Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale Québec	**POLITIQUE**
	Code : PO-67
	Direction responsable : Direction de l'enseignement et des affaires universitaires Approuvée par : Martin Lafleur
	Adoptée au comité de direction le : 7 mai 2024
	Adoptée par le conseil d'administration le : Non applicable Résolution no : Non applicable
	Entrée en vigueur le : 7 mai 2024 Cette politique annule la politique no : non applicable

TITRE : Politique de confidentialité relative au recueil de renseignements personnels par l'entremise de sondages en ligne, par les services de l'enseignement de la DEAU

CONSULTATIONS

☐ Conseil des infirmières et infirmiers : Non applicable.
☐ Conseil multidisciplinaire : Non applicable.
☐ Conseil des médecins, dentistes et pharmaciens : Non applicable.
☐ Cadre : 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 des lois et règlements suivants :

- *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 individus qui utilisent les applications technologiques Forms de Microsoft et Lime Santé, déployées dans le cadre de l'organisation des stages d'enseignement au 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 individus qui utilisent Forms de Microsoft et Lime Santé déployés dans le cadre de l'organisation des stages d'enseignement au CIUSSS de la Capitale-Nationale.

5. DÉFINITIONS

TERME 1 : Étudiant
Toute personne inscrite à un établissement d'enseignement reconnu du Québec, à une activité ou un programme de formation pratique universitaire, collégial ou de formation professionnelle.

TERME 2 : STAGES D'ENSEIGNEMENT
Ensemble d'activités supervisées, d'une durée déterminée, prévu à un programme de formation pratique d'un établissement d'enseignement reconnu par le ministère de l'Éducation et/ou le ministère de l'enseignement supérieur du Québec, et se déroulant dans les installations du CIUSSS de la Capitale-Nationale. La notion de stages d'enseignement exclut les visites d'exploration ou d'observation du milieu qui permettent aux personnes de faire un choix d'étude, ou tout autre motif ne contribuant pas directement à la diplomation d'un programme d'études reconnu.

TERME 3 : STAGIAIRE
Toute personne qui effectue un stage dans les installations du CIUSSS de la Capitale-Nationale.

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 des fournisseurs (des tiers) pour recueillir des renseignements nécessaires à l'organisation de stages d'enseignement dans ses installations. Ces derniers recueillent des renseignements personnels par l'entremise de sondages en ligne. Pour plus d'information sur ces fournisseurs, se reporter à l'annexe 1.

6.2 RENSEIGNEMENTS PERSONNELS RECUEILLIS

Forms de Microsoft et Lime Santé permettent de recueillir des renseignements personnels des étudiants dans les milieux de stages d'enseignement au CIUSSS de la Capitale-Nationale. Dépendamment du type de stagiaire, ceux-ci peuvent notamment inclure, lorsque nécessaire:

- Pour les stages médicaux incluant les médecins résidents qui sont employés par le CIUSSS :
    - Date de naissance;
    - Adresse;
    - Numéro d'assurance sociale;
    - Code permanent du réseau de l'éducation;
    - Numéro de permis de pratique;
    - Renseignements bancaires;
    - Données relatives à l'impôt des particuliers;
    - Statut vaccinal;
    - Données sur les antécédents judiciaires;
    - Renseignements relatifs au travail lorsque le stagiaire est également employé.
- Pour les stages d'autres disciplines :
    - Date de naissance
    - Numéro de permis de pratique;
    - Statut vaccinal
    - Données sur les antécédents judiciaires;
    - Renseignements relatifs au travail lorsque le stagiaire est également employé.

6.3 FINS AUXQUELLES LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS

- Constituer le dossier stagiaire de l'individu;
- Constituer le dossier employé du stagiaire qui est, par ailleurs, embauché comme employé;
- Vérifier l'admissibilité à effectuer un stage dans les installations du CIUSSS de la Capitale-Nationale;
- Créer les accès aux applications informatiques requises pendant le stage;
- Créer les accès requis aux installations pendant le stage.

