Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale Québec	**POLITIQUE**
	Code : PO-71
	Direction responsable : Direction des ressources informationnelles Approuvée par : Geneviève Bouchard
	Adoptée au comité de direction le : 5 novembre 2024
	Adoptée par le conseil d'administration le : Non applicable Résolution no : Non applicable
	Entrée en vigueur le : 5 novembre 2024 Cette politique annule la politique no : Non applicable
TITRE : Politique de confidentialité relative au recueil de renseignements personnels des usagers par l'entremise des formulaires disponibles sur le site Internet du CIUSSS de la Capitale-Nationale	

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

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

- Loi sur les renseignements de santé et de services sociaux (RLRQ, chapitre R-22.1, ci-après la « LRSSS »)

2. PRINCIPES

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

3. OBJECTIF

Permettre aux usagers qui utilisent les formulaires sur la plateforme technologique Voxco, déployée 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 les formulaires recueillant des renseignements personnels déployés dans certains programmes cliniques du CIUSSS de la Capitale-Nationale.

5. DÉFINITIONS

Usager
Toute personne ou tout groupe à qui sont fournis des services prévus dans le cadre de la mission du CIUSSS de la Capitale-Nationale.

Renseignement personnel
Est un renseignement qui permet d'identifier une personne physique, **directement** ou **indirectement**. Les renseignements personnels sont confidentiels. Leur confidentialité découle du droit à la vie privée, permettant à toute personne d'exercer un contrôle sur l'utilisation et la circulation de ses renseignements.

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 au fournisseur Voxco, lequel recueille des renseignements personnels par l'entremise de formulaires disponibles sur le site Internet de l'établissement. Pour plus d'information sur ce fournisseur, nous vous référons à l'annexe 1.

6.2 RENSEIGNEMENTS PERSONNELS RECUEILLIS

Les formulaires permettent de recueillir des renseignements personnels des usagers. Ceux-ci peuvent entre autres inclure:

- Nom et prénom;
- Date de naissance;
- Âge;
- Sexe;
- Genre;
- Adresse civique;
- Numéro d'assurance sociale;
- Numéro de téléphone;
- Adresse courriel;
- Comportement émotionnel;
- Soins et services de proximité;
- État de santé physique et psychologique;
- Rapport médical;
- Rapport professionnel;
- Profil pharmacologique;
- Résumé du dossier;
- Et toutes autres informations de même nature.

6.3 FINS AUXQUELLES LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS

Dans le respect de la législation, les renseignements personnels sont recueillis afin de permettre notamment au CIUSSS de la Capitale-Nationale de :

- Identifier les besoins des usagers dans le but de leur fournir les services appropriés;
- Effectuer des suivis professionnels ou médicaux auprès des usagers concernés;
- Obtenir un rapport de situation émotionnelle ou personnelle ou médicale avant un rendez-vous de la part de l'usager;
- Partager de l'information entre professionnels pour le suivi d'un dossier usager.

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

- Médecins et résidents;
- Professionnels de la santé et des services sociaux;

- Archivistes médicales;
- La commissaire aux plaintes et à la qualité et/ou le médecin examinateur, pour toute situation en lien avec l'application du règlement no. 4: règlement relatif à la procédure d'examen des plaintes;
- Et toutes autres personnes qui ont la qualité pour le recevoir au sein du CIUSSS de la Capitale-Nationale lorsque la législation l'autorise.

6.5 MOYENS PAR LESQUELS LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS

Les renseignements personnels sont recueillis par la plateforme Voxco par l'entremise des formulaires électroniques sécurisés répondant aux normes de sécurité de l'établissement et du gouvernement du Québec.

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 de la plateforme Voxco sont soumis aux protections prévues par la LRSSS.

La LRSSS 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. Cette loi 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 de la plateforme Voxco sont hébergés au Canada.

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 les mesures présentées à l'annexe 1.

