

TITRE :	
CONFIDENTIALITÉ	
EN VIGUEUR LE :	APPROUVÉE PAR :
15 SEPTEMBRE 2025	DIRECTRIE GÉNÉRALE 15 SEPTEMBRE 2025
RÉDIGÉE PAR :	DERNIÈRE RÉVISION :
DIRECTION	15 SEPTEMBRE 2025
AUTRES RÉFÉRENCES :	
À DÉTERMINER	

1. POLITIQUE

L'Équipe de santé familiale communautaire de l'Est d'Ottawa (ÉSFCEO) s'engage à protéger la confidentialité et la vie privée de ses patients*, employés, bénévoles et partenaires conformément aux lois, règlements et normes applicables dans la province de l'Ontario, y compris la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS). Toutes les personnes ayant accès aux renseignements personnels sur la santé (RPS) ou aux renseignements personnels (RP) doivent veiller à leur collecte, utilisation, divulgation, conservation et destruction de manière sécuritaire et appropriée.

2. DÉFINITIONS

Renseignements personnels sur la santé (RPS) : Renseignements identifiables concernant la santé physique ou mentale d'un individu, la prestation de services de santé, les antécédents médicaux, le numéro de carte Santé, ou tout renseignement recueilli dans le cadre de la prestation de soins.

Renseignements personnels (RP) : Renseignements qui permettent d'identifier une personne, tels que le nom, l'adresse, la date de naissance, l'adresse courriel ou le numéro de téléphone.

Dépositaire de renseignements sur la santé (« Health Information Custodian (HIC) » en anglais.) : Personne ou organisme qui a la garde ou le contrôle de RPS dans le cadre de la prestation de soins de santé, tel que défini par la LPRPS.

Consentement : Autorisation donnée par une personne pour la collecte, l'utilisation ou la divulgation de ses renseignements, qui peut être implicite ou explicite selon le contexte, conformément à la LPRPS.

3. RESPONSABILITÉS

Conseil d'administration :

- Adopter et réviser la présente politique.

*Le genre masculin est utilisé comme générique dans le seul but de ne pas alourdir le texte.

- S'assurer que la direction générale met en place des mesures conformes aux lois et normes.

Direction générale :

- Superviser la mise en œuvre de la politique.
- Veiller à ce que la formation sur la confidentialité soit offerte à tous les employés et bénévoles.
- Assurer un mécanisme de plainte et de suivi des incidents liés à la vie privée.

Gestionnaires :

- S'assurer que les procédures de protection des RPS et RP sont respectées.
- Appliquer les protocoles de gestion des incidents de confidentialité.

Employés et bénévoles :

- Respecter en tout temps la politique et les procédures de la clinique.
- Signaler immédiatement toute violation réelle ou potentielle de la vie privée.
- Obtenir un consentement approprié avant de collecter, utiliser ou divulguer des renseignements.

4. PROCÉDURES

Les procédures suivantes s'appliquent à toute collecte, utilisation, divulgation, conservation et destruction de Renseignements personnels sur la santé (RPS) et de Renseignements personnels (RP) au sein de la clinique.

4.1 Collecte des renseignements

- **Consentement préalable** : Obtenir un consentement éclairé (implicite ou explicite) avant de recueillir tout RPS, sauf en cas d'urgence ou d'obligation légale.
- **Pertinence minimale** : Ne recueillir que les renseignements strictement nécessaires pour fournir les soins, gérer le dossier médical ou répondre à une exigence réglementaire.
- **Méthodes sécuritaires** : Utiliser des formulaires approuvés ou un système EMR sécurisé. Les formulaires papier doivent être remis directement au personnel autorisé et ne pas être laissés sans surveillance.

4.2 Utilisation des renseignements

- **But précis** : Utiliser les renseignements uniquement pour les raisons indiquées lors de la collecte ou autorisées par la loi.
- **Accès restreint** : L'accès est limité aux membres du personnel et bénévoles ayant besoin de ces renseignements pour accomplir leurs tâches.
- **Partage interne** : Tout partage de renseignements à l'intérieur de la clinique doit être consigné dans le dossier et respecter les principes de "besoin de savoir".

