

POLITIQUE

Code : PO-68

Direction responsable : Direction de services professionnels

Approuvée par : Elyse Berger-Pelletier

Adoptée par le président-directeur général le : 2024-10-01

Adoptée par le conseil d'administration le : Non applicable

Résolution no : Non applicable

Entrée en vigueur le : 2024-10-01

Cette politique annule la politique no : Non applicable

TITRE : Politique de confidentialité relative au recueil de renseignements personnels par l'entremise de l'application FMRQ Mobile

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 :

Table des matières

1.	FONDEMENTS	3
2.	PRINCIPES	3
3.	OBJECTIF	3
4.	CHAMP D'APPLICATION	3
5.	DÉFINITIONS	3
6.	RENSEIGNEMENTS PERSONNELS	4
6.1	<i>NOM DU TIERS QUI RECUEILLE DES RENSEIGNEMENTS PERSONNELS POUR LE CIUSSS DE LA CAPITALE-NATIONALE</i>	4
6.2	<i>RENSEIGNEMENTS PERSONNELS RECUEILLIS</i>	4
6.3	<i>FINS AUXQUELLES LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS</i>	4
6.4	<i>CATÉGORIES DE PERSONNES QUI, AU SEIN DU CIUSSS DE LA CAPITALE-NATIONALE, ONT ACCÈS AUX RENSEIGNEMENTS PERSONNELS RECUEILLIS</i>	4
6.5	<i>MOYENS PAR LESQUELS LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS</i>	4
6.6	<i>DROITS D'ACCÈS ET DE RECTIFICATION ET PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DU CIUSSS DE LA CAPITALE-NATIONALE</i>	4
6.7	<i>COMMUNICATION DES RENSEIGNEMENTS PERSONNELS</i>	5
6.8	<i>POSSIBILITÉ QUE LES RENSEIGNEMENTS PERSONNELS SOIENT COMMUNIQUÉS À L'EXTÉRIEUR DU QUÉBEC</i>	5
6.9	<i>MESURES PRISES POUR ASSURER LA CONFIDENTIALITÉ ET LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS</i>	5
6.10	<i>DROIT DE PORTER PLAINTÉ</i>	5
7.	MODIFICATIONS DE LA POLITIQUE	6
8.	COORDONNÉES UTILES	6
9.	RESPONSABILITÉS	6
10.	ENTRÉE EN VIGUEUR	6
11.	ANNEXES	7

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) ;
- *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 utilisateurs de l'application FMRQ Mobile déployée dans le cadre des activités de recrutement de médecins pour le Département régional de médecine générale (DRMG) de la Capitale-Nationale et la Direction des services professionnels (DSP) 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 utilisateurs de l'application FMRQ Mobile déployée dans le cadre des activités de recrutement de médecins pour le Département régional de médecine générale de la Capitale-Nationale (DRMG) et la Direction des services professionnels (DSP) du CIUSSS de la Capitale-Nationale.

5. DÉFINITIONS

FMRQ

La Fédération des médecins résident-e-s du Québec (FMRQ) est un syndicat professionnel qui regroupe les associations de médecins résident-e-s des quatre facultés de médecine de Montréal, McGill, Sherbrooke et Laval à Québec. La FMRQ a pour objet l'étude, la défense et le développement des intérêts financiers, sociaux, moraux, académiques et professionnels des syndicats et de leurs membres.

UTILISATEURS

Médecins résidents en médecine de famille ou en spécialité qui créent un profil sur l'application FMRQ Mobile. Personnel de soutien administratif impliqué dans les processus de recrutement de la DSP et du DRMG.

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 recueillir des renseignements personnels sur des candidats intéressés à travailler dans la Capitale-Nationale, soit l'application FMRQ Mobile. Pour plus d'information sur ce fournisseur, nous vous référons à l'annexe 1.

6.2 RENSEIGNEMENTS PERSONNELS RECUEILLIS

L'application FMRQ Mobile permet de recueillir des renseignements personnels des utilisateurs. L'utilisateur crée lui-même son profil sur l'application FMRQ Mobile avec ses renseignements personnels. L'utilisateur partage lui-même ses renseignements à partir de l'application. Ceux-ci peuvent entre autres inclure :

- Nom, prénom
- Adresse de courriel
- Identifiant de l'utilisateur
- Adresse postale
- Numéro de téléphone cellulaire

6.3 FINS AUXQUELLES LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS

Les renseignements recueillis permettront à la DSP et au DRMG de communiquer directement avec l'utilisateur pour lui transmettre des informations en lien avec les besoins d'effectifs médicaux dans la Capitale-Nationale et au CIUSSS, ainsi que les différentes procédures pour obtenir un avis de conformité et un avis de nomination.

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

- Techniciennes en administration de la DSP
- Techniciennes en administration du DRMG

6.5 MOYENS PAR LESQUELS LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS

Une fois que l'utilisateur a complété son profil contenant ses renseignements personnels sur l'application FMRQ Mobile, il peut partager son profil à un autre utilisateur de la même application à l'aide d'un code QR.

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

L'application FMRQ Mobile permet de rectifier les renseignements personnels par l'utilisateur. Dans l'éventualité où une démarche de recrutement se formalise, la validation des renseignements personnels sera demandée à l'utilisateur.

