POLITIQUE ET PROCÉDURES RELATIVES À LA PROTECTION DE LA VIE PRIVÉE

N° de référence : ADM-SSC-001

Approuvé par : Conseil d'administration
Date : 16 mars 2016
Dernière révision : 24 octobre 2016

TABLE DES MATIÈRES

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

ACRONYMES

CCIM : Community Care Information Management
CCPVP : Cadre commun de protection de la vie privée
CGSO : Centre de gestion du sevrage d'Ottawa
DATIS : Drug and Alcohol Treatment Information System
DÉI : Dossier d'évaluation intégré
DG : Direction générale
DRH : Direction des ressources humaines
ÉCBO : Évaluation commune des besoins en Ontario
FSS : Fournisseurs de services de santé
GISC : Gestion de l'information en soins communautaires
LPRPS : Loi sur la Protection des renseignements personnels sur la santé
MGC : Maison Gilles Chagnon
MRI : Montfort Renaissance Inc.
SAATO : Service d'accès et d'aiguillage en toxicomanie d'Ottawa
SMC : Santé en milieu communautaire
SSCSM: Services de soutien communautaire en santé mentale

DÉFINITIONS

Consentement

Selon la Loi de 2004 sur la protection des renseignements personnels sur la santé (L.O. 2004, chap. 3, annexe A)

Éléments du consentement
18. (1) Si la présente loi ou une autre loi exige le consentement d'un particulier à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé par un dépositaire de renseignements sur la santé, le consentement réunit les conditions suivantes :

a) il doit être le consentement du particulier;
b) il doit être éclairé;
c) il doit porter sur les renseignements;
d) il ne doit être obtenu ni par supercherie ni par coercition. 2004, chap. 3, annexe A, par. 18 (1).

Consentement implicite

(2) Sous réserve du paragraphe (3), le consentement à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé concernant un particulier peut être exprès ou implicite. 2004, chap. 3, annexe A, par. 18 (2).

Exception
(3) Le consentement à la divulgation de renseignements personnels sur la santé concernant un particulier doit être exprès et non implicite si, selon le cas :

a) un dépositaire de renseignements sur la santé fait la divulgation à une personne autre qu'un dépositaire de renseignements sur la santé;

b) un dépositaire de renseignements sur la santé fait la divulgation à un autre dépositaire de renseignements sur la santé, mais non aux fins de la fourniture de soins de santé ou d'une aide à cet égard. 2004, chap. 3, annexe A, par. 18 (3).

Idem

(4) Le paragraphe (3) ne s'applique pas, selon le cas :

a) à la divulgation faite suivant le consentement implicite visé au paragraphe 20 (4);
b) à la divulgation faite suivant l'alinéa 32 (1) b);
c) à un genre prescrit de divulgation qui ne comprend pas de renseignements sur l'état de santé d'un particulier. 2004, chap. 3, annexe A, par. 18 (4).

Consentement éclairé

(5) Le consentement à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé est éclairé s'il est raisonnable dans les circonstances de croire que le particulier qu'ils concernent :

a) d'une part, connaît les fins visées par la collecte, l'utilisation ou la divulgation, selon le cas;
b) d'autre part, sait qu'il peut donner ou refuser son consentement. 2004, chap. 3, annexe A, par. 18 (5).

Avis concernant les fins visées

(6) Sauf si cela n'est pas raisonnable dans les circonstances, il est raisonnable de croire qu'un particulier connaît les fins visées par la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé le concernant par un dépositaire de renseignements sur la santé si celui-ci affiche ou rend facilement accessible un avis énonçant ces fins à un endroit où le particulier est susceptible d'en prendre connaissance ou s'il lui remet un tel avis. 2004, chap. 3, annexe A, par. 18 (6).

Disposition transitoire

(7) Le consentement que donne un particulier, avant le jour de l'entrée en vigueur du paragraphe (1), à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé est valide s'il satisfait aux exigences de la présente loi en la matière. 2004, chap. 3, annexe A, par. 18 (7).

Retrait du consentement

19. (1) Le particulier qui consent à ce qu'un dépositaire de renseignements sur la santé recueille, utilise ou divulgue des renseignements personnels sur la santé le concernant peut retirer son consentement, que celui-ci soit exprès ou implicite, en remettant un avis à ce dernier. Toutefois, le retrait du consentement n'a pas d'effet rétroactif. 2004, chap. 3, annexe A, par. 19 (1).

EMHWare

Système de gestion des données relatives aux clients, où les contacts directs, notes évolutives, statistiques et données sont stockés, manipulés, échangés et affichés sous forme de rapports. L'accès au logiciel se fait de façon sécurisée et tous les accès sont enregistrés dans un journal d'audits.

LISTE DES ANNEXES

ANNEXE 1- Formulaire d'entente de non divulgation

ANNEXE 2- Dépliant : La protection des renseignements personnels et votre évaluation

ANNEXE 3- Communiqué en matière de consentement et de la protection des renseignements personnels sur la santé

ANNEXE 4- Exemple de documentation adéquate d'un consentement éclairé

ANNEXE 5- Formulaire d'autorisation du client pour recueillir, utiliser et divulguer l'information reliée au service

ANNEXE 6- Formulaire de consentement aux services de MRI

ANNEXE 7a)- Formulaire de directive de consentement pour le partage des données de l'évaluation

ANNEXE 7b)- Brochure du centre d'appel du consentement

ANNEXE 8- Registre d'emprunts de dossiers client

ANNEXE 9a)- Formulaire de demande de consultation du dossier

ANNEXE 9b)- Formulaire de réponse à une demande de consultation de dossier

ANNEXE 9c)- Formulaire de confirmation d'accès au dossier

ANNEXE 9d)- Formulaire de demande de photocopie de renseignements contenus dans un dossier

ANNEXE 10- Registre des dossiers des clients archivés

ANNEXE 11- Formulaire de demande d'accès sécurisé

ANNEXE 12- Formulaire de demande de modification des informations d'un compte utilisateur

ANNEXE 13- Formulaire de communication d'un incident en matière de vie privée

1. PRÉAMBULE

Montfort Renaissance (MRI) souscrit à la *Loi de 2004 sur la Protection des renseignements personnels sur la santé* (LPRPS) en matière de collecte, d'utilisation et de divulgation de renseignements personnels sur la santé concernant un particulier. MRI souscrit à la LPRPS afin de conférer au particulier le droit d'accès aux renseignements personnels sur la santé qui le concernent, sous réserve d'exceptions restreintes particulières énoncées dans la loi. MRI respecte les exigences légales en ce qui se rapporte au soutien au droit du particulier d'exiger la rectification ou la modification de renseignements personnels sur la santé qui le concernent, sous réserve d'exceptions particulières énoncées dans la loi. Notre organisation prévoit l'examen indépendant et le règlement des plaintes présentées à l'égard de renseignements personnels sur la santé.

