Soins continus Bruyère
Comité d'éthique de la recherche

Planification de la gestion du risque : entreposage, transfert et destruction/élimination des informations sensibles

Un guide pour les chercheurs

Le présent document a pour but d'aider les chercheurs à mieux comprendre les normes et politiques législatives en vigueur pour protéger les informations (sur la santé des personnes) durant l'entreposage des données, pendant leur transfert depuis leur source, et enfin lors de leur élimination.

Les dépositaires de renseignements sur la santé (habituellement les hôpitaux) sont tenus de protéger les renseignements personnels contre le vol, la perte et la consultation, la copie, la modification, l'utilisation, la divulgation et l'élimination non autorisées. Les dépositaires ont l'obligation expresse d'avertir les individus de toute atteinte à leur vie privée.

1. Quand faut-il codifier les données contenant des renseignements personnels sur la santé?

Les lois régissant l'usage de renseignements personnels (sur la santé) précisent qu'à des fins de protection de la vie privée, tout renseignement de ce type doit être codifié ou crypté dans les meilleurs délais pendant la collecte des données, afin d'éviter que les individus concernés soient identifiables. Les données cryptées/codifiées et les clés de cryptage/codification doivent être conservées séparément, en sûreté.

Veuillez noter que les initiales du sujet ou tout autre identifiant personnel ne peuvent faire partie du code, à moins de bien les brouiller et les intégrer avec au moins une autre lettre non reliée au sujet. **À la section 19c de l'application CCER, vous devez décrire en détail quand et comment les données seront codifiées afin de retirer tous les identifiants personnels.**

À l'exception du code attribué au sujet de la recherche, aucun identifiant personnel direct ou indirect ne peut faire partie des données de la recherche.

2. Comment assurer un entreposage adéquat des renseignements personnels sur la santé?

La politique de Bruyère (DOC 02) stipule que tout renseignement en format papier (dossiers médicaux, notes de travail des professionnels de la santé, etc.) doit être entreposé dans un endroit sûr verrouillé, soit auprès du Service à la clientèle et de l'information sur la santé (auparavant Service des dossiers médicaux), soit dans une salle de stockage des dossiers médicaux, soit au sein de l'unité, soit à la clinique ou au service où le patient se trouve ou a été suivi, et uniquement accessible au personnel autorisé.
Tout renseignement personnel sur support électronique (y compris les dossiers médicaux électroniques) est stocké à un endroit protégé par des mécanismes matériels et techniques de sécurité. Les supports de stockage amovibles (CD, etc.) contenant des renseignements personnels sur la santé doivent être conservés dans des endroits sûrs ou verrouillés.

Tous les renseignements personnels sur la santé en format électronique doivent être protégés par un mot de passe. Il est recommandé de toujours choisir un mot de passe « complexe ». Pour de plus amples informations et des suggestions sur le choix d'un bon mot de passe, veuillez consulter sur InfoNet le site Web de Bruyère sur les systèmes informatiques.

Lorsqu'ils accèdent à distance par RPV (réseau privé virtuel) à des renseignements personnels sur la santé, les chercheurs doivent s'assurer que ceux-ci sont invisibles aux utilisateurs non autorisés.

Ne jamais stocker de données anonymisées (dépourvues de données identifiantes) au même endroit que les listes de sujets ou autres renseignements identifiants.

En plus de l'énoncé général de politique des trois Conseils, les Instituts canadiens de recherche en santé (ICRS) ont publié un document sur les pratiques à suivre en matière de protection de la vie privée dans la recherche médicale. Ce document souligne les points suivants sur le stockage des données sensibles (ICRS, 2005) :

- Les données doivent être évaluées en fonction de leur vulnérabilité aux menaces et au risque. Cette évaluation comporte sept étapes (déterminer quels biens doivent être protégés, contre quoi il faut se protéger, la probabilité de la menace, les conséquences éventuelles, les mesures de sécurité existantes, recommander des mesures additionnelles et faire une mise à jour régulière).

- Pour assurer la sécurité des données, il faut prendre des mesures organisationnelles, technologiques et physiques.

  - Parmi les mesures organisationnelles, il faut s'assurer que tous les participants à la recherche reconnaissent expressément l'importance de la protection de la vie privée, que l'accès aux renseignements personnels est strictement limité, que des conventions de partage sont signées entre le chercheur/l'institution et les parties concernées, que les conséquences d'une violation de la confidentialité sont clairement énoncées et consacrer des ressources suffisantes aux politiques et procédures sur la vie privée et la sûreté.

  - Les mesures technologiques comprennent le cryptage, le retrait des identifiants directs dès que possible (et, si le retrait n'est pas possible, l'isolement sur un serveur/réseau indépendant réservé à cette fin), le camouflage des échantillons au besoin pour y empêcher l'accès avant l'obtention d'un consentement, des mesures d'authentification (p.ex. mots de passe), une protection particulière pour l'accès à distance, des logiciels antivirus, des sauvegardes régulières des données et, dans la mesure du possible, un système de pistage et surveillance pour consigner le nom de l'utilisateur, l'heure et la nature de l'accès aux données.

