Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale Québec	**POLITIQUE**
	Code : PO-60
	Direction responsable : Direction des services professionnels Approuvée par : Isabelle Samson, directrice
	Adoptée au comité de direction le : 9 janvier 2024
	Adoptée par le conseil d'administration le : Non applicable Résolution no : Non applicable
	Entrée en vigueur le : 9 janvier 2024 Cette politique annule la politique no : Non applicable

TITRE : Politique de confidentialité relative au recueil de renseignements personnels par l'entremise du portail patient lié au dossier médical électronique

CONSULTATIONS

☐ Conseil des infirmières et infirmiers : Non applicable.
☐ Conseil multidisciplinaire : Non applicable.
☐ Conseil des médecins, dentistes et pharmaciens : Non applicable.
☐ Cadres : Non applicable.
☒ Autres : Comité sur l'accès à l'information et la protection des renseignements personnels du CIUSSS de la Capitale Nationale : 15 novembre 2023

Table des matières

1. FONDEMENTS

Cette politique s'inscrit dans le cadre de l'application de ces lois et règlement :

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, ci-après la « Loi sur l'accès »);
- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ, 2021, chapitre 25);
- *Loi sur les services de santé et les services sociaux* (RLRQ, chapitre s-4.2, ci-après la « LSSSS »)
- *Règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique.*

2. PRINCIPES

- Droit à la confidentialité;
- Protection des renseignements personnels.

3. OBJECTIF

Permettre aux usagers qui utilisent le portail patient lié au dossier médical électronique déployé dans certains programmes cliniques du CIUSSS de la Capitale-Nationale d'obtenir les informations nécessaires afin qu'ils puissent comprendre leurs droits et de quelles façons leurs renseignements personnels sont recueillis et utilisés.

4. CHAMP D'APPLICATION

Cette politique s'applique spécifiquement aux usagers qui utilisent le portail patient lié au dossier médical électronique déployé dans certains programmes cliniques du CIUSSS de la Capitale-Nationale.

5. DÉFINITIONS

DOSSIER MÉDICAL ÉLECTRONIQUE :
Système de gestion informatisé du dossier usager en première ligne. Il permet, notamment, la prise de notes clinique, la gestion des rendez-vous, la transmission de prescriptions et de requêtes ainsi que l'échange d'informations avec des usagers par l'entremise d'un portail patient.

PORTAIL PATIENT :
Plateforme liée au dossier médical électronique pour permettre une communication sécuritaire d'informations entre les professionnels et les usagers.

6. RENSEIGNEMENTS PERSONNELS

6.1 NOM DU TIERS QUI RECUEILLE DES RENSEIGNEMENTS PERSONNELS POUR LE CIUSSS DE LA CAPITALE-NATIONALE

Le CIUSSS de la Capitale-Nationale fait appel à un fournisseur (un tiers) pour le dossier médical électronique, lequel recueille des renseignements personnels par l'entremise du portail patient. Pour plus d'information sur ce fournisseur, nous vous référons à l'annexe 1.

6.2 RENSEIGNEMENTS PERSONNELS RECUEILLIS

Le portail patient du dossier médical électronique de l'établissement permet de recueillir des renseignements personnels des usagers. Ceux-ci peuvent entre autres inclure:

- L'identification de l'usager (nom, adresse, numéro de téléphone, numéro de carte d'assurance maladie, personne à contacter en cas d'urgence, personne autorisée à prendre des décisions au nom de l'usager);
- L'historique de santé et l'historique médical de l'usager et de sa famille;
- Les notes associées à chaque consultation de l'usager;
- Le détail des examens réalisés par le professionnel;
- Les rapports relatifs aux analyses en laboratoire, aux pathologies, aux consultations, aux tests ou aux examens par imagerie diagnostique, ainsi qu'aux procédures d'investigation;
- Le détail des diagnostics, des soins et des traitements;
- Les photos téléversées par l'usager ou le professionnel;
- Les demandes de traitement ou d'investigation;
- Les consentements écrits obtenus en lien avec les traitements prescrits;
- Le relevé des rendez-vous ratés ou annulés.