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 au Centre d'assistance informatique via l'adresse suivante : centre.assistance.ri.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 le Service des archives de la Direction des services multidisciplinaires et la Direction des affaires juridiques, institutionnelles et corporatives et des communications;
- Diffuser la présente politique sur le site Internet de l'établissement en collaboration avec le Service des communications de la Direction des affaires juridiques, institutionnelles et corporatives et des communications;
- Répondre aux questions sur la présente politique transmise par courriel.

DIRECTIONS DE PROGRAMMES CLINIQUES QUI ONT RECOURS AU FOURNISSEUR VOXCO:

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

10. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le 5 novembre 2024. Elle doit être révisée tous les 3 ans ou au besoin.

11. ANNEXES

Annexe 1 : Fournisseur Voxco 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 VOXCO POUR LE CIUSSS DE LA CAPITALE-NATIONALE

Le fournisseur de la plateforme est Voxco, ci-après désigné par Fournisseur.

Les informations du Fournisseur peuvent être consultées au https://www.voxco.com/fr/contact-us/

Coordonnées de Voxco:

1440 St. Catherine Street
West Suite 900
Montréal, Québec, Canada
H3A-3L6
1-514-861-9255

ENGAGEMENT DU FOURNISSEUR CONCERNANT LA SÉCURITÉ DE L'INFORMATION :

Le Fournisseur s'engage à respecter la Loi en matière de protection des renseignements personnels et confidentiels comme prévu à l'entente intervenue avec le CIUSSS de la Capitale-Nationale et dont les modalités pertinentes sont ici reproduites :

GOUVERNANCE

a) **Interdiction**
Le Fournisseur s'engage à ce que ni lui, ni aucun de ses employés, agents, représentants ou sous-traitants ne divulguent ou n'utilisent à d'autres fins que pour l'exécution du Contrat, sans y être dûment autorisés par le CIUSSS de la Capitale-Nationale, l'Information gouvernementale qui leur est communiquée dans le cadre du Contrat découlant du présent appel d'offres ou qui est générée à l'occasion de son exécution ou, plus généralement, quoi que ce soit dont ils auraient eu connaissance dans le cadre de l'exécution du Contrat.

b) **Règles de sécurité**
i) Respect
Le FOURNISSEUR s'engage à respecter les politiques, directives et autres règles de sécurité applicables à l'Information gouvernementale et identifiées par le CIUSSS de la Capitale-Nationale. À cet égard, le FOURNISSEUR s'engage à ce que toute personne qui participe à l'exécution du Contrat s'engage à respecter ces politiques, directives et autres règles de sécurité.
ii) Avis en cas de manquement
Le FOURNISSEUR s'engage à aviser sans délai le CIUSSS de la Capitale-Nationale de tout manquement, violation ou tentative de violation de ces politiques, directives et autres règles de sécurité, ainsi que de tout événement de sécurité.

c) **Mesures**
i) Valeur de l'Information gouvernementale
Le FOURNISSEUR s'engage à appliquer les Mesures de Sécurité de l'Information en fonction de la valeur de l'Information gouvernementale déterminée par le CIUSSS de la Capitale-Nationale.
ii) Compte-rendu
Le FOURNISSEUR s'engage également, dans un délai à convenir entre les PARTIES, à informer le CIUSSS de la Capitale-Nationale des mesures prises en vertu du paragraphe i) de la présente clause.
Dans le cas où le CIUSSS de la Capitale-Nationale estime que les Mesures de Sécurité de l'Information mises en place sont insuffisantes, il peut demander au FOURNISSEUR d'y apporter des modifications aux frais de ce dernier, le cas échéant.

iii) Autorisation préalable

Lorsque l'Information gouvernementale doit être conservée, utilisée ou communiquée à l'extérieur des installations du CIUSSS de la Capitale-Nationale, le FOURNISSEUR s'engage à obtenir du CIUSSS de la Capitale-Nationale son autorisation préalable et à prendre, à la satisfaction du CIUSSS de la Capitale-Nationale, toutes les Mesures de Sécurité de l'Information requises.

