

FICHER DE RENSEIGNEMENTS PERSONNELS

Tel que le prescrit l'article 76 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1), le Centre intégré de services de santé et de services sociaux de la Montérégie-Ouest (« CISSS Montérégie-Ouest ») rend publiques certaines informations concernant ce fichier contenant des informations personnelles telles que définies par l'article 54 de la même loi.

Date de l'analyse	
--------------------------	--

1. Identification du fichier
Désignation :
Description :

2. Catégories de renseignements contenus dans le fichier	
☐ Renseignements d'identité	☐ Services aux individus
☐ Santé et/ou services sociaux	☐ Permis
☐ Éducation	☐ Logement
☐ Emploi	☐ Loisirs
☐ Vie économique	☐ Organisations
☐ Justice	☐ Démographie
☐ Autre(s) (spécifier) :	

3. Fins pour lesquelles les renseignements sont conservés
☐ Application d'une loi :
☐ Application d'un règlement :
☐ Application d'un programme :
☐ Gestion interne de l'organisme:
☐ À des fins statistiques :
☐ Autre(s) fin(s) (spécifier) :

4. Mode de gestion du fichier	
4.1 Supports physiques	4.2 Mobilité du fichier (si support informatique)
☐ a. Manuel (papier, carton, etc.)	☐ d. Fichier centralisé
☐ b. Mécanique (microfiche, microfilm, etc.)	☐ e. Fichier transportable (clé USB, etc.)
☐ c. Informatique (disque, bande, etc.)	☐ f. Application informatique
Durée générale de conservation des renseignements :	Actif :
	Semi-actif :
	Inactif :

5. Provenance des renseignements versés au fichier
☐ La personne concernée (usager), son représentant légal, un membre de la famille ou un proche
☐ Un membre du personnel
☐ Un médecin
☐ Un autre organisme public :
☐ Un autre organisme privé :
☐ Autre(s) (spécifier) :

6. Catégories de personnes concernées par les renseignements versés au fichier Cochez la ou les cases appropriées
☐ a. L'utilisateur
☐ b. Un proche-aidant, membre de la famille ou représentant légal de l'utilisateur
☐ c. Un membre du personnel
☐ d. Médecins (incluant résidents/internes)
☐ e. Un organisme privé :
☐ f. Un organisme public :
☐ g. Autre(s) (spécifier) :

7. Catégories de personnes ayant accès au fichier dans l'exercice de leurs fonctions
☐ Direction générale
☐ Gestionnaires
☐ Professionnels cliniques
☐ Professionnels administratifs
☐ Personnel administratif
☐ Personnel des archives médicales
☐ Autres membres du personnel
☐ Autre(s) (spécifier) :

8. Mesures de sécurité prises pour assurer la protection des renseignements personnels	
8.1 Pour un fichier manuel ou mécanique	
☐ a. Contrôle des entrées / sorties de personnes	☐ e. Règles et pratiques de destruction
☐ b. Contrôle physique des locaux / installations	☐ f. Signature d'une entente de confidentialité
☐ c. Contrôle à l'utilisation du document	☐ g. Vérification de l'intégrité du personnel
☐ d. Contrôle des procédures	☐ h. Autre(s) (spécifier)
8.2 Pour un fichier informatique	
☐ a. Contrôle préventif de l'accès au fichier	☐ e. Règles et pratiques de vérification du fichier
☐ b. Journaux d'accès aux données	☐ f. Règles et pratiques de destruction
☐ c. Règles et pratiques de vérification des logiciels	☐ g. Signature d'une entente de confidentialité
☐ d. Mesures liées aux outils informatiques	☐ h. Autre(s) (spécifier)
8.3 Pour un fichier mobile	
☐ a. Mécanisme de sécurité adéquats pour la mobilité	
☐ b. Autre(s) (spécifier)	
9. Information complémentaire	

Précisions :

- **8.1 a. Contrôle des entrées / sorties de personnes :** Mécanisme de contrôle de l'accès aux installations (ex. : carte magnétique).
 - **8.1 b. Contrôle physique des locaux / installations :** Verrouillage des espaces et/ou équipements de rangement.
 - **8.1 c. Contrôle à l'utilisation du document :** Mécanisme permettant de contrôler qui consulte un document.
 - **8.1 d. Contrôle des procédures :** Mise en place de procédures d'accès aux documents.
 - **8.1 e. Règles et pratiques de destruction :** Mise en place de procédures de destruction des documents incluant la destruction confidentielle.
 - **8.1 f. Signature d'une entente de confidentialité :** Signature par les employés d'un engagement à garder strictement confidentiels les renseignements consultés.
 - **8.1 g. Vérification de l'intégrité du personnel :** Approbation lors de l'embauche ou de l'entrée en fonction dans des affectations associées à la manipulation ou à la consultation des documents.
-
- **8.2 a. Contrôle préventif de l'accès au fichier :** Attribution d'un identifiant et d'un mot de passe, environnement réseau sécurisé.
 - **8.2 b. Journaux de vérification des données :** Vérification des accès aux fichiers.
 - **8.2 c. Règles et pratiques de vérification des logiciels :** Processus permettant de vérifier et de maintenir la pérennité, l'efficacité et la sécurité des logiciels utilisés.
 - **8.2 d. Mesures liées aux outils informatiques :** Mesures assurant le maintien et l'entretien de l'équipement informatique, y compris l'emplacement sécurisé de ce dernier.
 - **8.2 e. Règles et pratiques de vérification du fichier :** Processus permettant de s'assurer que la signature électronique du fichier demeure la même (veille des modifications ou suppressions).
 - **8.2 f. Règles et pratiques de destruction :** Mise en place de procédures de destruction des documents incluant la destruction confidentielle.
 - **8.2 g. Signature d'une entente de confidentialité :** Signature par les employés d'un engagement à garder strictement confidentiels les fichiers ou les données consultés.
-
- **8.3 a. Mécanisme de sécurité adéquats pour la mobilité :**