6.3 FINS AUXQUELLES LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS

- Fournir des services aux usagers tels que:
    - La prise de rendez-vous en ligne;
    - L'envoi de rappels automatisés pour confirmer on annuler un rendez-vous;
    - Les communications sécurisées entre professionnels et usagers par messagerie privée;
    - La transmissions de formulaires à compléter.
- Améliorer des fonctionnalités ou résoudre des problèmes techniques;
- Analyser et résoudre les incidents, ou donner suite aux plaintes des usagers;
- Cerner les besoins et les préférences des professionnels et des usagers.

6.4 CATÉGORIES DE PERSONNES QUI, AU SEIN DU CIUSSS DE LA CAPITALE-NATIONALE, ONT ACCÈS AUX RENSEIGNEMENTS PERSONNELS RECUEILLIS

- Médecins et résidents;
- Infirmières praticiennes spécialisées;
- Professionnels en soins infirmiers;
- Travailleurs sociaux;
- Pharmaciens;
- Autres professionnels de la santé s'il y a lieu (ex. nutritionniste, inhalothérapeute, physiothérapeute, ergothérapeute, etc.)
- Étudiants et stagiaires;

- Personnel administratif qui soutient le professionnel clinique;
- Archivistes médicales.

6.5 MOYENS PAR LESQUELS LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS

Les renseignements personnels sont recueillis dans le portail patient, donc par l'entremise d'un support électronique sécurisé.

6.6 DROITS D'ACCÈS ET DE RECTIFICATION ET PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DU CIUSSS DE LA CAPITALE-NATIONALE

Les modalités afin d'accéder au dossier ou pour demander une rectification de celui-ci ainsi que pour connaître le nom et les coordonnées de la personne responsable de la protection des renseignements personnels du CIUSSS de la Capitale-Nationale se retrouvent à l'annexe 2.

6.7 COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

Les renseignements personnels recueillis par l'entremise du portail patient sont soumis aux protections prévues par la Loi sur l'accès ainsi qu'aux articles 17 à 28 de la LSSSS.

L'article 19 de la LSSSS précise que le dossier de l'usager est confidentiel et que nul ne peut y avoir accès, si ce n'est avec le consentement de l'usager ou de la personne pouvant donner un consentement en son nom. Cet article précise également les situations où un renseignement contenu au dossier de l'usager peut être communiqué sans son consentement.

6.8 POSSIBILITÉ QUE LES RENSEIGNEMENTS PERSONNELS SOIENT COMMUNIQUÉS À L'EXTÉRIEUR DU QUÉBEC

Les renseignements personnels recueillis par l'entremise du portail patient sont hébergés au Québec. Les données des usagers peuvent être consultées à partir d'une autre province que le Québec, mais les données en transit sont protégées et encryptées.

6.9 MESURES PRISES POUR ASSURER LA CONFIDENTIALITÉ ET LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS

- Le CIUSSS de la Capitale-Nationale a publié un Guide sur les règles de gouvernance en matière de protection des renseignements personnels, qui vise à résumer ce que l'établissement applique en matière de protection des renseignements personnels. Ce dernier comporte les informations relatives aux éléments suivants :
    - Les rôles et responsabilités en matière de protection des renseignements personnels, notamment dans le cadre du traitement d'un incident de confidentialité, de l'évaluation des facteurs relatifs à la vie privée (ÉFVP) ou de la diffusion d'une politique de confidentialité en lien avec les renseignements personnels recueillis par moyen technologique;
    - Les mesures prises par l'établissement afin de protéger les renseignements personnels;
    - Le processus de traitement des plaintes;
    - Les activités de formation et de sensibilisation offertes au personnel en matière de protection des renseignements personnels.
- Plusieurs mesures sont prises par le CIUSSS de la Capitale-Nationale pour assurer la confidentialité et la sécurité des renseignements personnels dans le cadre de la mise en œuvre de différents documents administratifs (voir le résumé de celles-ci en Annexe 3);

