POLITIQUE DE GESTION DES RENSEIGNEMENTS PERSONNELS

Centre de communication santé des Capitales (CCSC)

(Juillet 2025)

1. Objectif de la politique

La présente politique vise à encadrer, de manière claire et accessible, la gestion des renseignements personnels au Centre de communication santé des capitales (CCSC), conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, ainsi qu'aux meilleures pratiques recommandées par la Commission d'accès à l'information du Québec (CAI).

Elle définit les responsabilités, les balises de conservation, les droits des individus concernés, ainsi que les règles d'accès, de rectification et de sécurité applicables.

2. Définition d'un renseignement personnel

Un renseignement personnel désigne toute information qui concerne une personne physique et permet de l'identifier, directement ou indirectement.

Cela inclut, entre autres : le nom, le numéro de téléphone, l'adresse, les enregistrements audio, les données de santé, les identifiants internes, ainsi que tout autre élément susceptible de révéler l'identité ou les caractéristiques personnelles d'un individu.

3. Types de renseignements personnels détenus par le CCSC

Le CCSC traite différents types de renseignements personnels dans le cadre de ses mandats :

- données d'appel (911 médical, informations sensibles transmises par les usagers);
- informations d'identification des appelants;
- dossiers de formation et d'évaluation du personnel;
- données de performance, dossiers des ressources humaines, évaluations internes;
- enregistrements audio et transcriptions des appels;
- renseignements liés à la santé ou à des urgences médicales.

4. Rôle et responsabilités du personnel

Chaque employé du CCSC, quel que soit son poste, a la responsabilité de protéger les renseignements personnels qu'il traite, et ce, tout au long de leur cycle de vie : de la collecte à la destruction.

Tous les membres du personnel doivent :

- suivre les formations obligatoires en matière de protection des renseignements personnels;
- appliquer les principes de sécurité et de confidentialité en tout temps;
- signaler immédiatement tout incident ou bris de confidentialité au responsable de la protection des renseignements personnels.

Les gestionnaires doivent en plus :

- s'assurer que les processus de leur secteur respectent la présente politique;
- réviser périodiquement les accès et les autorisations accordées à leurs équipes.

5. Accès et personnes autorisées

L'accès aux renseignements personnels est strictement limité aux personnes dont les fonctions l'exigent, selon le principe du moindre privilège.

Catégories de personnes autorisées :

- répartiteurs médicaux d'urgence (RMU) : uniquement pour les appels en cours ou les suivis directs requis par les protocoles cliniques;
- superviseurs de quart : pour assurer la qualité, la conformité et la formation continue des RMU;
- gestionnaires des opérations : dans le cadre d'analyses, de revues de performance ou d'enquêtes internes;
- responsable de la protection des renseignements personnels : pour tout ce qui concerne la gestion, l'évaluation et le traitement des demandes;
- service des ressources humaines : uniquement pour les dossiers du personnel, selon les balises légales;
- direction générale et direction adjointe : dans le cadre de décisions stratégiques, de contrôles qualité ou de litiges;

- partenaires contractuels ou technologiques (uniquement si une entente légale et sécuritaire est en place, conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*).

Règles d'accès :

- chaque accès est consigné dans un registre électronique sécurisé;
- tout accès non justifié est considéré comme une faute grave et traité selon les mécanismes disciplinaires internes;
- des audits périodiques sont effectués pour assurer le respect de cette politique.

6. Sécurité des renseignements personnels

Le CCSC applique des mesures de sécurité rigoureuses pour protéger les renseignements personnels :

- authentification multifactorielle pour les accès sensibles;
- registre de journalisation des accès;
- chiffrement des fichiers contenant des données personnelles;
- partage restreint via des plateformes sécurisées (ex. : SharePoint CCSC);
- formation continue sur la cybersécurité et la confidentialité.

7. Conservation et destruction

Les renseignements personnels sont conservés uniquement pour la durée nécessaire à l'accomplissement des finalités pour lesquelles ils ont été recueillis.

Le CCSC applique un calendrier de conservation conforme à la *Loi sur les archives*.

À l'issue des délais légaux ou organisationnels, les renseignements sont soit :

- détruits de manière sécuritaire, ou;
- archivés dans un environnement restreint et chiffré, si une obligation légale l'exige.

8. Rectification d'un renseignement personnel

Toute personne peut demander l'accès à ses renseignements personnels et faire corriger toute information inexacte, incomplète ou équivoque.

Pour ce faire, il suffit d'en faire la demande par écrit à l'adresse suivante :

acces@ccscapitales.com

Le CCSC s'engage à traiter chaque demande dans les délais prescrits par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et informera l'individu des suites données à sa demande.

9. Responsabilité du responsable de la protection des renseignements personnels

Le CCSC désigne officiellement une personne responsable de la protection des renseignements personnels, chargée de :

- s'assurer du respect des obligations légales;
- traiter les demandes d'accès ou de rectification;
- intervenir en cas d'incident ou de bris de confidentialité;
- offrir des conseils à la direction et au personnel;
- réviser annuellement la présente politique.

Nom du responsable :

Éric Raymond
Chargé de projet à la gestion documentaire
Courriel : acces@ccscapitales.com

10. Communication à des tiers

Aucun renseignement personnel n'est communiqué à des tiers sans le consentement explicite de la personne concernée, sauf dans les cas prévus par la loi. Toute communication doit être balisée par un encadrement contractuel rigoureux.

11. Diffusion et révision

Cette politique est révisée annuellement ou dès qu'une modification légale ou organisationnelle le justifie.

Tout le personnel est informé de sa mise à jour et doit en prendre connaissance.