  - Les mesures physiques comprennent le rangement des ordinateurs et des fichiers dans des pièces fermées à clé, celui des documents sur papier dans des meubles verrouillés, le confinement des renseignements personnels, l'interdiction au public des lieux d'entreposage, une surveillance systématique et une protection contre les incendies et les inondations.

Tous les renseignements médicaux personnels au format papier ou sur supports de stockage amovibles (CD, etc.) doivent être conservés dans un meuble verrouillé et accessible uniquement aux membres de l'équipe de recherche impliqués dans ce projet précis et qui ont transmis un serment de confidentialité au CÉR.

Dans la section 19e de l'application CCER, vous devez indiquer l'endroit où la liste des codes sera stockée et le moment de sa destruction. Décrire aussi les mesures prises pour garantir le stockage en sûreté de la liste des codes au cas où le chercheur principal du site ou un autre membre du personnel autorisé n'est plus actif sur le site.

Conformément à la politique de Bruyère (DOC 12), par mesure de sécurité, la liste de référence originale des codes peut être conservée au sein du Service à la clientèle et de l'information sur la

santé (auparavant Service des dossiers médicaux) pour une durée approuvée. La liste des codes doit être accompagnée d'une fiche d'information donnant le titre du projet, le nom du chercheur principal, et une déclaration affirmant que toutes les copies de la liste des codes ont été détruites (ou la date prévue de la destruction).

3. Durée de la conservation

Les ICRS stipulent que les données personnelles doivent être conservées aussi longtemps que nécessaire aux fins de la recherche. Elles peuvent ensuite être détruites conformément aux dispositions de l'entente initiale de collecte et de partage des données, des politiques de l'établissement et des exigences réglementaires.

Dans l'application CCER, les chercheurs doivent être explicites quant à ce qu'ils comptent faire des données qu'ils collectent, y compris le stockage, les procédures de gestion et de destruction.

4. Transfert des données identifiables depuis la source

Éviter, autant que possible, de sortir les données du site, que ce soit au format papier ou électronique.

Les directives de la section 19f de l'application CCER stipulent que les données contenant des identifiants personnels ne doivent pas quitter les locaux du centre de recherche. En cas de transfert des données contenant des identifiants personnels vers une autre installation de recherche, il faut en expliquer la raison dans cette section. De plus, il faut décrire les méthodes qui seront utilisées pour que ces renseignements demeurent confidentiels au site de destination. Inclure également la preuve qu'un représentant (p.ex. directeur général ou directeur des finances) du site de destination (habilité à engager son institution) a consenti à conserver et détruire les données contenant des identifiants personnels conformément au protocole de l'étude décrit dans cette application.

En cas de transport des renseignements personnels en format papier ou sur supports de stockage amovibles (CD, etc.), ceux-ci doivent être conservés dans un meuble verrouillé et accessible uniquement aux membres de l'équipe de recherche impliqués dans ce projet précis et qui ont transmis un serment de confidentialité au CÉR. Voici quelques directives générales :

a. Ne jamais laisser les données sans surveillance ou dans des endroits non sûrs (p.ex. voiture fermée à clé), car cela accroît le risque de violations accidentelles de la confidentialité.
b. S'assurer que les ordinateurs et les fichiers sont protégés par un mot de passe.
c. Ne jamais transporter avec les données anonymisées des listes d'identifiants ou toute autre indication permettant d'identifier des individus de la base de données anonymisée.
d. Toujours transporter au plus vite les données collectées vers le site sécurisé approuvé, et s'assurer que les données collectées hors site sont anonymisées dans les meilleurs délais.
e. Toujours faire très attention en cas de transfert des données par courriel; le courriel n'est pas un moyen de communication sûr. Les procédures de sûreté pour l'envoi par courriel sont particulièrement importantes.

5. Destruction/élimination des renseignements personnels sur la santé

Afin de protéger la confidentialité des renseignements personnels, les documents sur papier doivent être déchiquetés après usage, avant d'être recyclés.

Pour le déchiquetage des CD, on peut faire appel à Shred-It, une entreprise sous contrat avec l’hôpital.

Lorsque les ordinateurs qui contiennent des renseignements médicaux personnels ne sont plus nécessaires, il faut nettoyer les lecteurs par un triple effacement (DOC 02, alinéa 5.2). Lorsque l’on efface l’information sur un disque dur, elle n’est pas vraiment effacée – ou plutôt elle peut être récupérée. La procédure du triple effacement se fait avec un logiciel appelé GDisk (édité par Symantec), qui inscrit des zéros sur tous les secteurs des disques durs, et ce par trois fois. Pour de plus amples informations sur l’utilisation de GDisk, veuillez consulter le guide de référence de Symantec Ghost.

Le triple effacement n’est pas identique à la défragmentation d’un disque dur. La défragmentation réorganise les données éparpillées à travers le disque (fragmenté), de manière à ce qu'il soit plus organisé; cela facilite la recherche de données sur le disque dur. Le triple effacement détruit définitivement les renseignements sur le disque ou lecteur.