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

- Le personnel administratif des services de l'enseignement du CIUSSS de la Capitale-Nationale pour l'organisation des stages d'enseignement;
- Le personnel administratif de la Direction des ressources humaines pour les aspects en lien avec le dossier employé;
- Le personnel de la Direction des ressources informationnelles, pour les aspects en lien avec les accès aux systèmes informatiques. Ces derniers peuvent transférer l'information au besoin aux pilotes des différents systèmes, dans les directions cliniques et administratives.
- La cheffe des services de l'enseignement, l'adjoint au directeur de l'enseignement et des affaires universitaires ou le directeur de l'enseignement et des affaires universitaires, dans le traitement d'une plainte ou d'un événement particulier;
- 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;
- Les superviseurs de stages d'enseignement et leurs adjoints, pour les demandes d'accès requis en lien avec les différents logiciels nécessaires à la formation des stagiaires sous leur supervision.
- Toute autre personne qui a qualité pour le recevoir au sein du CIUSSS lorsque ce renseignement est nécessaire à l'exercice de ses fonctions.

6.5 MOYENS PAR LESQUELS LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS

Les renseignements personnels sont recueillis dans des sondages en ligne, donc par l'entremise d'un support électronique sécurisé.

6.6 DROITS D'ACCÈS ET DE RECTIFICATION - 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.

Me Annie Caron, Directrice des affaires juridiques et institutionnelles, est responsable de la protection des renseignement personnels pour le volet administratif.

6.7 COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

Les renseignements personnels recueillis par l'entremise des formulaires en ligne 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 des formulaires en ligne sont hébergés au Canada.
- Les renseignements personnels sont exclusivement utilisés pour l'organisation des stages d'enseignement dans les installations du CIUSSS de la Capitale-Nationale et ne peuvent pas être communiquées à l'extérieur du Québec.

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.

6.10 DROIT DE PORTER PLAINTE

La personne concernée par les renseignements personnels, comme tous les usagers du CIUSSS 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 stagiaire ou de son représentant qui concerne la protection des renseignements personnels peut se faire :

- Auprès de la Directrice des affaires juridiques et institutionnelles
- Auprès de la Commission d'accès à l'information du Québec (CAI).

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, s'adresser à enseignement.ciussscn@ssss.gouv.qc.ca.

9. RESPONSABILITÉS

DIRECTION DE L'ENSEIGNEMENT ET DES AFFAIRES UNIVERSITAIRES :

- Développer et réviser, au besoin, la présente politique, et ce, en collaboration avec 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 à enseignement.ciussscn@ssss.gouv.qc.ca.

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 : Fournisseurs pour le CIUSSS de la Capitale-Nationale
Annexe 2 : Coordonnées de la Directrice des affaires juridiques et institutionnelles et de la Commission d'accès à l'information du Québec
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
Annexe 4 : Mesures minimales de sécurité exigées par le ministère de la Cybersécurité et du Numérique

ANNEXE 1
FOURNISSEURS POUR LE CIUSSS DE LA CAPITALE-NATIONALE

Le fournisseur de FORMS est Microsoft. Lorsque cette solution est utilisée pour la collecte de renseignements personnels, une authentification à 2 facteurs est requise. Le répondant doit détenir un compte Microsoft 365 du Réseau de la santé et des services sociaux.

De plus amples informations sont disponibles ici Microsoft Forms | Enquêtes, sondages et questionnaires

Le fournisseur de Lime Santé est la compagnie Lime Health. De plus amples informations sont disponibles ici: Sécurité et confidentialité (lime.Santé)

ANNEXE 2

COORDONNÉES DE LA DIRECTRICE DES AFFAIRES JURIDIQUES ET INSTITUTIONNELLES ET DE LA COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC

Me Annie Caron
Directrice des affaires juridiques et institutionnelles
Dossiers administratifs et employés
2915, av. du Bourg-Royal
Québec, (QC), G1C 3S2
Tél. 418-266-1019 #31430
Télec. 418 661-2845
responsabledelacces.ciussscn@ssss.gouv.qc.ca

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

Commission d'accès à l'information du Québec
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9
Tél. : 418-528-7741 ou sans frais, 1-888-528-7741
Télécopieur : 418-529-3102
Courriel : renseignements@cai.gouv.qc.ca

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

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 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.
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.
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.

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 sécurisé
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