- Les mesures minimales de sécurité exigées par le ministère de la Cybersécurité et du Numérique doivent être en vigueur lors du déploiement d'un nouvel actif informationnel (voir Annexe 4);
- Les professionnels de la santé et des services sociaux membres d'un ordre professionnel sont soumis à des devoirs de confidentialité et de secret professionnel par l'entremise de leur code de déontologie.
- Le contrat entre le CIUSSS de la Capitale-Nationale et le fournisseur prévoit que l'établissement est responsable de la sécurité des données du dossier médical électronique dont il confie l'hébergement à un fournisseur qui doit mettre en œuvre des mécanismes de sécurité proportionnels à la valeur de ces données :
    - Le fournisseur doit faire le nécessaire pour que les mesures de sécurité qu'il déploie assurent, en tout temps, la sécurité des données, et ce, en fonction de la valeur de ces données;
    - Le fournisseur doit garantir la protection de la confidentialité des données au moyen de l'application de la gestion de l'identification, de l'authentification et de la gestion des droits d'accès du dossier médical électronique et aussi, par les procédures d'exploitation et de soutien qu'il applique pour ses employés et sous-traitants.

6.10 DROIT DE PORTER PLAINTE

La personne concernée par les renseignements personnels, comme tous les usagers de la Capitale-Nationale, a le droit de se prévaloir du processus de traitement des plaintes relatives à la protection des renseignements personnels.

Une plainte de la part d'un usager ou de son représentant qui concerne la protection des renseignements personnels en lien avec le dossier d'un usager peut se faire :

- Auprès du Commissaire local aux plaintes et à la qualité des services (CPQS).
- Auprès de la Commission d'accès à l'information du Québec (CAI).

Vous trouverez les coordonnées du CPQS et de la CAI à l'annexe 5.

7. MODIFICATIONS DE LA POLITIQUE

Cette politique de confidentialité ne peut être modifiée avant l'expiration d'un délai de 15 jours à compter de la date de publication d'un avis de modification de cette politique ou, le cas échéant, avant l'expiration d'un délai plus court mentionné dans cet avis de modification.

L'avis de modification doit :

- Indiquer la date de sa publication;
- Indiquer l'objet général des modifications apportées à la politique de confidentialité dans une section dédiée à cette politique sur le site Internet de l'établissement;
- Indiquer la date d'entrée en vigueur des modifications.

Si l'avis mentionne un délai plus court que le délai de 15 jours, les motifs pour lesquels la politique doit être modifiée dans ce délai plus court doivent être indiqués dans l'avis de modification.

L'avis de modification concernant une modification significative à la politique doit faire l'objet d'une consultation auprès du comité sur l'accès à l'information et la protection des renseignements personnels de l'établissement.

8. COORDONNÉES UTILES

Pour toute question relative à cette politique de confidentialité, vous pouvez vous adresser à votre professionnel de la santé avec qui vous échangez des informations par l'entremise du portail patient lié au dossier médical électronique. Au besoin, celui-ci peut communiquer par courriel avec le pilote du dossier médical électronique à cette adresse : dme.ciussscn@ssss.gouv.qc.ca

9. RESPONSABILITÉS

DIRECTION DÉTENTRICE DE L'ACTIF INFORMATIONNEL :

- Développer et réviser, au besoin, la présente politique, et ce, en collaboration avec la Direction des ressources informationnelles, le Service des archives de la Direction des services multidisciplinaires et la Direction des affaires juridique, institutionnelles et corporatives;
- Diffuser la présente politique sur le site Internet de l'établissement en collaboration avec le Service des communications de la Direction des ressources humaines et des communications;
- Répondre aux questions sur la présente politique transmise par courriel au pilote du Dossier médical électronique.

DIRECTIONS DE PROGRAMMES CLINIQUES QUI ONT RECOURS AU PORTAIL PATIENT DU DOSSIER MÉDICAL ÉLECTRONIQUE :

- Diffuser cette politique par tout moyen propre à atteindre les personnes concernées par celle-ci et veiller à son application.
- Communiquer avec le pilote du dossier médical électronique en cas de questionnement en lien avec l'application de cette politique.

10. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date d'adoption par le Comité de direction. Elle doit être révisée aux 3 ans ou au besoin.