4.3 Divulgence des renseignements

- **Consentement requis** : Avant de partager des RPS ou RP avec un tiers (p. ex. autre prestataire de soins, organisme communautaire), obtenir un consentement écrit du

patient, sauf si la divulgation est autorisée ou exigée par la loi (p. ex. menace grave, obligation de déclaration).

- **Canaux sécurisés** : Utiliser des moyens sécurisés pour transmettre les renseignements:
 - Fax vers des numéros confirmés
 - Courriel chiffré ou via portail sécurisé
 - Transmission physique en main propre, sous enveloppe scellée
- **Documentation** : Documenter toutes les divulgations dans le dossier du patient, incluant la date, la nature des renseignements partagés, le destinataire et le motif.

4.4 Conservation et archivage

- **Période de conservation** : Conserver les dossiers médicaux pendant au moins 10 ans après la dernière entrée ou, si le patient était mineur, 10 ans après avoir atteint l'âge de 18 ans, conformément aux exigences légales.
- **Classement sécurisé** :
 - Dossiers papier : dans un espace verrouillé avec accès restreint.
 - Dossiers électroniques : sur des serveurs conformes aux normes de sécurité et avec sauvegardes régulières.
- **Inventaire des archives** : Tenir à jour une liste des documents archivés, incluant la date prévue de destruction.

4.5 Destruction sécuritaire

- **Documents papier** : Déchiquetage croisé ou incinération par un fournisseur certifié.
- **Documents électroniques** : Suppression sécuritaire avec écrasement des données, conformément aux normes de l'industrie.
- **Preuve de destruction** : Obtenir et conserver un certificat de destruction pour tout lot de documents éliminés par un fournisseur externe.

4.6 Sécurité et protection physique/électronique

- **Contrôle d'accès** :
 - Utiliser des cartes magnétiques ou clés pour les zones restreintes.
 - Les mots de passe doivent être uniques, robustes et renouvelés tous les 90 jours.
- **Surveillance** : Installer des systèmes de verrouillage et, au besoin, des caméras de sécurité dans les zones d'archivage.
- **Formation annuelle** : Tout le personnel doit suivre une formation annuelle sur la confidentialité et la cybersécurité.

4.7 Gestion des incidents de confidentialité

- **Signalement immédiat** : Tout incident ou soupçon de violation de la vie privée doit être rapporté dans les 24 heures au Responsable de la protection des renseignements personnels (RPRP).
- **Documentation** : Un rapport d'incident doit être complété avec les détails (date, nature, parties impliquées, mesures prises).

- **Notification** : En cas de violation confirmée, le patient et, si requis, le Commissaire à l'information et à la protection de la vie privée de l'Ontario doit/ doivent être avisé.s sans délai.
- **Mesures correctives** : Identifier les causes et mettre en place des actions préventives pour éviter la répétition.

4.8 Consentement et retrait du consentement

- **Documentation du consentement** : Consigner dans le dossier médical la nature du consentement (implicite/explicite), la date et la signature, lorsque requis.
- **Retrait** : Un patient peut retirer son consentement en tout temps; la demande doit être enregistrée immédiatement et confirmée par écrit.

4.9 Utilisation de l'intelligence artificielle et des "IA scribes"

- L'utilisation de l'intelligence artificielle (IA) et des « IA scribes » dans la clinique est assujettie à la **Politique sur l'utilisation de l'intelligence artificielle et des « AI scribes »**.
- Lors de l'utilisation d'un AI scribe :
 - Le consentement explicite du patient doit être obtenu avant toute utilisation, particulièrement en cas d'enregistrement audio.
 - Le patient doit être informé à chaque visite lorsque l'IA scribe est activée.
 - Si le patient retire son consentement, l'utilisation doit cesser immédiatement.

Toutes les données recueillies par un IA scribe sont traitées conformément à la présente politique et aux lois applicables sur la protection de la vie privée.

5. RÉFÉRENCES

Loi sur la protection des renseignements personnels sur la santé (LPRPS / PHIPA) – Ontario:
<https://www.ontario.ca/fr/lois/loi/04p03>

Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) :
<https://www.ipc.on.ca/fr/>

Association médicale de l'Ontario – Ressources sur la confidentialité :
<https://www.oma.org/fr/advocacy/confidentialite-des-patients/>

Bureau du Commissaire à la protection de la vie privée du Canada :
<https://www.priv.gc.ca/fr/>

6. ANNEXES

(À DÉTERMINER)