Guide

Gestion des données numériques de recherche



Présenté par

Recherche clinique Québec[MD]

Propulsé par

CATALIS[MD]

TABLE DES MATIÈRES

Table des matières 2

Avant-propos 4

Introduction 4

Ce que vous trouverez dans ce guide 4

Ce que ce guide n'est pas 5

Comment utiliser ce guide 5

1. Données numériques de recherche, de quoi parle-t-on? 6

1.1 Une définition des données de recherche 6

1.2 Exemples concrets de données numériques de recherche 6

1.3 Explication des types de données 7

2. Le cycle de vie des données numériques en recherche 9

3. Planifier et concevoir un projet de recherche mobilisant des données 10

3.1 Les questions essentielles à se poser avant de commencer 10

3.2 Une bonne pratique à adopter : le Plan de gestion des données (PGD) 11

3.3 Faut-il réaliser une Évaluation des facteurs relatifs à la vie privée (EFVP)? 12

4. Collecter et documenter les données 13

4.1 Les risques importants à considérer 13

4.2 Les bonnes questions à se poser pour protéger les participants dès la collecte et la saisie des données 14

4.3 Les bonnes pratiques pour assurer la qualité et la traçabilité des données 15

5. Stocker et sécuriser les données 16

5.1 Les risques importants à considérer 16

5.2 Les bonnes questions à se poser avant de débuter le stockage 16

5.3 Les bonnes pratiques pour stocker et sécuriser les données 17

6. Utiliser et analyser les données 18

6.1 Les risques importants à considérer 18

6.2 Les bonnes questions à se poser avant de choisir et d'utiliser un outil d'analyse 19

6.3 Utiliser l'IA générative pour analyser les données de recherche : enjeux spécifiques et bonnes pratiques 19

7. Transférer les données et donner accès 20

7.1 Ce que signifie transférer des données ou donner accès 20

7.2 Les risques importants à considérer en matière de transfert et d'accès 21
7.3 Les bonnes questions à se poser avant de transférer des données ou de donner accès 21
8. Déposer et permettre la réutilisation des données 22
8.1 Ce que signifie permettre la réutilisation des données 22
8.2 Les bonnes questions à se poser avant de déposer des données ou d'en permettre la réutilisation 23
8.3. Choisir où et comment déposer ses données 24
9. Clôturer un projet 25
9.1 Les risques importants à considérer 25
9.2 Les bonnes questions à se poser au moment de clôturer un projet 25
9.3 Les bonnes pratiques à adopter pour archiver les données à long terme 26
Annexe : Liste des ressources utiles en gestion des données de recherche 28

AVANT-PROPOS

CATALIS est un organisme québécois à but non lucratif (OBNL), neutre et indépendant, qui collabore avec les établissements de santé, les compagnies pharmaceutiques et les associations de patients. L'information offerte vise à expliquer certains concepts de la recherche clinique et ne constitue pas un avis juridique ou professionnel.

INTRODUCTION

À l'ère de la recherche numérique et de l'intelligence artificielle, les données occupent une place considérable au sein de la recherche clinique. Que l'on parle de questionnaires électroniques, de dossiers cliniques, d'images médicales, les données numériques sont maintenant omniprésentes en recherche et nécessitent une attention particulière.

Bien gérer ces données de recherche est en effet essentiel. Il ne s'agit pas uniquement de respecter un ensemble d'exigences légales, éthiques ou institutionnelles encadrant la recherche. En conduisant une bonne gestion des données numériques de recherche, on s'assure en fait de préserver la qualité et l'intégrité de ces données, d'assurer la traçabilité des activités de recherche et de favoriser la reproductibilité des résultats produits. Et si l'on est amené à traiter des renseignements personnels de participants, la gestion des données numériques de recherche vise à assurer la protection de la confidentialité et le maintien de la confiance. Voici donc la raison d'être du guide élaboré par CATALIS.

Ce que vous trouverez dans ce guide

Ce guide a été conçu pour accompagner les équipes dans la gestion des données numériques tout au long de leur projet de recherche. Il commence par quelques notions essentielles pour bien comprendre ce que sont les données numériques de recherche et les différents types de données que vous pouvez rencontrer.

Il présente ensuite leur cycle de vie à travers sept grandes étapes : planifier et concevoir; collecter et documenter; stocker et sécuriser; utiliser et analyser; transférer et donner accès; déposer et permettre la réutilisation; et enfin, clôturer le projet de recherche.

