécessaires pour les protéger adéquatement. Cette formation inclue des sujets tels que la confidentialité, la sécurité des données, les lois sur la protection des données et les meilleures pratiques pour la protection des renseignements personnels. Le personnel administratif et les spécialistes de la santé seront formés régulièrement pour s'assurer qu'ils sont informés des dernières évolutions en matière de protection des données et pour renforcer les pratiques sécurisées. Cette formation pourra être offerte en interne ou en faisant appel à des experts externes.

Surveillance

La surveillance de la politique de protection des renseignements personnels est un aspect crucial pour garantir la confidentialité et la sécurité des données sensibles de la patientèle. La surveillance inclue des vérifications régulières des systèmes informatiques et des documents papier, ainsi que des audits internes pour s'assurer de la conformité aux normes de protection des données. Le personnel administratif et les spécialistes de la santé doivent être conscients de leurs responsabilités en matière de protection des données et signaler tout manquement ou incohérence à la politique immédiatement. La ou le gestionnaire prendra les mesures nécessaires pour corriger les violations et de veiller à ce que la politique soit mise en œuvre de manière efficace. Enfin, la formation continue peut également être utilisée pour renforcer la compréhension de la politique et des pratiques de protection des données.

Incidents de confidentialité

Quiconque qui constate l'un des évènements non autorisés décrits ci-dessous doit immédiatement le signaler à la ou le gestionnaire, responsable de la protection des renseignements personnels .

a. **Accès non autorisé par la loi à un renseignement personnel**. Tout accès non autorisé par la loi à un renseignement personnel est strictement interdit et constitue une violation de cette politique.

b. **Communication non autorisée par la loi d'un renseignement personnel.** Toute communication non autorisée par la loi d'un renseignement personnel est strictement interdite et constitue une violation de cette politique.

c. **Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement**. Toutes les mesures raisonnables doivent être prises pour protéger les renseignements personnels contre la perte ou toute autre atteinte à leur protection.

Dans le cadre de son engagement à protéger les renseignements personnels de la patientèle, la direction du CORQ considère les facteurs suivants lors de l'évaluation du risque de préjudice causé par un incident de confidentialité:

- La sensibilité des informations concernées;
- Les conséquences possibles de leur utilisation;
- La probabilité de leur utilisation à des fins néfastes.

La ou le gestionnaire effectuera une évaluation complète du risque.

Registre

Afin de se conformer aux réglementations gouvernementales, la direction tient un registre des incidents de confidentialité. Ce registre inclut les détails pertinents des incidents de violation de la confidentialité, tels que la date de l'incident, les personnes impliquées et les mesures prises pour corriger la situation. En cas de demande de la Commission d'accès à l'information, une copie de ce registre sera transmise pour examen. Il est important que tous les incidents de confidentialité soient enregistrés de manière précise et complète pour garantir la conformité et la transparence.

Le registre d'incidents de confidentialité contient les informations suivantes :

- Date et heure de l'incident.
- Description détaillée de l'incident, y compris les circonstances entourant l'incident et les personnes impliquées.
- Informations sur les renseignements personnels impliqués, y compris le type et la quantité de données.
- Étapes de la gestion de l'incident, y compris les mesures prises pour remédier à l'incident et prévenir les récurrences futures.
- Documentation des communications avec les parties concernées, y compris la patiente ou le patient, le membre du personnel administratif, le spécialiste de la santé, les autorités réglementaires et les parties tierces impliquées.
- Évaluation des risques pour la vie privée et les conséquences potentielles pour les personnes impliquées.
- Conclusion de l'enquête et plan d'action pour prévenir les incidents similaires à l'avenir.

Le registre doit être actualisé régulièrement et conservé en sécurité pour garantir la confidentialité des informations.

Informations recueillies

La direction s’engage à ne recueillir que les informations nécessaires à ses activités déterminées. Elle s’efforcera de ne collecter que les renseignements pertinents pour les fins pour lesquelles ils ont été demandés et de ne pas collecter plus d'informations que nécessaire.

La collecte des renseignements personnels est limitée aux fins déterminées en amont. En cas de demande de la personne concernée, soit la patiente, le patient ou quiconque est apte à la ou le représenter légalement, celui ou celle qui a collecté les renseignements doit informer cette dernière de la source de ces renseignements.

