Centre intégré
universitaire de santé
et de services sociaux
du Nord-de-
l'Île-de-Montréal

Québec

Direction de la recherche

MON 23 CR-CIUSSS-NÎM	Sécurité et confidentialité des données

1. Objectifs

Les objectifs de ce MON sont de :

- Décrire le processus qui permet d'assurer la sécurité et la confidentialité des données cliniques recueillies ou à notre disposition dans le cadre d'une étude clinique;
- Décrire les procédures de protection des données contre tout risque de destruction accidentelle ou involontaire;
- Décrire les procédures de protection des données contre tout accès non autorisé.

2. Renseignements généraux

- Toute personne ayant un accès direct aux données cliniques doit s'assurer de respecter la Déclaration d'Helsinki, les BPC et les exigences réglementaires applicables pour le maintien de la confidentialité, de l'identité du participant et du respect de la propriété des informations par le promoteur ou le promoteur-investigateur;
- L'identification de toute personne ayant un accès aux données constitue l'aspect le plus important de la sécurité. Elle détermine le niveau global de protection et est reliée aux éléments clés de la sécurité des données.

3. Responsabilités

Le promoteur doit s'assurer que :

- Le protocole ou toute autre entente écrite précise que l'investigateur/établissement autorise l'accès direct aux données/documents sources aux fins de surveillance, de vérification, de l'examen du CÉR et d'inspection réglementaire concernant l'essai. (BPC 5.15.1);
- Tous les participants ont autorisé par écrit (en signant le formulaire d'information et de consentement [FIC]) l'accès direct à leur dossier médical original aux fins de la surveillance, de la vérification, de l'examen du CÉR et d'inspection réglementaire concernant l'essai. (BPC 5.15.2).

Le chercheur principal doit s'assurer :

- De respecter les procédures en vigueur au CIUSSS-NÎM et au CR-CIUSSS-NÎM en matière de confidentialité : PO-12-002 Politique institutionnelle sur la conduite responsable en recherche;
- De former son personnel sur les procédures à appliquer;
- Que tous les participants ont autorisé, par écrit (en signant le FIC), l'accès direct à leur dossier médical original aux fins de surveillance, de vérification et d'inspection. (BPC 4.8.10. n).

Un professionnel peut prendre connaissance d'un dossier médical à des fins d'étude, d'enseignement ou de recherche, avec l'autorisation du directeur des services professionnels ou, à défaut d'un tel directeur, avec l'autorisation du directeur général.

4. Sécurité des données

4.1. Sécurité physique

La sécurité physique concerne les locaux où sont conservées les filières contenant les documents essentiels, les données cliniques, les dossiers de recherche ainsi que le matériel informatique utilisé pour la gestion des données, tels que serveurs de télécommunications, serveurs de base de données, ordinateurs ou autre.

Ces locaux doivent :

- Être situés dans un endroit protégé de toute catastrophe (p. ex. : dégâts d'eau ou de feu, etc.);
- Être protégés par un système de contrôle sécurisé des accès, dont le mécanisme doit être mis en place et documenté (MSSS : cadre global de gestion des actifs informationnels – Volet Sécurité);
  - Le mécanisme de contrôle recommandé, basé sur l'utilisation de cartes magnétiques s'applique déjà dans plusieurs locaux du CIUSSS-NÎM, à la pharmacie, à l'unité de recherche clinique et à l'entrée du CR-CIUSSS-NÎM;
  - Dans les locaux où ce mécanisme n'est pas disponible, un système de hiérarchie de clés avec liste des détenteurs spécifiques doit être mis en place;
- Toutes les données (documents de recherche [CRF], documents sources, dossiers d'archives, etc.) doivent être conservées selon le principe de double verrouillage.