11. ANNEXES

Annexe 1 : Fournisseur de dossier médical électronique et de portail patient pour le CIUSSS de la Capitale-Nationale
Annexe 2 : Accès au dossier, rectification et personne responsable de la protection des renseignements personnels
Annexe 3 : Mesures prises pour assurer la confidentialité et la sécurité des renseignements personnels dans le cadre de la mise en œuvre de différentes politiques et directives du CIUSSS de la Capitale-Nationale
Annexe 4 : Mesures minimales de sécurité exigées par le ministère de la Cybersécurité et du Numérique
Annexe 5 : Coordonnées du CPQS et de la CAI

ANNEXE 1

FOURNISSEUR DE DOSSIER MÉDICAL ÉLECTRONIQUE ET DE PORTAIL PATIENT POUR LE CIUSSS DE LA CAPITALE-NATIONALE

Le fournisseur de dossier médical électronique et de portail patient pour l'établissement est Télus.

La solution de dossier médical électronique utilisée est **Medesync**. Pour plus d'information sur cette solution, vous pouvez consulter cette page du site Internet de Telus.

La solution de portail patient utilisée est **Pomelo**. Pour plus d'information sur cette solution, vous pouvez consulter cette page du site Internet de Telus.

Télus est engagé dans un **Programme de gestion de la protection de la vie privée**. Pour plus d'information sur ce programme, vous pouvez consulter cette page du site Internet de Telus.

ANNEXE 2

ACCÈS AU DOSSIER, RECTIFICATION ET PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Pour présenter une demande d'accès ou de rectification concernant le dossier d'un usager, vous devez vous adresser au service des archives du CIUSSS de la Capitale-Nationale.

Une demande d'accès doit être présentée sur le formulaire spécifiquement prévu à cet effet. Vous trouverez plus d'information à ce sujet sur cette page du site Internet du CIUSSS de la Capitale-Nationale.

Nous vous informons également que la personne responsable de la protection des renseignements personnels au CIUSSS de la Capitale-Nationale est la suivante :

Mme Anne Thibault
Coordonnatrice du service des archives
2601, ch, de la Canardière
Tél. 418 663-5000 poste 27757
Télec. : 418 660-3027
Courriel : anne.thibault.ciussscn@ssss.gouv.qc.ca

ANNEXE 3

MESURES PRISES POUR ASSURER LA CONFIDENTIALITÉ ET LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS DANS LA CADRE DE LA MISE EN ŒUVRE DE DIFFÉRENTS DOCUMENTS ADMINISTRATIFS DU CIUSSS DE LA CAPITALE-NATIONALE

Documents administratifs	**Mesures prévues pour assurer la confidentialité, la protection et la sécurité des renseignements personnels**
Politique relative à la sécurité de l'information	• Clarification de la responsabilité et l'imputabilité de différents acteurs de l'établissement face à la sécurité de l'information; • Définition d'une approche globale de la sécurité de l'information; • Gestion intégrée des risques de sécurité et de l'information; • Activités de sensibilisation et de formation des utilisateurs à la sécurité de l'information; • Droit de regard du ministre de la Santé et des Services sociaux sur tout usage des actifs informationnels du réseau de la santé et des services sociaux; • Sanctions lorsqu'un utilisateur contrevient ou déroge à cette politique ou les directives en découlant.
Cadre de gestion de la sécurité de l'information	• Mise en place d'une structure fonctionnelle de la sécurité de l'information et définition des rôles et responsabilités en la matière. Ces rôles et responsabilités concernent l'approbation, la mise en place, la coordination, le développement, le suivi et l'évaluation de la sécurité de l'information dans l'établissement.
Politique relative à la tenue de dossier et la protection des renseignements personnels	• Précisions sur le contenu et les règles de gestion des dossiers d'usagers; • Règles afin d'assurer l'intégralité et l'accessibilité au dossier de l'usager; • Règles de consultation à l'interne du dossier de l'usager; • Ce qui est prévu en cas de dérogation aux obligations de confidentialité; • Définition du droit d'accès de l'usager à son dossier et du droit de rectification; • Encadrement de la demande d'accès au dossier d'un usager par des tiers; • Mode de transmission de renseignements personnels recommandés; • Clarification des rôles et responsabilités des divers intervenants dans l'application de cette politique.
Directive relative à la tenue et la gestion du dossier de l'usager	• Définitions relatives à l'usager et au dossier; • Définitions relatives à la pratique professionnelle; • Précisions sur les modalités liées au fonctionnement du Service des archives, à l'ouverture d'un dossier, au dossier en CLSC, au dossier parallèle, au dossier de groupe, au dossier communautaire, à la tenue de dossier de l'usager, à la fin du suivi et à la conservation; • Sanctions en cas de non-respect de cette directive.
Directive relative à la consultation et à l'accès au dossier de l'usager	• Précisions sur les modalités liées à l'accès au dossier des usagers et le droit de consultation, le dossier d'adoption, le changement de nom ou de sexe et la circulation de renseignements personnels; • Règles générales sur la confidentialité du dossier de l'usager, la confidentialité des renseignements de tiers, les obligations de l'intervenant ainsi que le secret professionnel; • Spécifications liées au consentement écrit, au délai d'accès au dossier, à la tarification, à l'assistance professionnelle et au droit d'accompagnement;