Lors de la collecte de renseignements personnels auprès de la personne concernée, celle-ci sera informer sur demande des fins pour lesquelles les renseignements sont recueillis, des moyens utilisés pour les recueillir, des droits d'accès et de rectification prévus par la loi ainsi que du droit

de retirer son consentement à la communication ou à l'utilisation des renseignements. Si nécessaire, la personne concernée sera informée du nom du tiers pour lequel la collecte est faite, du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements et de la possibilité que les renseignements soient transmis à l'extérieur du territoire concerné.

Sur demande, la personne concernée aura accès aux informations sur les renseignements personnels recueillis auprès d'elle, les catégories de personnes ayant accès à ces renseignements au sein de l'entreprise, la durée de conservation de ces renseignements et les coordonnées de la ou du gestionnaire.

Quiconque collecte des renseignements personnels doit informer sur demande la personne concernée sur les points suivants :

- La technologie utilisée pour la collecte.
- Les moyens disponibles pour activer les fonctions de protection de l'identité et de la localisation ainsi que pour empêcher le profilage.

Le profilage se réfère à la collecte et à l'utilisation de renseignements personnels pour évaluer certaines caractéristiques, telles que la performance au travail, la situation économique, la santé, les préférences personnelles, les centres d'intérêt ou le comportement.

L'information doit être transmise de manière simple et claire à la personne concernée, peu importe le moyen utilisé pour recueillir les renseignements personnels.

Afin de garantir la protection des renseignements personnels, la direction s'engage à respecter les principes suivants :

Utilisation limitée : Les renseignements personnels seront utilisés que pour les fins pour lesquelles ils ont été recueillis, sauf si la personne concernée donne son consentement explicite pour une utilisation différente.

Consentement nécessaire : Tout renseignement personnel sensible nécessitera le consentement explicite de la personne concernée pour être utilisé.

Cas d'utilisation sans consentement : Dans certains cas, l'utilisation des renseignements personnels sans l'obtention du consentement de la personne concernée sera permise lorsque celle-ci est :

a. Compatible avec les fins pour lesquelles ils ont été recueillis.
b. Manifestement bénéfique pour la personne concernée.
c. Nécessaire à la prévention et à la détection de la fraude, ainsi qu'à l'évaluation et à l'amélioration de nos mesures de protection et de sécurité.

d. Requise pour la fourniture ou la livraison d'un produit ou d'un service demandé par la personne concernée.

e. Nécessaire à des fins d'étude, de recherche ou de production de statistiques et que les renseignements sont dépersonnalisés.

Mise à jour de la politique

La direction publie sur le site internet de la clinique et diffuse par tout moyen adéquat une politique de confidentialité claire et compréhensible. Toute modification à cette politique fera l'objet d'un avis similaire.

La direction prend au sérieux la protection des renseignements personnels qui sont recueillis et utilisés pour ses activités. Une fois que les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la direction s'engage à le détruire de manière irréversible, en conformité avec les meilleures pratiques généralement reconnues dans son domaine. Les délais de conservation légaux prévus par les lois applicables sont respectés.

Réponse à la demande d'accès ou de rectification

La ou le gestionnaire doit répondre par écrit à une demande d'accès ou de rectification avec diligence dans un délai de 30 jours suivant la réception de celle-ci. En cas de non-réponse dans les 30 jours, il sera présumé que la demande est refusée.

En cas de refus d'accéder à une demande de renseignements personnels, la ou le gestionnaire doit fournir une motivation écrite pour ce refus et indiquer la disposition légale sur laquelle il est fondé. Elle ou il informera la requérante ou le requérant des recours disponibles et des délais dans lesquels ils peuvent être exercés. La ou le gestionnaire doit fournir une assistance adéquate pour aider à comprendre le refus, sur demande.

Accès gratuit aux renseignements personnels

L'accès aux renseignements personnels est gratuit. Cependant, des frais raisonnables peuvent être exigés pour la transcription, la reproduction ou la transmission de ces renseignements. Le montant approximatif des frais sera transmis à la requérante ou au requérant avant de procéder.

Examen des mésententes

Toute personne intéressée peut faire appel à la Commission d'accès à l'information pour examiner tout différend quant à l'application des lois régissant l'accès ou la correction des informations personnelles.

Québec
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741
Télécopieur : 418 529-3102

Montréal
Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4
Téléphone : 514 873-4196
Télécopieur : 514 844-6170