MRI se conforme au Cadre commun de protection de la vie privée (CCPVP) qui a été créé par la Gestion de l'information en soins communautaires (GISC) dans le but de constituer une base de référence pour les pratiques en matière de protection de la vie privée des fournisseurs de services de santé (FSS) en soins communautaires de l'Ontario, et ce, afin d'aborder les préoccupations en matière de protection de la vie privée des FSS et de leurs clients.

Les activités de protection de la vie privée qui sont incluses dans cette stratégie comprennent : les politiques et procédures en matière de protection de la vie privée, la gouvernance de la protection de la vie privée, la gestion du consentement, la gestion des incidents, le soutien des droits du client en matière de protection de la vie privée, la révision des registres de consentement, la sensibilisation et la formation du personnel, la communication en matière de protection de la vie privée et la révision des activités de protection de la vie privée.

2. PRINCIPES

MRI élabore des politiques et des procédures qui reflètent la réalité de ses divers programmes. Ces pratiques sont fondées sur les principes suivants :

- Approche collaborative
- Communication ouverte et honnête
- Transparence
- Efficacité et souplesse
- Information pertinente
- Sécurité de l'information
- Soutien des droits des clients

3. POLITIQUE SUR LA PROTECTION DE LA VIE PRIVÉE

La présente politique en matière de protection de la vie privée a pour but d'exposer clairement les bonnes pratiques en matière de protection de la vie privée. La politique protège le droit d'un client au respect de sa vie privée en ce qui concerne l'information détenue par le personnel de MRI relativement à ses antécédents sociaux et médicaux, à sa condition physique et mentale passée et présente, à son plan de traitement et de réadaptation, sa médication, sa situation financière, son niveau de fonctionnement et l'endroit où il habite. La politique sur la protection de la vie privée de MRI contribue à orienter le développement des procédures qui sont adoptées par le personnel de l'organisation à tous les niveaux.

MRI promouvoit des pratiques qui protègent la confidentialité et la vie privée du particulier tout en facilitant la fourniture efficace des soins de santé. L'organisation pratique le consentement éclairé et adopte des approches souples qui tiennent compte du consentement implicite, du consentement exprès ou d'un mélange des deux, le cas échéant. MRI encourage une communication efficace et informée sur le consentement et utilise des moyens électroniques et non électroniques pour gérer le consentement. L'organisation s'assure d'une gestion efficace du processus complet de la directive de consentement qui tient compte de la cueillette de l'information, de sa mise à jour, de son archivage et de son stockage. Enfin, MRI assure à son personnel l'accès à de la formation en matière de pratiques exemplaires sur la vie privée.

Aux fins de cette politique, les actions suivantes constituent une violation de la confidentialité de l'information personnelle sur la santé :

- Le non-respect de la vie privée ou de la dignité d'un client découlant d'une divulgation inutile de renseignements confidentiels;
- La divulgation de renseignements identificatoires sur le client dans un endroit public;
- Toute négligence dans la manipulation de documents écrits relatifs au client.

Une violation de la confidentialité peut entraîner la prise de mesures disciplinaires pouvant aller jusqu'au congédiement.

3.1 EXCEPTION À LA POLITIQUE

Les renseignements confidentiels peuvent être communiqués dans le cadre des situations suivantes :

- Réunions d'équipe et de supervision;
- Processus d'affectation ou de réaffectation d'un client en suivi communautaire;
- Ordonnance du tribunal;
- Mauvais traitement d'enfants.

Le client est informé que le **besoin d'assurer la sécurité** peut avoir préséance sur l'obligation de confidentialité dans les cas où le non-dévoilement de renseignements représente un abus/danger pour le client, le personnel ou le public.

3.2 PROCÉDURE DE NOMINATION DU RESPONSABLE DE LA PROTECTION DE LA VIE PRIVÉE

La présente procédure vise à définir la pratique de MRI quant au processus décisionnel mis en place afin de nommer un responsable de la protection de la vie privée. Le responsable de la protection de la vie privée fait partie de la haute direction ou relève de celle-ci. Le responsable de la protection de la vie privée est autorisé à aborder les problèmes en matière de protection de la vie privée au sein de MRI et en a la responsabilité.

1. La direction générale (DG) de MRI nomme officiellement le responsable de la protection de la vie privée. Le nombre de responsables de la protection de la vie privée est déterminé selon les besoins de l'organisation par programme/service.

2. La DG demande au personnel de transmettre à la Direction des ressources humaines toute requête ou préoccupation relative à la protection de la vie privée. Cette direction se chargera d'acheminer l'information à la personne désignée comme responsable de la protection de la vie privée.

3. La DG indique, sur tout le matériel d'information à l'intention du public, le nom du responsable de la protection de la vie privée et informe le personnel de tout changement.

4. PROCÉDURES DE GESTION DU CONSENTEMENT

4.1 PROCÉDURE DE NON-DIVULGATION

Le personnel de MRI agit dans l'intérêt du client. Il fait preuve de discernement dans le type de renseignements qu'il demande au sujet du client. Il ne recueille que les renseignements qu'il juge essentiels pour assurer l'efficacité des services et dans la mesure du possible. Il s'adresse au client plutôt qu'à une tierce partie pour obtenir des renseignements ou des documents.

Dans le but de respecter la confidentialité des renseignements personnels sur la santé, le personnel de MRI complète, lors de son entrée en fonction, une entente de non-divulgation (ANNEXE 1).