d) **Vérification**

Le CIUSSS de la Capitale-Nationale peut procéder, sur préavis raisonnable, à une vérification de la conformité du FOURNISSEUR aux politiques, directives et autres règles de sécurité identifiées par le CIUSSS de la Capitale-Nationale en vertu de la clause b) i). Cette vérification est effectuée par le CIUSSS de la Capitale-Nationale ou par toute personne autorisée par celui-ci. À la suite de cette vérification de la sécurité, le CIUSSS de la Capitale-Nationale peut prendre toute mesure qu'il juge appropriée.

e) **Responsable de la Sécurité de l'Information**

Le FOURNISSEUR doit désigner, au sein de son organisation, un responsable de l'application des Mesures de Sécurité de l'Information et communiquer son nom et ses coordonnées au CIUSSS de la Capitale-Nationale dans les DIX (10) jours suivant l'adjudication du Contrat.

ÉVÉNEMENTS DE SÉCURITÉ

a) **Processus de gestion des Événements de Sécurité**

Le FOURNISSEUR s'engage à mettre en place un processus et des procédures de gestion des Événements de Sécurité qui permettent une intervention rapide, efficace et pertinente, lorsque requis.

Sur demande du CIUSSS de la Capitale-Nationale, le FOURNISSEUR doit lui transmettre une copie du processus et des procédures mises en place.

b) **Signalement des Événements de Sécurité**

Le FOURNISSEUR doit signaler immédiatement tout Événement de Sécurité au CIUSSS de la Capitale-Nationale. Ce signalement doit minimalement inclure les informations suivantes :

i) Une description de l'Événement de Sécurité et de son objet, de ses circonstances et de ses causes;
ii) Une description de l'Information gouvernementale visée par l'Événement de Sécurité;
iii) La date et l'heure de l'occurrence et/ou de la détection;
iv) L'évaluation de la gravité;
v) L'évaluation du nombre de personnes concernées par l'Événement de Sécurité, le cas échéant;
vi) L'identification des préjudices potentiels;
vii) Le nom et les coordonnées de toute autre personne susceptible de contribuer à la résolution de l'Événement de Sécurité.

c) **Gestion des Événements de Sécurité**

Dès qu'elle est disponible, le FOURNISSEUR doit transmettre au CIUSSS de la Capitale-Nationale, promptement et sécuritairement, toute information nécessaire à la compréhension, au suivi et à la résolution de l'Événement de Sécurité, de même qu'à l'atténuation des préjudices ou des risques encourus. Il doit également communiquer toute autre information pertinente demandée par le CIUSSS de la Capitale-Nationale, dans les plus brefs délais.

En tout temps, le FOURNISSEUR doit agir avec diligence et collaborer avec le CIUSSS de la Capitale-Nationale ainsi qu'avec toute personne que ce dernier désigne, dans le but de diminuer les risques

qu'un préjudice soit causé et éviter que de nouveaux Événements de Sécurité de même nature ne se produisent. À ce titre, le FOURNISSEUR doit notamment :

i) Appliquer et documenter, avec diligence, les mesures nécessaires à la résolution de l'Événement de Sécurité et à l'atténuation des préjudices ou des risques encourus;
ii) Rendre compte au CIUSSS de la Capitale-Nationale ou à la personne qu'il désigne, de l'application et de l'efficacité de ces mesures;
iii) Collecter et préserver les éléments de preuve susceptibles de démontrer les faits entourant l'Événement de Sécurité ainsi que sa gestion.

d) **Suivi des événements de sécurité**

Dès que possible, le FOURNISSEUR doit entreprendre une enquête pour identifier la cause de l'Événement de Sécurité. Il doit également produire et communiquer promptement au CIUSSS de la Capitale-Nationale un rapport post-événement, consignant notamment :

i) La ou les causes;
ii) Les actions entreprises;
iii) Les mesures de sécurité mises en place pour éviter que de nouveaux événements de sécurité de même nature ne se produisent.