4.2. Contrôle d'accès aux données

Afin d'assurer ce contrôle, les mesures suivantes doivent être appliquées :

- L'autorisation d'accès est limitée aux personnes de l'équipe de recherche identifiées dans le formulaire de délégations de tâches et aux personnes mandatées par les organismes identifiés dans le protocole et dans le FIC;
- Les privilèges d'accès physique ou informatique aux données sont accordés et mis à jour selon les rôles et responsabilités définis par le promoteur-investigateur ou le chercheur principal;
- Un formulaire de délégation de tâches doit être généré. Il contient les signatures et initiales de toutes les personnes autorisées à consigner les données ou à apporter des corrections au dossier de recherche (CRF), ainsi que les dates de début et de fin du privilège accordé. Il doit être conservé dans la documentation essentielle à l'étude;
- Dans le cas où un membre de l'équipe de recherche quitte l'équipe de recherche (démission, maladie, retrait préventif ou autre), l'autorisation d'accès qui lui était attribuée doit être terminée. Le formulaire de délégations de tâches doit refléter cette date de fin;
- Toute personne travaillant avec des données nominatives ou dossiers d'archives doit fermer et verrouiller son local si elle doit s'absenter, ne serait-ce que quelques instants. Il est aussi recommandé de ranger le dossier;
- En aucun cas, un participant de recherche ne doit rester seul en présence de dossiers accessibles autres que son propre dossier;
- Les dossiers des archives devront être gardés sous clé lorsqu'ils sont non utilisés dans les locaux de recherche;
- Changement de surveillant du promoteur : Tout changement dans le surveillant doit être annoncé par le promoteur avant la visite de ce nouveau surveillant.

4.3. Sécurité des données électroniques

En plus de ce qui s'applique à toutes les données papier, certaines précautions supplémentaires doivent être prises lorsqu'il s'agit de données électroniques :

- Nommé par le promoteur/promoteur-investigateur, le responsable de la gestion du système, appelé administrateur du système, peut suspendre l'autorisation d'accès d'un utilisateur après un nombre déterminé d'erreurs. Les autres utilisateurs doivent être informés de cette suspension. Le formulaire de délégations de tâches doit refléter cette suspension;
- Le code d'identification doit être différent pour chaque utilisateur du système de gestion des données. Le mot de passe, propre à chaque utilisateur et confidentiel, donnant l'accès au système, doit être changé régulièrement selon la période définie par l'administrateur du système;
- L'administrateur du système doit s'assurer de la confidentialité de l'identification des utilisateurs du système. Il doit également documenter la traçabilité des accès;
- Un plan de sauvegarde et de récupération des données doit être établi, en cas de perte ou de sinistre;
- Les informations contenues sur les postes de travail doivent être protégées par des codes d'accès et mot de passe conformément à la Directive 1 – Profils et codes d'accès aux actifs informationnels, afférent à la politique AG-037;
- Un écran de veille doit obligatoirement être activé sur les ordinateurs conformément à politique AG-037.

5. Confidentialité des données

5.1. Lois

La confidentialité des dossiers pouvant servir à identifier les participants doit être protégée conformément aux règles relatives à la protection des renseignements personnels et à la confidentialité établies dans les exigences réglementaires applicables. Référence BPC 2.11 et le MSSS : cadre global de gestion des actifs informationnels – Volet Sécurité.

Selon la Loi du Québec sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, un organisme public ne peut communiquer un renseignement nominatif sans le consentement de la personne concernée. Toutefois il peut communiquer un tel renseignement sans le consentement de cette personne dans les cas et aux strictes conditions qui suivent :

- À une personne qui est autorisée par la Commission d'accès à l'information; conformément à l'article 125;
- Les renseignements nominatifs sont confidentiels;
    - Dans un document, sont nominatifs les renseignements qui concernent une personne physique et permettent de l'identifier;
    - Toute personne a le droit d'être informée de l'existence, dans un fichier de renseignements personnels, d'un renseignement nominatif la concernant. Cette notion doit-être indiquée au FIC.

5.2. Confidentialité des dossiers et données de recherche

- Le participant qui autorise l'accès aux données le concernant doit être raisonnablement assuré et que le promoteur/promoteur-investigateur, le chercheur principal, les représentants autorisés par le promoteur/promoteur-investigateur, le CÉR et les vérificateurs et inspecteurs des autorités réglementaires, ont pris toutes les précautions pour que les données vérifiées et recueillies demeurent confidentielles, BPC 5.15.1.;

- La confidentialité des données doit être maintenue et respectée pendant et après l'étude.

EPTC2 : Les établissements et les organismes où sont conservées des données de recherche ont la responsabilité d'établir des mesures de sécurité appropriées pour protéger ces données (EPTC2 article 5.4).