À chacune de ces étapes, vous trouverez des explications sur les principaux enjeux et risques à considérer, des questions pour vous aider à évaluer vos pratiques ainsi que des recommandations concrètes pour vous guider dans une gestion efficace et responsable de vos données numériques de recherche. À la toute fin du guide, un ensemble de ressources vous aident également à approfondir plusieurs enjeux et bonnes pratiques.

Ce que ce guide n'est pas



Bien qu'il propose un ensemble d'informations utiles et de nombreuses références, ce guide ne peut aborder toutes les obligations, les responsabilités et les recommandations en matière de gestion des données de recherche. **Vous n'y trouverez donc pas l'ensemble des exigences qui peuvent s'appliquer à votre projet de recherche et à vos données.** Ce guide ne peut non plus remplacer la connaissance et l'analyse des politiques, des procédures et des directives de votre établissement, de votre comité d'éthique, de votre promoteur ou de votre organisme subventionnaire.

De plus, le présent guide ne vise pas à recommander une plateforme ou un outil unique pour la gestion des données numériques de recherche. En effet, les solutions disponibles et autorisées varient selon les établissements, les projets et la nature des données utilisées. L'objectif du guide est donc plutôt de vous orienter dans les bonnes questions à se poser avant de choisir une plateforme ou un outil.

Comment utiliser ce guide

Vous pouvez lire ce guide dans son ensemble pour mieux comprendre le cycle de vie des données, mais aussi le consulter au fur et à mesure de l'avancement de votre projet. Vous pouvez également explorer en priorité une étape du cycle qui vous semble plus importante pour votre recherche et vos données.

L'objectif est finalement de vous donner des repères simples pour mieux gérer vos données au quotidien et savoir quelles vérifications effectuer lorsque vous devez prendre une décision.

Veuillez considérer ce guide comme un complément de la formation RCQ Gestion des données d'études.

1. DONNÉES NUMÉRIQUES DE RECHERCHE, DE QUOI PARLE-T-ON?

1.1 Une définition des données de recherche



Pour commencer, il est important de bien définir **ce que sont les données de recherche**. Selon la définition qu'en donnent les Trois Conseils au Canada (les Instituts de recherche en santé du Canada (IRSC), le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) et le Conseil de recherches en sciences humaines du Canada (CRSH)) :

« Les données de recherche sont des données qui sont utilisées en tant que sources principales à l'appui d'une enquête technique ou scientifique, d'une recherche, de travaux d'érudition ou de pratiques créatives et qui sont utilisées comme éléments de preuve dans un processus de recherche ou qui sont communément acceptées au sein de la communauté de recherche comme nécessaires pour valider les conclusions et les résultats de recherche. »

Pour en savoir plus

Dans ce guide, nous nous intéressons en particulier aux **données numériques de recherche**, c'est-à-dire à l'ensemble des données de recherche qui se trouvent dans un format électronique et non dans un format papier.

Mais qu'entend-on exactement par « données numériques de recherche »?

1.2 Exemples concrets de données numériques de recherche

Les données numériques de recherche peuvent être, par exemple :

- Les extraits de dossiers cliniques provenant d'un dossier patient informatisé;
- Les résultats de questionnaires et autres formulaires électroniques de collecte de données;
- Les verbatims d'entrevues et autres données qualitatives;
- Les images médicales, les données génomiques, les résultats de laboratoire et autres données concernant les participants;
- Les données générées par des appareils, des capteurs ou d'autres dispositifs médicaux;
- Les carnets de laboratoire électroniques;
- Les données relatives aux vérifications, aux corrections et aux requêtes (*queries*) effectuées dans la base de données;

- Les pistes d'audit (*audit trails*) et historiques de modifications permettant de retracer les opérations effectuées sur les données;
- Les données permettant de suivre le déroulement de l'étude, comme le recrutement, les visites, les déviations au protocole ou le statut des participants;
- Les communications, courriels et décisions qui sont prises lors du déroulement d'une étude.