Documents administratifs	Mesures prévues pour assurer la confidentialité, la protection et la sécurité des renseignements personnels

	• Précisions des modalités pour différents types de demandes d'accès :
	  ○ Par l'usager, son représentant ou un tiers dûment autorisé;
	  ○ Sans autorisation de l'usager ou son représentant légal;
	  ○ Pour un usager décédé;
	  ○ Par un centre jeunesse d'une autre région;
	• Sanctions en cas de non-respect de cette directive.

Procédure relative à l'accès au dossier de l'usager à des fins de recherche	• Marche à suivre en lien avec l'accès au dossier à des fins de recherche : approbation du comité d'éthique de la recherche, demande d'accès au dossier avec ou sans consentement de l'usager, modalités d'accès au dossier, consultation de dossier en vue de présélection, consultation par une ressource externe (organisme autorisé), contact avec l'usager par l'intermédiaire de l'archiviste médical, classement du formulaire d'information et de consentement au dossier de l'usager, demande de conservation de dossiers d'usagers, frais si applicable, modalités pour demander une prolongation des accès aux dossiers et possibilité de révocation des accès; • Clarification des rôles et responsabilités de différents acteurs de l'établissement en lien avec l'accès au dossier à des fins de recherche.
Politique relative à la protection des données et des renseignements personnels dans le cadre de toute activité de recherche impliquant des sujets humains	• Règles relatives à la gestion, la sécurité des données et la confidentialité des données recueillies dans le cadre de toute activité de recherche; • Exigences et responsabilités quant à toute activité de recherche, à la gestion de tout dossier de recherche et toute banque; • Règles concernant la constitution, la conservation et la gestion de toute banque; • Modalités afin de veiller à ce que toute banque soit utilisée de manière scientifique et éthique, au bénéfice des participants et de la collectivité; • Règles concernant la propriété intellectuelle et les ententes contractuelles à être conclues de tout banque, le cas échéant; • Modalités pour la création d'une liste de noms pour des projets de recherche futurs.
Directive relative à l'utilisation des postes informatiques, de l'Internet et du courriel	• Description de ce que les utilisateurs des postes informatiques, de l'Internet et des réseaux informatiques de l'établissement doivent faire et ce qu'ils ne doivent pas faire afin d'assurer le bon emploi des ressources et la sécurité des actifs informationnels; • Description des responsabilités de l'utilisateur à qui est octroyé, dans le cadre de ses fonctions, le privilège d'utiliser le courriel vérifié et fourni par le Réseau de la santé et des services sociaux; • Sanctions pouvant être imposées pour non-respect de cette directive.
Politique de gestion des accès aux actifs informationnels numériques	• Lignes directrices qui visent à encadrer les conditions par lesquelles l'accès aux actifs informationnels numériques du CIUSSS de la Capitale-Nationale est permis; • Précisions sur les modalités d'identification et d'authentification des utilisateurs; • Définition des responsabilités des différents intervenants en lien avec l'accès aux actifs informationnels numériques.