6.7 COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

Les renseignements personnels recueillis par l'entremise de l'application FMRQ Mobile sont soumis aux protections prévues par la Loi sur l'accès.

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

Les renseignements personnels recueillis par l'entremise de l'application FMRQ Mobile sont hébergés au Québec et ne sont pas communiqués à l'extérieur de la province.

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 2) ;
- 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 3) ;
- 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.

6.10 DROIT DE PORTER PLAINTÉ

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 4.

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 la technicienne en administration avec qui vous échangez des informations par l'entremise de l'application FMRQ Mobile. Au besoin, celui-ci peut communiquer par courriel avec le DRMG à l'adresse : drmg.ciusssc@sss.gouv.qc.ca.

9. RESPONSABILITÉS

DIRECTION DES SERVICES PROFESSIONNELS ET DÉPARTEMENT RÉGIONAL DE MÉDECINE GÉNÉRALE DE LA CAPITALE-NATIONALE

- 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 juridiques, 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 DRMG.

10. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le 1^{er} octobre 2024. Elle doit être révisée aux 3 ans ou au besoin.

11. ANNEXES

Annexe 1 : Fournisseur FMRQ pour le CIUSSS de la Capitale-Nationale

Annexe 2 : 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 3 : Mesures minimales de sécurité exigées par le ministère de la Cybersécurité et du Numérique

Annexe 4 : Coordonnées du CPQS et de la CAI

ANNEXE 1

FOURNISSEUR DE L'APPLICATION FMRQ MOBILE POUR LE CIUSSS DE LA CAPITALE-NATIONALE

Le fournisseur de l'application FMRQ Mobile est La Fédération des médecins résident·e·s du Québec (FMRQ). Celui-ci recueille les renseignements personnels au bénéfice de la DSP et du DRMG de la Capitale-Nationale.

Politique de confidentialité de la FMRQ : [Politique de confidentialité - FMRQ](#)

Adresse

630 rue Sherbrooke Ouest, bureau 510
Montréal, Québec, Canada
H3A 1E4

Téléphone

514 282-0256

Courriel

info@fmrq.qc.ca

ANNEXE 2

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Précisions sur le contenu et les règles de gestion des dossiers d'utilisateurs ;• Règles afin d'assurer l'intégrité et l'accessibilité au dossier de l'utilisateur ;• Règles de consultation à l'interne du dossier de l'utilisateur ;• Ce qui est prévu en cas de dérogation aux obligations de confidentialité ;• Définition du droit d'accès de l'utilisateur à son dossier et du droit de rectification ;• Encadrement de la demande d'accès au dossier d'un utilisateur 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'utilisateur	<ul style="list-style-type: none">• Définitions relatives à l'utilisateur 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'utilisateur, 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'utilisateur	<ul style="list-style-type: none">• Précisions sur les modalités liées à l'accès au dossier des utilisateurs 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'utilisateur, la confidentialité des renseignements de tiers, les obligations de l'intervenant ainsi que le secret professionnel ;

Documents administratifs	Mesures prévues pour assurer la confidentialité, la protection et la sécurité des renseignements personnels
	<ul style="list-style-type: none"> • Spécifications liées au consentement écrit, au délai d'accès au dossier, à la tarification, à l'assistance professionnelle et au droit d'accompagnement ; • Précisions des modalités pour différents types de demandes d'accès : <ul style="list-style-type: none"> – Par l'utilisateur, son représentant ou un tiers dûment autorisé ; – Sans autorisation de l'utilisateur ou son représentant légal ; – Pour un utilisateur 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'utilisateur à des fins de recherche	<ul style="list-style-type: none"> • 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'utilisateur, modalités d'accès au dossier, consultation de dossier en vue de présélection, consultation par une ressource externe (organisme autorisé), contact avec l'utilisateur par l'intermédiaire de l'archiviste médical, classement du formulaire d'information et de consentement au dossier de l'utilisateur, demande de conservation de dossiers d'utilisateurs, frais si applicables, 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	<ul style="list-style-type: none"> • 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 toute 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Lignes directrices qui visent à encadrer les conditions par lesquelles l'accès aux actifs informationnels numériques du CIUSSS de la Capitale-Nationale est permis ;

Documents administratifs	Mesures prévues pour assurer la confidentialité, la protection et la sécurité des renseignements personnels
	<ul style="list-style-type: none"> • 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.
Procédure du président-directeur général relative à la communication d'un renseignement contenu au dossier de l'utilisateur en vue de protéger l'utilisateur, une autre personne ou le public dans certaines circonstances	<ul style="list-style-type: none"> • 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'utilisateur est autorisée aux fins de la protection de l'utilisateur 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'utilisateur en vue de protéger l'utilisateur, une autre personne ou le public dans certaines circonstances.
Politique relative au télétravail	<ul style="list-style-type: none"> • 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 renseignements personnels.
Politique relative à la télésanté	<p>Obligations prévues pour les professionnels lors d'un soin ou service en télésanté :</p> <ul style="list-style-type: none"> • 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 3

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 multifacteurs.
5. Copies de sauvegarde, tests de couverture 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 autres 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.
16. Gestion sécuritaire des appareils mobiles.
17. Documentation des infrastructures technologiques.
18. Journalisation des événements de sécurité.

ANNEXE 4

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.ciusscn@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