Les ressources humaines sont responsables de faire signer cette entente avec le personnel et cette entente est déposée au dossier de l'employé au cours de sa première semaine de travail.

4.2 PROCÉDURE D'OBTENTION D'UN CONSENTEMENT ÉCLAIRÉ

Le consentement est la permission donnée par le client de procéder à un plan d'action (p. ex. plan de services, plan de soins, évaluations cliniques, etc.). Le consentement éclairé exige que la personne qui prend la décision reçoive toute l'information qu'une personne raisonnable aurait besoin de connaître dans les mêmes circonstances pour prendre une décision. Cela consiste aussi à expliquer d'autres options à la personne concernée et à répondre à ses demandes de renseignements additionnels.

Le consentement favorise la transparence dans nos pratiques, facilite l'ouverture et l'honnêteté dans la communication et incite le client à avoir des attentes réalistes.

1. Le personnel de MRI s'assure que le client comprend bien la nature du consentement et a la capacité de prendre une décision éclairée (voir la notion de consentement éclairé dans la liste des définitions et acronymes en page 3; l'annexe 4 propose une marche à suivre pour documenter le processus d'obtention du consentement). Si le client n'est pas en mesure de fournir un consentement éclairé, l'intervention doit être effectuée ultérieurement.

2. À la première rencontre, le personnel aide le client à comprendre et à saisir la nature et l'étendue des services qui lui seront fournis. Ceci implique que les conseillers doivent expliquer au client les informations relatives au consentement requis, en utilisant un niveau de langage qui tient compte de facteurs pouvant altérer la capacité de comprendre la portée du consentement : p. ex. une altération du fonctionnement cognitif liée aux problèmes de santé mentale, ou encore une difficulté de concentration causée par un traitement médicamenteux.

3. Avant de procéder à toute collecte d'information, le personnel informe le client concernant la collecte, l'utilisation et la divulgation de ses renseignements personnels. Il reçoit l'information concernant ses droits en matière de protection de la vie privée. Pour ce faire, le personnel remet au client le dépliant intitulé « La protection de la vie privée et votre évaluation » (ANNEXE 2). On explique au client la nature exacte des services fournis tant au début des services que sur une base continue. Le personnel informe le client quant aux renseignements précis qui seront recueillis, à quoi ils serviront et à qui, ainsi que comment ils seront communiqués.

4. Le personnel informe le client des conséquences positives et négatives du consentement.

5. Le personnel explique au client la portée de son consentement pour qu'il puisse prendre une décision éclairée par rapport à ce consentement. Le personnel explique précisément sur quoi porte le consentement, quels sont les renseignements qui seront recueillis, divulgués et partagés. (p. ex. ÉCBO, SMC, évaluations dans le cadre des SAATO, ou tout le dossier d'information de santé du client). Le personnel s'assure de bien informer le client sur la portée de son consentement : tout partager, ne rien partager ou partager en partie.

6. À l'admission au service/programme, le personnel remet au client le « Communiqué en matière de consentement et de la protection des renseignements personnels sur la santé » (ANNEXE 3). Le client signe le communiqué pour signifier sa compréhension en matière de consentement. Ce communiqué est placé au dossier du client et le client en reçoit une copie.

7. Le client prend une décision éclairée en accordant son consentement ou en refusant le consentement. Il émet de ce fait, une directive de consentement.

8. Les membres du personnel mettent à jour les données sur le système local de gestion des données (EMHWare), et ce, dans les plus brefs délais, avec la directive de consentement reçue conformément au processus de consentement existant.

Pour ce faire, le personnel documente les informations suivantes:

- La raison d'être du service/programme;
- La portée de la demande de service/programme;
- Les destinataires des informations recueillies, des documents acquis et des rapports écrits et verbaux;
- La garantie de confidentialité et l'explication des exceptions à la règle de confidentialité (p. ex. dossiers exigés par la cour, signalement obligatoire des mauvais traitements à l'égard d'enfants; risque de blessure grave pour soi ou autrui);
- La possibilité pour le client de s'adresser au superviseur de l'intervenant pour toute question ou préoccupation;
- La preuve que le client ou son représentant légal comprend et accepte d'entreprendre le traitement / les services / la démarche (après avoir eu l'occasion de poser des questions);
- La possibilité de retirer le consentement à n'importe quel moment.

4.2.1 Exigences relatives à l'obtention d'un consentement continu

- L'obtention du consentement doit être un processus continu et interactif;

- Le personnel de MRI demande au client à son admission au programme s'il consent à ce que des étudiants, des bénévoles ou d'autres membres du personnel participent aux visites de traitement ou y assistent en tant qu'observateurs;

- Le client reçoit des explications quant au rôle de l'étudiant ou du bénévole et sur sa présence pour observer, donner un traitement, ou les deux;

- Le personnel rappelle au client qu'il peut retirer son consentement à la présence de l'étudiant ou du bénévole à n'importe quel moment.

4.3 PROCÉDURE D'OBTENTION D'UN CONSENTEMENT IMPLICITE

Selon le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation, « le consentement implicite survient lorsque les actes ou l'inaction de la personne permettent raisonnablement de déduire qu'il y a consentement » (voir la notion de consentement implicite dans la liste des acronymes et définitions en page 3).

En fonction du contexte d'intervention, le personnel peut présumer du consentement implicite du client. C'est ainsi que deux intervenants dépositaires de renseignements sur la santé d'une personne sont soumis aux mêmes exigences de confidentialité et peuvent, dans le cas où ils s'occupent de la même personne, échanger sans préjudice une information jugée pertinente en regard de leurs responsabilités cliniques à la condition qu'ils œuvrent dans le même centre fonctionnel. Par exemple,

si l'intervenant pivot d'un client recevant des services à la fois au soutien judiciaire et au soutien au logement détenait une information judiciaire limitant les options résidentielles auxquelles le client peut accéder, il pourrait sans préjudice communiquer cette information au conseiller du soutien au logement sous la rubrique du consentement implicite. Si d'autre part, les exigences de confidentialité sont différentes, les règles les plus contraignantes doivent s'appliquer. L'échange de renseignements privés entre les intervenants de différents centres fonctionnels en santé mentale et en toxicomanie doit toujours faire l'objet d'un consentement explicite.