ACCEPTATION D'INSCRIPTION AU PROGRAMME PRIME AUX BOGUES

Le FOURNISSEUR accepte son inscription au Programme de primes aux bogues mis en place par le Centre gouvernemental de cyberdéfense depuis septembre 2023.
Le Programme en référence vise à structurer et à renforcer les interventions pour assurer une cybersécurité au sein du gouvernement. Le Programme contribue aussi à renforcer la résilience des actifs informationnels de l'administration publique.
Voici plus d'informations sur le programme (YesWeHack : Centre gouvernemental de cyberdéfense: Programme prime bogues).

TEST DE PÉNÉTRATION

LE FOURNISSEUR autorise le CIUSSS de la Capitale-Nationale à demander aux Centres opérationnels de cyberdéfense - COCD et au ministère de la cybersécurité et du numérique – MCN de procéder à des tests de pénétration (Pentest) pour valider la conformité de la solution avant sa mise en production ainsi que la résolution des vulnérabilités trouvées pendant le test de pénétration et prime aux bogues.

DÉLAIS DE SOLUTION DE MENACES

LE FOURNISSEUR doit s'assujettir aux différents délais de résolution des menaces, vulnérabilités et incidents dans les délais contractuels avec le CIUSSS de la Capitale-Nationale.
Lorsqu'un appel de service ou une panne est détecté par le CIUSSS de la Capitale-Nationale, ce dernier assigne un niveau de priorité au problème selon le classement suivant :

- **Problème critique** : problème d'une très grande importance qui met en péril la sécurité du CIUSSS de la Capitale-Nationale ou sa capacité à réaliser sa mission. Ce problème doit être résolu dans les plus brefs délais;
- **Problème majeur** : problème d'une grande importance ayant un impact sur la sécurité du CIUSSS de la Capitale-Nationale ou sur la réalisation de sa mission;
- **Problème mineur** : problème de moindre importance ayant peu d'impact sur la sécurité et/ou la mission du CIUSSS de la Capitale-Nationale;
- **Délai de confirmation de prise en charge** : période allouée au manufacturier pour entrer en contact avec le CIUSSS de la Capitale-Nationale une fois que l'incident a été ouvert;

• **Délai de résolution** : période allouée au manufacturier pour résoudre le problème avec le CIUSSS de la Capitale-Nationale;
• **Pénalités :** les pénalités sont sous forme d'ordre monétaire par journée de non-résolution.

Niveau de gravité	**Délai de confirmation de prise en charge**	**Délai de résolution**	**Pénalités**
Problème critique	0,5 heure	4 heures	100$/jour
Problème majeur	1 heure	48 heures	50$/jour
Problème mineur	4 heures	5 jours	20$/jour

EMPLOYÉS

Le FOURNISSEUR est responsable des actes et omissions de ses employés et de ses représentants autorisés dans l'accomplissement des obligations qui leur incombent en vertu du Contrat et aucune disposition de celui-ci ne peut être interprétée de manière à libérer le FOURNISSEUR d'une quelconque responsabilité lui incombant.

IDENTIFICATION

Le personnel du FOURNISSEUR doit porter en tout temps des papiers officiels d'identification personnelle et d'identification du FOURNISSEUR.

CONDUITE

Le FOURNISSEUR doit, en tout temps, faire preuve de diligence, d'intégrité, de probité et de bonne foi à l'endroit des personnes qu'il sollicite pour intervenir dans le cadre de la prestation des Services. Il doit en outre s'assurer de la bonne tenue de ses employés et limiter leurs déplacements dans l'édifice aux exigences particulières des Services à rendre.

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
Téléc. : 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 LE 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;

Documents administratifs	Mesures prévues pour assurer la confidentialité, la protection et la sécurité des renseignements personnels
	• 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 : o Par l'usager, son représentant ou un tiers dûment autorisé; o Sans autorisation de l'usager ou son représentant légal; o Pour un usager décédé; o 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 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	• 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	• 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;

Documents administratifs	Mesures prévues pour assurer la confidentialité, la protection et la sécurité des renseignements personnels
	• 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'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 renseignements 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'échange 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 multifacteurs
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 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 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