

## Mesures de précaution relatives à la protection de la vie privée et à la sécurité du dossier d'évaluation médicale intégré (demi)

Protection de la vie privée et sécurité :

### Mesures de précaution administratives

- Une ou des personnes sont désignées pour veiller au respect de la vie privée et de la sécurité.
- Un cadre de gouvernance organisationnel en place concernant la protection de la vie privée, la confidentialité et la sécurité comprend des rôles et des responsabilités clairement définis.
- Des politiques et procédures organisationnelles concernant la gestion de la vie privée et de la sécurité ont été élaborées puis mises en œuvre; elles font l'objet d'un suivi et on s'assure qu'elles sont respectées. Un mécanisme permet de les revoir et de les actualiser.
- Seul le personnel autorisé peut consulter le DEMI et l'utiliser, selon le principe de connaissance sélective (c'est-à-dire lorsqu'il en a besoin pour accomplir ses tâches).
- Des ententes de non-divulgaration ou de confidentialité régissant tous les employés et membres du personnel, ainsi que les bénévoles et les entrepreneurs, font mention de sanctions adéquates concernant l'atteinte à la protection de la vie privée, à la confidentialité ou à la sécurité, qui peuvent aller jusqu'au congédiement ou à la résiliation de l'entente, selon le cas.
- Une évaluation des risques et des menaces de même qu'une EIPVP ont eu lieu relativement au DEMI.
- Tous les employés et membres du personnel ainsi que les bénévoles et les entrepreneurs utilisant le DEMI doivent suivre une formation continue sur la protection de la vie privée, la confidentialité et la sécurité.
- Un protocole concernant les atteintes à la protection de la vie privée ou à la sécurité ayant trait au DEMI et à ses données a été élaboré et mis en œuvre.
- Un processus de gestion intégré du consentement permet de gérer et de faire respecter celui des clientes et des patients au sein des organismes participants.
- Un processus intégré de gestion des incidents permet de détecter ceux-ci, de les gérer et d'enquêter à leur sujet, au sein des organismes participants.
- Un processus intégré de soutien aux clients en matière de vie privée permet de gérer les demandes d'accès de ceux-ci et des patients et/ou de corriger leurs renseignements personnels sur la santé dans le DEMI, ainsi que de vérifier la conformité des fournisseurs de services de santé participants à la protection de la vie privée.
- Des plans de reprise des opérations acceptables comprenant notamment un plan antisinistre et de sauvegarde informatique sont en place.

- Conformément au présent accord, des ententes signées avec les tiers, qui sont fournisseurs d'un réseau d'information sur la santé aux dépositaires de renseignements sur la santé, sont en vigueur et exigent que ces tiers mettent en place les mesures de précaution adéquates relatives à la protection de la vie privée et à la sécurité pour offrir de tels services.

#### **Mesures de précaution techniques**

- Des mécanismes rigoureux de contrôle d'accès, y compris des mesures d'autorisation et d'authentification (p. ex. des ordinateurs protégés par mot de passe et un code d'accès unique), ont été implantés pour s'assurer que seul le personnel autorisé a accès au DEMI.
- Les données du DEMI sont codées pendant leur stockage et leur transmission.
- Les utilisatrices et utilisateurs sont incapables de modifier les données du DEMI.
- L'accès électronique à distance à l'environnement d'hébergement du DEMI est interdit, sauf s'il est nécessaire à la prestation de services de soutien par les gens en étant responsables, au nom du fournisseur du réseau d'information sur la santé, et à qui le fournisseur en question a accordé des droits d'accès adéquats.
- Des logiciels antivirus sont en place.
- Des pistes de vérification détaillées en temps réel ont été implantées pour enregistrer le nom d'utilisateur et pour horodater l'accès aux données et leur nature.

#### **Mesures de précaution matérielles**

- Les ordinateurs et les fichiers du DEMI se trouvent dans des endroits sécuritaires, à savoir dans des salles protégées par des serrures à combinaison ou des portes munies de cartes à puce, et les dossiers papier sont rangés dans des classeurs verrouillés.
- Les employés et le personnel possèdent une pièce d'identité avec photo ou une carte magnétique.
- Les entrepreneurs et les bénévoles doivent avoir une pièce d'identité avec photo ou une carte magnétique adéquate qui leur donne uniquement accès aux secteurs nécessaires à leurs fonctions.
- Les visiteuses et visiteurs au centre de données subissent un contrôle de sécurité et sont supervisés.
- Des systèmes d'alarme sont en place.
- Le nombre d'emplacements où le DEMI est entreposé est limité et précisé d'avance.
- La conception architecturale du fournisseur du réseau d'information sur la santé empêche le public d'accéder aux secteurs où le DEMI se trouve.
- On mène une surveillance courante des lieux.

- Des systèmes d'extinction protègent le DEMI contre les risques d'incendie.