Cela comprend les situations où l'utilisation ou la communication prévue est évidente, compte tenu du contexte et où l'organisation peut présumer qu'il y a peu ou pas de risque pour le client de fournir ses renseignements personnels, en autant que le client est conscient de l'utilisation ou de la communication prévue et y consent. Ainsi, si les circonstances indiquaient que la personne comprend, connaît ou accepte qu'une certaine information soit divulguée, le consentement pourrait être implicite.

Afin de déterminer s'il convient de considérer un consentement comme implicite, il faut tenir compte des éléments suivants :

- La personne concernée s'attend raisonnablement à ce que les renseignements personnels la concernant soient utilisés ou communiqués de la façon proposée. Cet élément requiert que l'on tienne compte de nombreux facteurs, à savoir quelle information a été fournie à la personne, si l'objet de la collecte était bien indiqué et si les pratiques courantes sont généralement connues.

- Les renseignements sont de nature sensible. Cet élément pourrait très bien influencer les attentes raisonnables d'une personne. Le personnel de MRI devrait donc chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Tous les renseignements sur la santé d'une personne sont considérés comme étant des renseignements sensibles.

Si le consentement implicite est invoqué, il est alors documenté par une note évolutive au dossier électronique du client en reprenant les mots exacts prononcés par le client pour exprimer son consentement. Un exemple de documentation adéquate d'un consentement éclairé est disponible à l'ANNEXE 4.

4.4 PROCÉDURE DE CONSENTEMENT AU RECUEIL, À L'UTILISATION ET AU PARTAGE DE L'INFORMATION PERSONNELLE SUR LA SANTÉ

1. Les formulaires de demande de service remplis par le personnel de MRI au nom d'un client contiennent des renseignements confidentiels. Ces formulaires doivent être remplis en présence du client et signés par ce dernier. Autrement, ces formulaires doivent être accompagnés d'un formulaire « Autorisation du client pour recueillir, utiliser et divulguer l'information reliée au service » (ANNEXE 5) dûment signé.

2. Le formulaire « Autorisation du client pour recueillir, utiliser et divulguer l'information reliée au service » (ANNEXE 5) doit être signé pour autoriser les Services de soutien communautaire en santé mentale (SSCSM) à communiquer des renseignements avec les autres centres fonctionnels au sujet d'un client commun (par exemple : les Services d'accès et d'aiguillage en toxicomanie d'Ottawa (SAATO), les différents programmes chapeautés par le Centre de gestion du sevrage d'Ottawa (CGSO), dont la Maison Gilles Chagnon (MGC), les Ateliers de l'Élan). La durée de la validité du formulaire est spécifiée et paraphée par le client, mais ne doit pas excéder une période d'un an. Passé ce délai, il faut faire signer un nouveau formulaire au client. En effet, la notion de « cercle de soins » ne représente pas un consentement implicite dans les cas où la collaboration entre différents centres fonctionnels de MRI est requise pour assurer la couverture des besoins complexes de certains clients, notamment pour les SSCSM et les services en toxicomanie. L'organisation des profils d'accès aux données client du système local de gestion des données (EMHWare) tient aussi compte de cette limite, et ne permet pas aux intervenants d'un centre fonctionnel d'accéder aux données des clients des autres centres fonctionnels de MRI.

3. Le formulaire de consentement aux services (ANNEXE 6) doit être signé lorsque le client commence à recevoir des services de l'organisation. Les clients doivent pouvoir consentir de façon éclairée aux conditions reliées aux particularités de certains programmes, et la signature du consentement aux services doit comporter une explication détaillée, par l'employé conduisant le processus d'admission, des conditions propres au programme dans lequel le client est admis.

4. Le personnel obtient un nouveau consentement et l'inscrit au dossier chaque fois qu'il y a un changement ou une modification dans les programmes/services (p. ex. : admission à un nouveau centre fonctionnel, le recours aux services d'un consultant ou une entente interagence).

5. Le personnel doit obtenir le consentement exprès conformément au processus de consentement existant afin de partager les évaluations particulières requises par certains programmes/services, tels que l'Évaluation commune des besoins en Ontario (ÉCBO), le formulaire d'évaluation de la Santé en milieu communautaire (SMC), ou les évaluations dans le cadre des SAATO. Ce consentement peut être obtenu à partir du formulaire fourni à l'ANNEXE 7a. Lorsque le consentement a été obtenu, le formulaire signé doit être numérisé et ajouté aux « Fichiers joints » du système local de gestion des données (EMHWare), étant donné que les échanges d'information entre les centres fonctionnels de MRI ainsi qu'avec les agences partenaires dans le cadre de l'accès centralisé des SAATO sont pris en compte par le système.

   Les informations recueillies à l'aide des outils ÉCBO, SMC, et du processus d'évaluation dans le cadre des SAATO sont téléchargées dans des bases de données provinciales pour des fins statistiques et pour faciliter l'accès aux services à l'extérieur de la région (DÉI, DATIS). Les clients doivent également consentir à ce que leurs données d'évaluation soient téléchargées. La brochure à l'ANNEXE 7b) explique aux clients comment ils peuvent enregistrer directement leurs directives concernant leur niveau de consentement par rapport au DÉI (Dossier d'évaluation intégré).

6. Toute information au sujet d'une personne identifiée, obtenue verbalement ou par écrit, est confidentielle et ne peut être divulguée sans un formulaire signé de divulgation de renseignements. Seule l'information consignée par le personnel peut être communiquée.

7. Les renseignements obtenus, par écrit, d'une autre organisation **ne peuvent pas** être divulgués. Les demandes de renseignements doivent être adressées directement à l'organisation d'où proviennent les renseignements.

4.4.1 Discussion de cas clinique

- Le personnel qui convoque une discussion de cas clinique doit autant que possible inclure le client dans la planification de la rencontre.