5.3. Politique institutionnelle et cadre réglementaire de la recherche

Respect de la confidentialité :

- Toute personne qui œuvre en recherche clinique doit respecter les règles et normes de l'établissement concernant la confidentialité des dossiers des patients et des renseignements qui s'y trouvent. Les énoncés de la Loi sur les services de santé et les services sociaux doivent être suivis par les chercheurs et leur personnel pour leur accès aux dossiers cliniques et pour la divulgation à des tiers de renseignements qui découlent de leur recherche.

Accès aux dossiers médicaux (D.U. 004) :

- Le dossier d'un usager est confidentiel et nul ne peut y avoir accès, si ce n'est avec l'autorisation de l'usager ou de la personne pouvant donner une autorisation en son nom, sur l'ordre d'un tribunal ou dans le cas où la présente loi prévoit que la communication de renseignements contenus dans le dossier peut être requise par un établissement.
- Toutefois, un professionnel peut prendre connaissance d'un tel dossier à des fins d'étude, d'enseignement ou de recherche, avec l'autorisation du directeur des services professionnels ou, à défaut d'un tel directeur, avec l'autorisation du directeur général, accordée conformément aux critères établis à l'article 125 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q, chapitre A-2.1).

Engagement du chercheur à respecter la confidentialité (D.U 004 annexe 5) :

- Être conscient que toutes les données contenues dans les dossiers qu'il consultera sont strictement confidentielles et s'engage à en respecter la confidentialité;
- Identifier les participants de façon codifiée. La clé du code sera gardée secrète par le directeur du projet et divulguée seulement lorsqu'absolument nécessaire (par exemple, si la loi l'exige).

6. Bris de confidentialité

Lorsqu'un bris de confidentialité se produit, peu importe la raison, la personne qui en prend connaissance doit immédiatement :

- Aviser la personne ou l'organisation qui a reçu l'information confidentielle par erreur;
  - De la détruire;
  - De confirmer que l'information reçue par erreur n'a pas été transférée ni communiquée à quiconque;
  - De confirmer la destruction de l'information par écrit;
  - De confirmer qu'une déclaration de bris de confidentialité a été effectuée auprès du commissaire à la vie privée de cette organisation;

- S'assurer de rapporter le bris de confidentialité au bureau d'appui à la recherche (B.A.R.) du CIUSSS-NÎM par courriel à l'adresse suivante : appui.recherche.cnmtl@ssss.gouv.qc.ca et de suivre l'ensemble des recommandations émises par la suite.

7. Références

Santé Canada, Règlement sur les aliments et drogues, partie C, titre 5, « Drogues destinées aux essais cliniques sur des sujets humains » (annexe 1024), 20 juin 2001.

Gouvernement du Canada, Règlement sur les instruments médicaux, DORS/98-282, 7 mai 1998; dernière modification effectuée le 13 février 2017, règlement à jour en date du 20 mars 2017.

Gouvernement du Canada, Règlement sur les produits de santé naturels, partie 4 : Essais cliniques sur des sujets humains, DORS/2003-196, 5 juin 2003; dernière modification effectuée le 1er juin 2008; règlement à jour en date du 20 mars 2017.

International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH), ICH Harmonised Guideline, Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice, E6(R2), 9 novembre 2016.

Instituts de recherche en santé du Canada Conseil de recherches en sciences naturelles et en génie du Canada, Conseil de recherches en sciences humaines du Canada, Énoncé de politique des Trois Conseils : Éthique de la recherche avec des êtres humains, décembre 2014.

Ministère de la Justice. Loi sur la protection des renseignements personnels et les documents électroniques (LPRDPE), dernière modification effectuée le 23 juin 2015, loi à jour en date du 31 décembre 2016.

États-Unis. Food and Drug Administration. Code of Federal Regulations, Title 21, Volume 1 :

- Part 11, « Electronic Records; Electronic Signatures » (21CFR11);
- Part 50, « Protection of Human Subjects » (21CFR50);
- Part 54, « Financial Disclosure by Clinical Investigators » (21CFR54);
- Part 56, « Institutional Review Boards » (21CFR56);
- Part 312, « Investigational New Drug Application » (21CFR312);
- Part 314, « Applications for FDA Approval to Market a New Drug » (21CFR314).

États-Unis. Department of Health and Human Services. Code of Federal Regulations, Title 45, Part 46, « Protection of Human Subjects » (45CFR46).

États-Unis. Department of Health and Human Services, Guidance for Industry: Computerized Systems Used in Clinical Investigations, may 2007.