

Titre	Sécurité et confidentialité des données
Codification	MON 22
Pages	4

Historique des versions validées

Date jj/mm/aaaa	Version	Pages	Description de la modification

Historique de la mise en place du MON

Version	Date jj/mm/aaaa	Version	Date jj/mm/aaaa	Version	Date jj/mm/aaaa

Approbation du MON

	Signature	Date jj/mm/aaaa

Table des matières

1. Politique
2. Objectifs
3. Procédures
 - 3.1 Généralités
 - 3.2 Sécurité des données
 - 3.3 Confidentialité des données
4. Références

1. Politique

Ce mode opératoire normalisé décrit les procédures à suivre pour assurer la sécurité et la confidentialité des données reliées à un essai clinique.

2. Objectifs

Décrire le processus qui permet d'assurer la qualité, disponibilité, intégrité, confidentialité, authenticité et irrévocabilité des données cliniques recueillies dans le cadre d'un essai clinique.

L'autre objectif est de décrire les procédures de protection des données contre tout risque de destruction accidentelle ou involontaire.

3. Procédures

3.1 Généralités

3.1.1 Le promoteur-chercheur ou le chercheur est responsable de l'autorisation d'accès aux données cliniques. Cette autorisation doit être documentée dans le protocole et sur le formulaire de délégations;

3.1.2 Toute personne ayant un accès direct aux données cliniques doit s'assurer de respecter, la Déclaration d'Helsinki, les directives de la CIH/BPC, les exigences réglementaires applicables pour le maintien de la confidentialité de l'identité du sujet, le respect de la propriété des informations par le promoteur ou le promoteur-chercheur.

L'authentification de la 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.

3.2 Sécurité des données

3.2.1 Un mécanisme de contrôle des accès aux locaux sécurisés doit être mis en place et documenté. Il est recommandé que le mécanisme de contrôle soit basé sur l'utilisation de cartes magnétiques ou de reconnaissance de paramètres biométriques permettant la reconstitution des allées et venues, s'il y a lieu;

3.2.2 Un document de traçage faisant état des signatures et initiales de toute personne autorisée à consigner les données ou à apporter des corrections au FEC, doit être conservé dans les documents obligatoires à remplir pour l'essai clinique;

- 3.2.3 La **sécurité physique** concerne les locaux où sont conservées les filières contenant les documents essentiels, les données cliniques, ainsi que le matériel informatique utilisé pour la gestion des données, tels que serveurs de télécommunications, serveurs de base de données, ordinateurs. Ces locaux doivent :
- être situés dans un endroit protégé de toute catastrophe (ex : dégâts d'eau ou de feu, etc.),
 - être protégés par un système de contrôle sécurisé des accès.
- 3.2.4 La **sécurité logique** concerne principalement la gestion du contrôle d'accès aux données lequel comprend l'identification, l'authentification et l'autorisation. Afin d'assurer la sécurité logique, les mesures suivantes doivent être appliquées :
- L'autorisation d'accès est limitée aux personnes de l'équipe de recherche et à celles identifiées dans le protocole, le formulaire de consentement et le formulaire de délégation de tâches;
 - Les privilèges d'accès physique ou informatique aux données sont accordés au personnel et mis à jour selon les rôles et responsabilités définis par le promoteur-chercheur ou le chercheur;
 - Nommé par le promoteur/promoteur-chercheur, 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;
 - Dans le cas où un membre de l'équipe de recherche quitte l'équipe de recherche (démission, maladie, retrait préventif, autre raison), l'autorisation d'accès qui lui était attribuée doit être annulée. Le formulaire de délégation de tâches doit refléter cette annulation;
 - 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'authentification des utilisateurs du système. Il doit également documenter le traçage des accès;
 - Un plan de sauvegarde et de récupération des données doit être établi, en cas de perte ou de sinistre;
 - Des modes opératoires normalisés sur la sécurité logique doivent être développés, mis en vigueur et respectés.

3.3 Confidentialité des données

Tel que mentionné dans le MON 17 et 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, à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique; (1982, c. 30, a.59; 1983, c. 38, a.55; 1984, c. 27, a.1; 1985, c. 30, a. 5; 1987, c. 68, a. 5; 1990, c. 57, a. 13);

- b) les renseignements nominatifs sont confidentiels; (1982, c. 30 a. 53; 1985, c. 30, a. 3; 1989, c.54, a. 150; 1990, c. 57, a. 11.);
- c) dans un document, sont nominatifs les renseignements qui concernent une personne physique et permettent de l'identifier; (1982, c. 30, a. 54.);
- d) toute personne a le droit d'être informée de l'existence, dans un fichier de renseignements personnels, d'un renseignement nominatif la concernant; (1982, c. 30, a. 83, 1987, c.68, a.6; 1990, c.57, a.21; 1992, c.21, a. 74);

3.3.1 La confidentialité des dossiers pouvant servir à identifier les sujets doit être protégée conformément aux règles relatives à la protection des renseignements personnels et à la confidentialité établies dans les exigences réglementaires applicables; référence CIH 2.11 et le MSSS : *cadre global de gestion des actifs informationnels* – Volet Sécurité,

3.3.2 Le sujet qui autorise l'accès aux données le concernant doit être raisonnablement assuré que le promoteur/promoteur-chercheur, le chercheur, les représentants autorisés par le promoteur/promoteur-chercheur, le comité d'éthique et les auditeurs et inspecteurs des autorités réglementaires ont pris toutes les précautions pour que les données vérifiées et recueillies demeurent confidentielles, CIH 5.15.1

3.3.3 La confidentialité des données doit être maintenue et respectée pendant et après l'essai clinique.

4. Références

CHUM, Politique cadre sur la gestion de l'information.

CIH, 1^{er} mai 1996, E6, Les bonnes pratiques cliniques.

Santé Canada, Lois et règlements sur les aliments et drogues – Titre 5 : Drogues destinées aux essais cliniques sur des sujets humains.

Déclaration d'Helsinki 2002.

L.R.Q., Chapitre A-2.1, Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

FRSQ, Guide d'éthique de la recherche et d'intégrité scientifique, Cadre réglementaire des Bonnes pratiques de la recherche dans les établissements universitaires de santé du Québec, août 2003.

MSSS, Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux : Volet Sécurité, septembre 2002.

FDA, 21 CFR Part 11, Electronic Records; Electronic Signatures Final Rule. Federal Register Vol. 62, No 54, 13429, March 20, 1997.

MON 03, Équipe de recherche.

MON 08, Processus de consentement et FC du sujet.

MON 18, Gestion des données et documents de base.