4.4.2 Envoi par télécopieur

- Des mesures de prudence doivent être prises pour l'envoi par télécopieur de documents contenant des renseignements confidentiels;

- Les politiques des organisations partenaires ayant des critères plus restrictifs relativement à la protection de la vie privée auront préséance sur la procédure de consentement de MRI lors d'échange d'information par télécopieur (p. ex. hôpitaux ou milieu carcéral). Le personnel doit s'informer de la politique qui prévaut lors de ces échanges d'informations.

- Lorsque l'accès à des services particuliers (p. ex. l'Aide supplémentaire) se fait par télécopieur, le personnel peut transmettre de l'information par télécopieur à la demande du client. Dans la mesure du possible, on offre de l'aide au client pour qu'il envoie lui-même sa demande par télécopieur.

4.4.3 Ordonnance du tribunal et assignation à comparaître

- Le responsable de la protection de la vie privée ou l'avocat de l'organisation est consulté si des renseignements sur un client doivent être divulgués en vertu d'une ordonnance du tribunal ou d'une assignation à comparaître.

- Le client doit être informé avant la divulgation des renseignements;

- Une note évolutive est rédigée au dossier du client dans le système local de gestion des données (EMHWare) concernant ces communications.

4.4.4 Demande de renseignements à une organisation partenaire

- On peut recueillir de l'information sur un client sans détenir un formulaire « Autorisation du client pour recueillir, utiliser et divulguer l'information reliée au service » (ANNEXE 5). C'est la politique de confidentialité de l'organisation partenaire qui détermine si l'on peut ou non

recevoir l'information. Par exemple, les hôpitaux ne dévoilent aucune information sans ce formulaire. Pour faciliter l'accès aux dossiers de l'hôpital, il faut demander au client de signer ce formulaire qui sera transmis à l'hôpital;

- Le personnel peut solliciter de l'information sur les clients de n'importe quelle source professionnelle. Il doit par contre informer verbalement les clients des démarches qu'il compte effectuer.

4.4.5 Procédure de mise à jour de la directive de consentement (implicite ou exprès)

1. Le client demande au personnel de MRI de mettre à jour sa directive de consentement (retrait/rétablissement).

2. Le personnel explique au client les conséquences de retrait/rétablissement du consentement.

3. Le personnel obtient un consentement ou une directive de consentement verbal ou écrit dans les meilleurs délais en utilisant le formulaire de consentement approprié.

4. Le personnel met la directive de consentement à jour dans le système de gestion des données (EMHWare).

5. Lorsque le client souhaite changer sa directive de consentement pour son évaluation ou son dossier d'évaluation intégré (DÉI), le personnel lui remet l'information qui paraît sur la brochure du Centre d'appel du consentement (ANNEXE 7b). Le personnel de MRI peut aider le client à faire l'appel téléphonique afin de faire modifier sa directive de consentement pour son DÉI.

6. Le membre du personnel avise la DRH, qui en l'occurrence est la personne responsable de la protection de la vie privée ou son délégué dans les meilleurs délais.

7. Le responsable de la protection de la vie privée ou son délégué enregistre la directive de consentement dans le registre de directives de consentements.

4.4.6 Procédure d'archivage de l'information sur les consentements

Le consentement des clients de MRI est consigné de façon appropriée aux fins de suivi.

1. Le responsable de la protection de la vie privée prend des mesures appropriées pour s'assurer que le consentement verbal ou écrit implicite ou exprès est inscrit dans le système de gestion des données (EMHWare) du client pour les évaluations.

2. Le responsable de la protection de la vie privée pour l'organisation ou son délégué est responsable de vérifier annuellement auprès des gestionnaires des différents programmes/services le bon déroulement de la gestion des consentements.

3. La direction de programmes est responsable de s'assurer de la mise sur pied et du bon fonctionnement la révision du système électronique mis en place pour la gestion efficace des consentements.

4.4.7 Procédure de mise à jour des politiques et procédures de gestion des consentements

Les politiques et les procédures de MRI en matière de gestion des consentements sont actualisées sur une base annuelle.

1. Le responsable de la protection de la vie privée de MRI commence le processus de révision des politiques et des procédures en avril.

2. Le responsable de la protection de la vie privée et les directions s'assurent de consulter le personnel de première ligne dans le processus de vérification et de mise à jour des politiques et des procédures.

3. Le responsable de la protection de la vie privée présente à la haute direction les modifications apportées annuellement, au plus tard en juillet.

4. La direction générale est responsable de faire approuver les mises à jour par le conseil d'administration en septembre.

5. Le responsable de la protection de la vie privée communique au personnel de première ligne les mises à jour qui ont été apportées.

6. Le superviseur immédiat du personnel d'intervention de première ligne a la responsabilité de s'assurer que son personnel applique le processus de gestion du consentement conformément aux présentes politiques et procédures.

5. PROCÉDURES DE SOUTIEN AU RESPECT DE LA VIE PRIVÉE DE LA CLIENTÈLE

5.1 PROCÉDURE DE CONCEPTION ET DE CONSERVATION DU DOSSIER DU CLIENT

5.1.1 Dossiers papier

1. Le dossier est créé par le personnel au cours des 3 premiers jours suivant l'admission au service.

2. Le dossier du client est codé par le personnel intervenant qui a la responsabilité de créer le dossier client. La codification du dossier s'effectue selon la méthode suivante : 3 premières lettres du nom de famille suivi des 2 premières lettres du prénom suivi des 2 derniers chiffres de l'année d'admission au programme (p. ex. TARJE13).

3. Les dossiers papier des clients doivent être gardés sous clé en tout temps. Le classeur qui contient les dossiers client doit être situé dans un endroit où le public n'a pas accès. L'accès aux dossiers client est limité au personnel et aux gestionnaires.

4. L'emprunt du dossier papier d'un client doit être inscrit au Registre d'emprunts de dossiers client (ANNEXE 8).

5. Pour signaler le vol, la perte et la violation de renseignements sur un client, il faut se reporter à la **procédure de gestion des incidents liées à la sécurité des clients (ADM-SSC-004)**.

6. Les dossiers fermés sont gardés sous clé pendant sept ans, après quoi les documents sont détruits au moyen d'une déchiqueteuse. Le processus à suivre pour procéder à l'archivage du dossier est indiqué dans la section **5.2.4 Procédure d'archivage du dossier client**.