Cette liste n'est bien sûr pas exhaustive. Mais vous pouvez voir d'emblée que **les données numériques de recherche sont extrêmement variées.**

1.3 Explication des types de données

Pour y voir plus clair dans le vaste monde des données numériques de recherche, il est important de les catégoriser. **Cela permet d'appliquer des pratiques de gestion différentes selon les types de données concernées.**

Voici quelques distinctions importantes pour bien différencier les types de données numériques de recherche :

- Suivant l'origine des données :

Type de données	Ce qu'il faut retenir	Exemple
Données brutes	Données telles qu'elles sont initialement recueillies ou générées, avant leur traitement pour l'analyse. Ce sont les seules données dont la perte est irrécupérable.	Réponses originales à un questionnaire électronique, signes vitaux.
Données dérivées	Données créées à partir d'autres données par un calcul, une transformation ou une combinaison.	Âge calculé à partir de la date de naissance, surface corporelle.
Données analysées	Données préparées ou utilisées pour réaliser les analyses et produire les résultats de recherche.	Jeu de données nettoyé utilisé pour une analyse statistique.

- Suivant la façon de présenter les données :

Type de données	Ce qu'il faut retenir	Exemple
Données non structurées	Données qui ne sont pas organisées selon une structure prédéfinie.	Images médicales, notes, verbatims, fichiers audio
Données structurées	Données organisées selon une structure prédéfinie, généralement en champs, lignes et colonnes.	Liste d'évolution des signes vitaux dans le temps, profil pharmacocinétique. Base de données clinique
Données agrégées	Données regroupées ou résumées à partir de plusieurs observations ou individus, suivant des critères, plutôt que présentées individuellement.	Nombre moyen de visites à l'urgence par groupe d'âge et suivant le mois de l'année.

Parmi les données numériques de recherche, certaines constituent des **renseignements personnels**, c'est-à-dire des informations qui concernent une personne physique et qui permettent de l'identifier directement (comme par le nom d'un patient, son numéro d'assurance maladie) ou indirectement (par un regroupement d'identifiants, tels qu'un code postal et une profession).
En recherche chez l'humain, une attention particulière doit être portée aux **renseignements de santé et de services sociaux**, qui sont encadrés au Québec par un régime juridique spécifique (voir **Encadré 1**).

Encadré 1 : Des données numériques de recherche aux renseignements de santé et de services sociaux

Toutes les données de recherche ne sont pas des renseignements personnels. Cependant, en recherche chez l'humain, les équipes travaillent fréquemment avec des renseignements concernant des personnes physiques identifiables ou pouvant être identifiées.

Parmi les renseignements personnels utilisés en recherche, certains constituent **des renseignements de santé et de services sociaux**, tels que les informations provenant du dossier clinique d'une personne. Au Québec, ces renseignements font l'objet d'un régime particulier de protection prévu par la *Loi sur les renseignements de santé et de services sociaux* (Loi 5). Celle-ci encadre notamment leur collecte, leur utilisation, leur

communication, leur conservation et leur accès, lorsque ces renseignements sont détenus ou utilisés au sein du réseau de la santé et des services sociaux du Québec.

Ce qu'il faut retenir : Dès qu'un projet de recherche mobilise des renseignements de santé et de services sociaux, des exigences particulières peuvent s'appliquer. Avant de les collecter, de les utiliser, de les transférer ou de les partager, vérifiez les autorisations requises et les règles applicables auprès de votre établissement.