Documents administratifs	Mesures prévues pour assurer la confidentialité, la protection et la sécurité des renseignements personnels
Procédure du président-directeur général relative à la communication d'un renseignement contenu au dossier de l'usager en vue de protéger l'usager, une autre personne ou le public dans certaines circonstances	• Conditions et modalités requises pour la communication en vue de prévenir un acte de violence, dont le suicide, avec ou sans arme à feu; • Conditions et modalités requises pour le signalement d'une personne blessée par le projectile d'une arme à feu; • Précisions sur les autres circonstances pour lesquelles la divulgation de renseignements contenus au dossier de l'usager est autorisée aux fins de la protection de l'usager ou du public; • Clarification des rôles et responsabilités de différents acteurs de l'établissement en lien avec la communication d'un renseignement contenu au dossier de l'usager en vue de protéger l'usager, une autre personne ou le public dans certaines circonstances.
Politique relative au télétravail	• Critère d'admissibilité au télétravail prévoyant que l'employé doit disposer d'un environnement de travail assurant la confidentialité et la sécurité des données; • Précision sur le rôle du gestionnaire qui doit veiller à ce que le télétravailleur respecte les règles et la politique concernant la confidentialité, la sécurité des données et la protection des renseignement personnels.
Politique relative à la télésanté	Obligations prévues pour les professionnels lors d'un soin ou service en télésanté : • Utiliser les plateformes et logiciels approuvés par l'établissement et le MSSS; • Utiliser les adresses courriel sécurisées du réseau de la santé et des services sociaux; • Recourir à un mécanisme de chiffrement supplémentaire approuvé par le MSSS et par l'établissement lors d'échanges courriel incluant des données nominatives ou confidentielles avec un destinataire externe; • Rappeler les consignes de confidentialité à domicile; • S'assurer que l'environnement est configuré de sorte que les soins et services soient administrés dans le respect de la confidentialité (ex. : utiliser les fonds d'écran reconnus et autorisés par l'établissement, favoriser l'usage d'un casque d'écoute avec microphone, si possible); • Juger de la pertinence de l'accompagnement par une tierce personne et des enjeux liés à la confidentialité; • Se questionner sur les enjeux de sécurité et de confidentialité des données lors des échanges et prendre des décisions sur les précautions à prendre.

ANNEXE 4

MESURES MINIMALES DE SÉCURITÉ EXIGÉES PAR LE MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE

1. Inventaire et désuétude du matériel et des systèmes d'exploitation
2. Détection des vulnérabilités et application des correctifs
3. Déploiement d'un antivirus à jour et moderne
4. Authentification multi-facteurs
5. Copies de sauvegarde, tests de couvrement et relève
6. Solution de courriel sécurisée
7. Balayage des vulnérabilités des applications externes
8. Journalisation et surveillance continue des systèmes exposés
9. Authentification aux services externes critiques protégée par un dispositif CAPTCHA
10. Notifications d'accès et de changements au compte
11. Transmissions sécuritaires des informations autre que le courriel
12. Campagne de simulation à l'hameçonnage de façon continue
13. Directive sur l'utilisation du courriel et de l'Internet
14. Gestion des accès accordés aux utilisateurs
15. Plan de sensibilisation du personnel

ANNEXE 5

COORDONNÉES DU COMMISSAIRE AUX PLAINTES ET À LA QUALITÉ DES SERVICES DU CIUSSS DE LA CAPITALE-NATIONALE ET DE LA COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC

COMMISSAIRE AUX PLAINTES ET À LA QUALITÉ DES SERVICES (CPQS) :

Site Internet : Page du Commissariat sur le site Internet de l'établissement

Téléphone : 418 691-0762 ou, sans frais, 1 844 691-0762

Télécopieur : 418 643-1611

Courriel : commissaire.plainte.ciussscn@ssss.gouv.qc.ca

Poste : Commissariat aux plaintes et à la qualité des services
CIUSSS de la Capitale-Nationale
2915, avenue du Bourg-Royal, bureau 3005.1
Québec (Québec) G1C 3S2

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC (CAI) :

Site Internet : Commission d'accès à l'information du Québec

Téléphone : 418 528-7741 ou, sans frais, 1 888 528-7741

Télécopieur : 418 529-3102

Courriel : renseignements@cai.gouv.qc.ca

Poste : Commission d'accès à l'information du Québec
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9