5.1.2 Dossiers électroniques

Dans la mesure du possible, il est préférable de consigner les informations personnelles sur la santé dans le dossier électronique du client.

- Suivant la réception du consentement à recevoir les services et le consentement à la collecte, l'utilisation et la divulgation du client, le personnel crée le dossier client dans le système de gestion de données (EMHWare).

- La procédure de tenue du dossier client est déterminée par chaque programme selon la procédure clinique à cet effet; elle est précisée dans les manuels de politiques et procédures propres à chacun des programmes.

- L'accès aux informations contenues dans le dossier client électronique est limité au personnel du programme où le client est admis et à la direction. Les profils de permissions du système de gestion des données (EMHWare) sont configurés de façon à ce que seul le personnel rattaché aux centres fonctionnels dans lesquels le client est inscrit ait accès aux données du client. Le personnel de gestion ayant un profil administrateur, dont les membres de la direction, font exception et ont accès à tous les dossiers client électroniques.

- Le dossier client électronique contient les données qualitatives suivantes : les données démographiques, les indicateurs de l'état du rétablissement (p. ex. hospitalisation, incarcération, emploi, logement, etc.), les notes évolutives, les diagnostics, la médication, les informations médicales, le carnet d'adresses des membres du réseau de soutien et des outils d'évaluation et de planification cliniques (p. ex. ÉCBO, SMC, Plan de soutien résidentiel).

- Le dossier électronique du client contient les données quantitatives suivantes : le nombre et la durée des contacts directs (p. ex. visites personnelles, contacts téléphoniques, interactions entre les fournisseurs de service de santé).

- Le personnel qui fait des interventions dans la communauté peut utiliser des instruments servant à la consignation des données à l'extérieur du bureau (p. ex. ordinateur portable, IPad), à condition de prendre des précautions raisonnables contre le vol, la perte et la violation de la confidentialité.

- Aucun instrument servant à la consignation des données ne doit être laissé dans une automobile en l'absence du conducteur. Ils ne doivent pas être laissés sans surveillance en mode «Marche» en présence d'une personne non autorisée à accéder aux renseignements du dossier électronique.

- Pour signaler le vol, la perte et la violation de renseignements sur un client, il faut se reporter à la **procédure de gestion des incidents liées à la sécurité des clients (ADM-SSC-004)**.

- La procédure de fermeture du dossier client électronique est déterminée par chaque programme selon la procédure clinique à cet effet, précisée dans les manuels de politiques et procédures propres à chacun des programmes.

5.2 PROCÉDURE DE DEMANDE D'ACCÈS AU DOSSIER CLIENT

Lorsqu'ils acceptent de recevoir des services, les clients sont informés de toutes les politiques et procédures de l'organisation concernant la confidentialité de l'information privée.

Les clients ont le droit d'examiner leur dossier. Seule l'information recueillie par MRI peut être consultée par le client. Il faut s'adresser à la source pour avoir accès aux renseignements provenant d'une tierce partie.

Tout client a le droit d'être informé de l'existence d'un renseignement nominatif le concernant et a le droit d'accès à son dossier.

5.2.1 Traitement de la demande d'accès

1. Toute demande d'accès se fait par écrit par le requérant en remplissant le formulaire « Demande de consultation du dossier » (ANNEXE 9a).

2. La demande d'accès est transmise au directeur de programme ou au gestionnaire dans les meilleurs délais.

3. La demande d'accès doit être traitée dans les meilleurs délais et au plus tard dans les 15 jours ouvrables après la réception de la demande.

4. Le directeur ou le gestionnaire, après consultation avec l'intervenant principal et après avoir pris connaissance du dossier, avise le client par écrit de sa décision en remplissant le « Formulaire de réponse à une demande de consultation de dossier » (ANNEXE 9b).

5.2.2 Assistance pour l'accès au dossier

1. Lors de la rencontre d'accès au dossier, le personnel remet au client le formulaire « Confirmation d'accès au dossier » (ANNEXE 9c). Le client signe ce formulaire et il en garde une copie. Le personnel place au dossier du client une copie de ce formulaire.

2. Le client peut se faire accompagner d'une autre personne lors de la consultation de son dossier. Notez que seule l'information recueillie par MRI peut être consultée par le client; toute information provenant d'une tierce partie aura été retirée aux fins de la consultation.

3. Le client peut demander l'aide du personnel pour l'aider à comprendre les renseignements contenus au dossier.

4. Durant la consultation du dossier, le personnel assure une surveillance adéquate afin qu'aucun document ne soit retiré ou modifié.

5.2.3 Demande de photocopie du dossier

L'accès au dossier est gratuit. Les frais de reproduction le sont aussi pourvu qu'ils n'excèdent pas 5 $ (environ 50 pages).

1. Dans le cas où le client souhaite procéder à la demande de photocopie d'une partie ou de la totalité de son dossier, il doit remplir le « Formulaire de demande de photocopier des renseignements contenus dans mon dossier » (ANNEXE 9d).

2. La demande d'accès, de photocopie et la décision prise doivent être inscrites au dossier électronique du client par le personnel dans les meilleurs délais.

5.2.4 Procédure d'archivage du dossier client

1. À la fermeture du dossier du client (selon la procédure clinique de chaque programme), le personnel identifie le dossier physique en y apposant une étiquette rouge sur la tranche. Cette étiquette comporte le code d'identification du dossier du client (p. ex. TARJE13) et la date de fermeture (p. ex. 20 juin 2013).

2. À la date de fermeture, le personnel remet à l'adjointe administrative responsable de l'archivage le dossier papier du client.

3. Le personnel est responsable d'inscrire la date de fermeture du dossier et de la réalisation du processus d'archivage complété au dossier client électronique.

4. L'adjointe administrative est responsable d'archiver le dossier client à l'emplacement réservé à cette fin.

5. L'adjointe administrative ou son délégué est responsable de tenir à jour le Registre des dossiers client archivés (ANNEXE-10).

6. Les dossiers archivés sont gardés sous clé pendant sept ans, après quoi l'adjointe administrative détruit les dossiers au moyen d'une déchiqueteuse ou en ayant recours aux services d'une compagnie reconnue pour la destruction sécuritaire des documents confidentiels.

