Clinique Maizerets
GMF UNIVERSITAIRE

# Politique relative à la conservation et la protection des renseignements personnels et de santé

La présente politique s'inscrit en cohérence avec les orientations et directives véhiculées dans la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.

La clinique Maizerets - GMF universitaire accorde une importance majeure à la sécurité des renseignements de santé de ses patients, de ses médecins, de ses apprenants et de tout son personnel.

Soucieuse de se conformer aux meilleures pratiques cliniques, pédagogiques et éthiques en la matière, la Clinique est heureuse de pouvoir compter sur son partenariat avec l'Université Laval et le Centre de recherche en santé durable VITAM du CIUSSS de la Capitale-Nationale.

**Dossier médical électronique (DME)**

Bien que le dossier clinique utilisé par la clinique soit intégralement virtuel et sécurisé par son fournisseur, la Clinique déploie un ensemble de moyens et balises qui renforcent la protection des renseignements qu'il contient. Notamment, son réseau wifi est rigoureusement sécurisé et l'ensemble des activités mettant en scène des informations confidentielles sont protégées au sein d'un serveur interne maillé.

L'ensemble des renseignements de santé contenus au DME sont destinés à assurer les soins et services de santé aux patients.

Toute activité d'amélioration continue de la qualité n'est possible à partir de ces données que sur la base d'un consentement explicite et écrit, consigné à ce même dossier. L'utilisation des données sera toujours dépersonnalisée lorsque ceci est possible.

L'ensemble des renseignements de santé conservés au DME l'est de manière permanente et ne peut pas être altéré. Tous les consentements établis à la Clinique doivent être réitérés aux cinq (5) ans.

L'administrateur TI de la clinique est le seul à disposer de privilèges d'accès au réseau. Lui et tout autre intervenant technologique s'engagent à adhérer aux politiques de protection des renseignements et de confidentialité de la clinique. Tout partenaire de la clinique est notamment choisi en raison de son engagement au plus grand respect de la confidentialité des identifiants et données auxquelles il pourrait accéder dans l'exercice de ses fonctions de gestion des actifs informationnels.

**Caméras et enregistrements vidéo**

La Clinique Maizerets est fière de participer à la formation de la relève professionnelle et à la recherche en santé durable. Cela dit, toutes les vidéos en direct ou enregistrées ne sont utilisées qu'à des fins d'amélioration des pratiques cliniques, des fins d'enseignement ou encore en soutien à d'éventuels travaux de recherche.

Les salles équipées de caméras sont toutes clairement identifiées et personne ne peut être filmé ni enregistré sans son consentement explicite.

Des témoins de couleur dans toutes les salles équipées de caméras permettent de savoir que la caméra filme (témoin vert) ou non (témoin rouge).

Tous les enregistrements réalisés sont conservés de manière cryptée sur un serveur local protégé à des fins exclusives d'enseignement et ne pourront être utilisés à des fins de recherche que lorsque dûment autorisés, à la fois par un comité d'éthique de la recherche reconnu par les autorités et la direction du comité de gestion de la clinique.

Les enregistrements ne seront aussi conservés qu'à condition que tous les acteurs (clinicien(ne), patient(e), accompagnateur-trice) y aient consenti au début de l'enregistrement, même si un consentement préalable écrit ou verbal différent avait été préalablement obtenu.

Sans égard aux balises d'utilisation précédemment détaillées, aucune donnée issue du DME ou de la banque d'enregistrements ne pourra être utilisée à moins qu'un consentement explicite et écrit ait été consigné à ce même dossier.

**Gouvernance relative à la protection des renseignements de santé**

**Responsable de la protection des renseignements :** Dr. Simon-Frédérick Richard, Directeur médical de la Clinique Maizerets-GMF-Universitaire.

La direction médicale de la clinique demeure en tout temps responsable de la protection et des accès aux renseignements de santé conservés par la clinique.

La protection des renseignements de santé contenus au DME est partagée entre le fournisseur de DME de la Clinique et la direction médicale de la Clinique. Cette dernière est notamment responsable de l'audit périodique des accès aux renseignements.

La direction médicale demeure l'unique responsable des octrois d'accès et de la tenue des registres d'accès.

La direction médicale de la Clinique est également responsable de l'élaboration, de la mise à jour et du respect intégral de la présente politique. C'est aussi elle qui assure le traitement des plaintes ou incidents relatifs à la protection des renseignements.

La direction médicale peut être jointe pour toute question ou enjeu relatifs à la protection des renseignements de santé en appelant la Clinique au 418-661-1413, poste 239 ou par courriel au secretariatmaizerets@melioremsante.ca.

**Commission d'accès à l'information (CAI)**

En cas d'incident ou de bris sérieux à la protection des renseignements de santé sous la gouvernance de la Clinique, celle-ci s'engage à interpeller la CAI et lui assurer toute sa collaboration dans l'investigation et la mise en œuvre de mesures de prévention et de correction requises.

**Assurances**

La Clinique dispose d'une assurance en cybersécurité adaptée sur mesure aux milieux cliniques.

**Responsabilités individuelles**

Chacun(e) des employé(e)s et professionnel(le)s de la clinique est tenu(e) à la plus grande rigueur dans la protection des renseignements de santé des usager(e)s de la clinique. À ce titre, le transport de données (sur clé, ordinateur ou tout autre moyen) n'est recommandé que s'il s'avère essentiel au travail de la personne. Dans un tel cas, les données doivent être systématiquement chiffrées durant leur transport.

Par ailleurs, tout cyberincident ou événement survenu hors de la clinique et susceptible d'entrainer une atteinte à la confidentialité doit être rapporté sans délai à la direction de la clinique. Tout événement laissant présager d'une cyberattaque (lenteur inhabituelle du système, fichiers déplacés, etc.) impose aussi une déclaration immédiate. De plus, tous les moyens possibles doivent être déployés pour mitiger les impacts d'un tel incident (ex. chiffrement ou suppression distants de données). Selon la nature et la gravité de l'incident, la direction médicale veillera à informer le Commissaire à la protection de la vie privée, la Commission de l'accès à l'information ou toute personne concernée. Un registre de tels incidents est tenu sous l'autorité de la direction médicale.

Tout(e) employé(e) ou professionnel(le) œuvrant à la clinique peut obtenir le soutien et la formation requise en matière de détection, signalement et intervention en cette matière en s'adressant à la direction médicale de la clinique.

**Départ d'un(e) employé(e)**

Au départ d'un(e) employé(e) ou professionnel(le), la direction médicale s'assure de la désactivation des comptes, de la récupération du matériel, de la destruction de toute information confidentielle ou renseignement de santé par cette personne. Par ailleurs, puisque la Clinique dispose d'un environnement informatique local hautement sécurisé, les invasions externes demeurent pratiquement impossibles.