5.3 PROCÉDURE DE MODIFICATION DES INFORMATIONS CONTENUES DANS LES ÉVALUATIONS ÉCBO OU SMC

1. Le client communique avec MRI, s'il est le fournisseur de service de santé principal qui a complété l'ÉCBO ou la SMC, afin d'effectuer des modifications aux informations qui y sont contenues.

2. Le client communique par écrit ou verbalement sa demande de modification au personnel responsable de l'ÉCBO ou de la SMC.

3. Le personnel de MRI s'assure de l'obtention du consentement du client pour l'ÉCBO ou la SMC en suivant la procédure d'obtention du consentement.

4. Si des modifications ont lieu d'être apportées au consentement, le personnel aide le client à contacter le Centre d'appel du consentement.

5. Le personnel effectue une réévaluation à l'ÉCBO ou à la SMC en précisant le motif de la demande qui correspond ici à la demande du client.

6. À la fin de la réévaluation, le personnel signe l'ÉCBO ou la SMC. Lors de la signature, l'ECBO ou la SMC est automatiquement téléversée dans le DÉI, à moins que le client n'ait complètement retiré son consentement à cet égard; dans ce cas cette option automatique pourrait être interrompue à même le système de gestion de données (EMHWare).

6. PROCÉDURE DE PLAINTE D'UN CLIENT SUR LES PRATIQUES DE RESPECT DE LA VIE PRIVÉE

Cette procédure de plainte n'enlève aucun droit au client aux recours officiels offerts par les lois, les normes et les règlements officiels existants.

6.1 DÉPÔT D'UNE PLAINTE D'ATTEINTE À LA VIE PRIVÉE

1. Lorsqu'une personne considère avoir été lésée dans ses droits eu égard à la politique sur la vie privée, elle peut déposer une plainte écrite ou verbale au responsable de la protection de la vie privée de MRI.

2. La Direction des ressources humaines est la personne mandatée par la direction générale de MRI comme responsable de la protection de la vie privée pour l'organisation.

   La Direction des ressources humaines peut être contactée par téléphone au 613-789-5144 au poste 218 ou par courrier électronique à rh@mri.ca
   - La Direction des ressources humaines peut être contactée par la poste au 162, rue Murray, Ottawa (Ontario) K1N 5M8.

6.2 TRAITEMENT DE LA PLAINTE CONCERNANT LA VIE PRIVÉE

1. À la suite d'une plainte, la responsable de la protection de la vie privée fera une analyse sommaire de la situation dans les 15 jours ouvrables suivant la plainte.

2. Des correctifs d'amélioration et d'ajustement seront proposés aux parties concernées.

3. Un résumé ainsi que les recommandations et correctifs proposés seront remis à la direction générale de l'organisation.

4. La direction générale fera rapport au conseil d'administration des correctifs apportés.

7. PROCÉDURES DE GESTION DES ACCÈS SÉCURISÉS

7.1 DEMANDE DE CRÉATION D'UN ACCÈS SÉCURISÉ

1. Lors de la création de comptes d'utilisateurs en vue de la mise en œuvre initiale du DÉI, le responsable de protection de la vie privée et les directeurs des programmes de MRI déterminent ensemble quels sont les membres du personnel qui auront besoin d'un accès sécurisé.
2. La demande de création des accès sécurisés est envoyée à la CCIM pour leur création. Le responsable de la protection de la vie privée reçoit ces accès par courriel dans un document sécurisé. Il est responsable de remettre ces accès sécurisés aux membres du personnel au moment où ceux-ci reçoivent la formation sur le DÉI.
3. Suite à la mise en œuvre initiale des accès sécurisés au DÉI, le directeur de chaque programme détermine les membres du personnel qui doivent avoir un accès sécurisé. La demande est acheminée par courriel au responsable de la protection de la vie privée en remplissant le « Formulaire de demande d'accès sécurisé » (ANNEXE11).
4. Le responsable de la protection de la vie privée de MRI attribue aux nouveaux utilisateurs leur accès sécurisé, ou transmet l'information aux gestionnaires des programmes visés, qui les remettront aux personnes concernées.
5. Le responsable de la protection de la vie privée de MRI ou les gestionnaires assurent la signature des nouveaux accès d'utilisation du DÉI.

6. L'accès au DÉI est actuellement limité aux directeurs et gestionnaires de programmes, étant donné qu'aucun besoin d'accès n'a été identifié jusqu'à présent pour les conseillers compte tenu des limitations du DÉI quant aux fonctionnalités pouvant comporter un intérêt clinique pour eux. Dans l'éventualité où des profils d'accès sécurisés seraient créés pour les conseillers, le responsable de la protection de la vie privée de MRI génèrera un « Registre des accès sécurisés », qui sera placé sur le serveur commun sous le répertoire « Agrément / DÉI / Gestion des accès DEI ».

7.2 Modification des informations ou suppression d'un compte d'utilisateur

1. Toute demande de modification des renseignements sur le compte d'utilisateur (p. ex. le numéro de téléphone, le nom, le lieu de travail, etc.) ou de suppression du compte doit être acheminée au responsable de la protection de la vie privée en remplissant le « Formulaire de demande de modification des informations d'un compte utilisateur » (ANNEXE 12).
2. Le responsable de la protection de la vie privée appose ses initiales sur la demande et l'achemine à l'adjointe administrative du programme/service.
3. L'adjointe administrative envoie la demande de modification numérisée au responsable du projet DÉI par courriel, à l'adresse IAR@ccim.on.ca. ou par **télécopieur au 1.416.314.1585**.
4. L'adjointe administrative du programme/service consigne les formulaires de demande de modification des informations d'un compte utilisateur sur le serveur commun sous le répertoire « Agrément / DÉI / Modification des comptes utilisateurs DEI ».

7.3 Procédure de révision des registres de vérification du DÉI

1. Le responsable de la protection de la vie privée ou le gestionnaire clinique s'assurera de vérifier mensuellement les habitudes d'accès et d'utilisation du personnel au DÉI. Une liste de contrôle est créée en collaboration avec chaque directeur de programme de MRI afin d'identifier les éléments à examiner ou à rechercher afin de veiller à ce que rien ne soit oublié lors de la révision du fichier du registre de vérification (la liste de contrôle sera créée dans l'éventualité où l'utilisation du DÉI comprend les conseillers).

2. Le responsable de la protection de la vie privée ou le gestionnaire vérifie mensuellement les activités du personnel de l'organisation par programme/service en procédant à la révision des journaux d'activités du DÉI suivants : le « Privacy Log », le « Clinical Log », le « Current Activity Log » et le « System Log ».

3. Il vérifie le moment, la fréquence, la durée des accès au DÉI. Il consulte les requêtes de visionnement par type d'évaluation placée au DÉI. Il effectue la vérification aléatoire des activités au DÉI par clients ou par utilisateurs.

4. Des registres et rapports peuvent sont exportés en format CSV (Excel) aux fins de triage, de filtrage, d'élaboration de rapports et de manipulations supplémentaires.

5. Une liste de contrôle mensuelle commentée est acheminée à chaque directeur de programme par le responsable de la protection de la vie privée ou le gestionnaire pour fins de vérification.

6. Ces rapports sont enregistrés de manière électronique sur le serveur commun sous le répertoire « Agrément / DÉI / Rapports d'incident Protection de la vie privée » et ensuite classés dans des dossiers qui sont triés de façon mensuelle. L'usage de ce répertoire est réservé à la direction.

8. PROCÉDURES DE GESTION DES INCIDENTS

8.1 PROCÉDURE DE DÉTECTION DES INCIDENTS

8.1.1 Communication de la procédure de détection des incidents

1. Dès l'entrée en fonction au sein de l'organisation, le responsable de la protection de la vie privée ou les gestionnaires des programmes/services assurent la formation du personnel en matière de gestion des incidents. La **procédure de formation du personnel** fait état des processus mis en œuvre pour tenir à jour le personnel quant aux pratiques en matière de respect de la vie privée.

2. Le client est informé par le personnel de MRI, dès son admission au service, de la façon dont il peut procéder pour déclarer une allégation relative à un incident portant sur la protection de ses renseignements personnels sur la santé. Cette procédure est communiquée dans le dépliant à l'intention du public qui s'intitule « La protection de la vie privée et votre évaluation ». Le personnel peut se référer à la **procédure de plainte en matière de protection de la vie privée**.

8.1.2 Détection des incidents

1. Les activités de surveillance mensuelle que mène le responsable de la protection de la vie privée visent à détecter des incidents qui pourraient potentiellement causer un risque à la protection des renseignements sur la santé.

2. Les situations suivantes correspondent à des exemples d'incidents par rapport à la présente politique sur la protection de la vie privée et elles doivent être rapportées au responsable de la protection de la vie privée de MRI :

    - la perte ou le vol du dossier d'un client (total ou partiel) contenant l'information personnelle sur la santé;
    - la perte ou le vol de tout document physique ou électronique contenant de l'information personnelle sur la santé;
    - l'accès inhabituel par un utilisateur au DÉI;

3. Le personnel de MRI est tenu de communiquer tout incident au responsable de protection de la vie privée par écrit, dans les meilleurs délais, en remplissant le « Formulaire de communication d'un incident en matière de vie privée » (ANNEXE 13). Le client ou tout autre tiers rapporte un incident en communiquant directement par écrit ou verbalement avec le responsable à la protection de la vie privée.

    - La Direction des ressources humaines est la personne mandatée par la direction générale de MRI comme la responsable de la protection de la vie privée pour l'organisation.

    - La Direction des ressources humaines peut être contactée par téléphone au 613-789-5144 au poste 218 ou par courrier électronique à rh@mri.ca ou au 162, rue Murray, Ottawa (Ontario) K1N 5M8.

8.2 PROCÉDURE DE TRAITEMENT ET DE COMMUNICATION DES INCIDENTS

1. Lorsqu'un incident est rapporté au responsable de la protection de la vie privée, il communique avec le gestionnaire ou directeur du programme pour discuter de l'incident dans les meilleurs délais.

2. Le responsable de la protection de la vie privée et le gestionnaire ont 10 jours ouvrables pour traiter l'incident, rencontrer le personnel concerné et apporter les correctifs nécessaires à la situation, le cas échéant.

3. Lorsqu'une autre organisation est concernée, le responsable de la protection de la vie privée communique par écrit avec le fournisseur responsable des informations sur la santé (FRIS).

4. À MRI, le responsable à la protection de la vie privée est la personne désignée comme étant celle à contacter par une autre organisation (partenaire, contributeur) concernée par un incident.

5. Si l'incident est causé par MRI, le responsable de la protection de la vie privée est responsable d'informer le client par écrit. Si l'incident est causé par l'organisation (partenaire, contributeur), ce dernier informe le client par écrit.

6. Tous les rapports d'incidents annuels sont consignés sur le serveur commun de l'organisation dans le répertoire « Rapports d'incident Protection de la vie privée » et ils sont triés par mois.

9. RÉFÉRENCES

Réseau local d'intégration des services de santé de Champlain (2013). A Privacy Issue Identification Briefing Note Regarding the Addictions Integrated Access Program and Best Practices Related to the PHIPA « Lock-Box » Provisions. Inédit.

Loi sur la protection des renseignements personnels (L.R. 1985, ch. P-21).

Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, c.5).

Loi sur la santé mentale (L.R.O. 1990, c. M.7, art.35).

Loi de 2004 sur la protection des renseignements personnels sur la santé (L.O. 2004, c.3, Annexe A).

Ministère de la Santé et des Soins de longue durée (2012). Consolidated Health Information Services – Dossier d'évaluation intégré. Entente de partage de données entre le MSSLD et Montfort Renaissance Inc. Inédit.

10. ENREGISTREMENT DES MISES À JOUR DE LA POLITIQUE

No.	Date de la mise à jour	Modifications	Enregistré par
1	2016-10-24	Ajout de la note de bas de page à la 1re page	Blanche Gagné-Lemieux
2	2016-10-24	Suppression de l'annexe 14 (formation des employés)	Blanche Gagné-Lemieux
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			