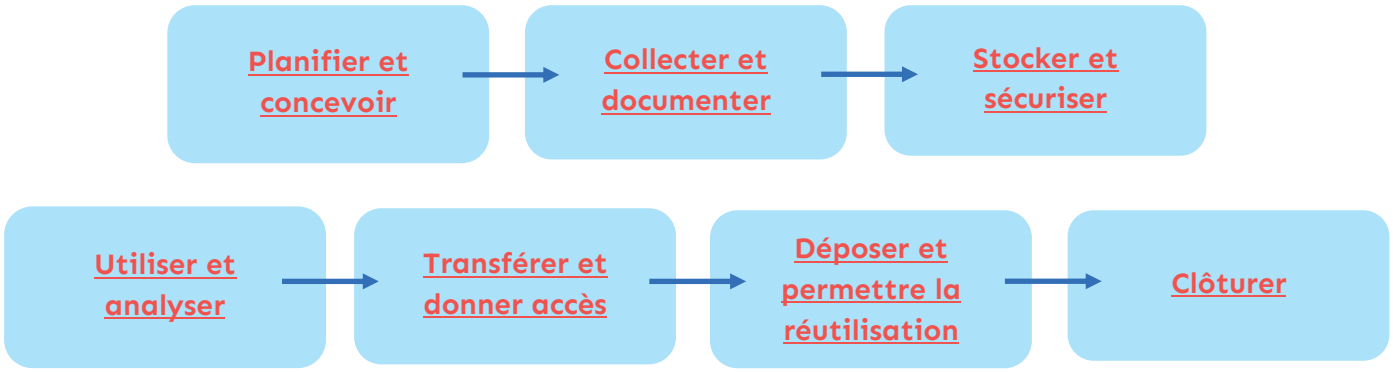
Pour en savoir plus

2. LE CYCLE DE VIE DES DONNÉES NUMÉRIQUES EN RECHERCHE

Les données numériques évoluent tout au long d'un projet de recherche. Elles sont planifiées, collectées, documentées, stockées, utilisées et parfois transférées, avant que leur devenir ne soit finalement déterminé au moment de la clôture du projet.

C'est ce qu'on appelle **le cycle de vie des données numériques de recherche**. Envisager les données numériques selon leur cycle de vie permet d'anticiper les décisions à prendre et d'adopter les bonnes pratiques au bon moment. La gestion des données ne commence donc pas au moment de leur collecte et ne se termine pas une fois les analyses réalisées. Elle doit être réfléchie dès la conception du projet et elle doit se poursuivre jusqu'à sa clôture.

Dans ce guide, le cycle de vie des données numériques de recherche vous est présenté à travers sept grandes étapes :



Ces étapes ne s'appliquent pas nécessairement à tous les projets, dans la mesure où elles peuvent varier selon le contexte. Par ailleurs, des personnes différentes peuvent être responsables des différentes étapes du cycle de vie. Il est donc important que les responsabilités soient clairement définies pour chaque projet de recherche.

De plus, les étapes du cycle de vie ne sont pas toujours parfaitement linéaires. Au cours d'un même projet, des données peuvent être collectées, vérifiées, corrigées et analysées à plusieurs reprises. Les décisions prises à une étape peuvent également avoir des conséquences sur les suivantes.

Enfin, la clôture d'un projet de recherche ne signifie pas nécessairement la destruction de toutes les données qui y sont associées. Selon leur nature et les exigences applicables, certaines données devront être archivées à long terme, d'autres pourront être réutilisées, et d'autres encore pourront être anonymisées ou détruites.

3. PLANIFIER ET CONCEVOIR UN PROJET DE RECHERCHE MOBILISANT DES DONNÉES

3.1 Les questions essentielles à se poser avant de commencer

Avant même de commencer à collecter ou à utiliser des données, il est important de préciser le contexte dans lequel elles seront utilisées. Quelques questions essentielles peuvent vous guider dans cette réflexion :



- Quelles sont les personnes responsables de la gestion des données et du suivi des étapes du projet?
- Quelles données seront réellement nécessaires pour répondre à la question de recherche et quel est l'usage prévu?
- D'où proviennent les données?
- Quels sont les lois, règlements, politiques et normes applicables aux types de données mobilisées dans le cadre du projet de recherche?
- Les BPC (ICH E6(R3)) préconisent la concentration des efforts sur les risques critiques. Il est important d'identifier les données critiques afin de leur attribuer le plus de précautions.
- Comment les données seront-elles collectées et de quelle(s) source(s)?
- Le projet de recherche comporte-t-il des risques particuliers en lien avec la nature des données ou le type de participants mobilisés?
- Est-ce que le protocole de mon projet de recherche prévoit toutes les étapes de gestion des données applicables?
- Quels outils et plateformes numériques seront utilisés pour la collecte, la saisie, le stockage, l'analyse et le partage des données?
- Quels seront les coûts envisagés pour assurer une bonne gestion des données de recherche?

Pour répondre à ces questions, l'élaboration d'un Plan de gestion des données (PGD) peut vous être d'une grande aide.

3.2 Une bonne pratique à adopter : le Plan de gestion des données (PGD)

Pour commencer, le PGD est un document qui décrit la manière dont les données seront gérées pendant toutes les étapes d'un projet de recherche. **Il s'agit d'un document « vivant » qui peut être révisé et adapté au fur et à mesure que votre projet évolue.**

Par ailleurs, la préparation d'un PGD fait de plus en plus partie des attentes des organismes subventionnaires, même si sa soumission n'est pas toujours exigée. Dans tous les cas, l'élaboration d'un PGD constitue une pratique exemplaire pour les projets de recherche, notamment en recherche clinique, puisqu'elle permet d'anticiper les besoins, les responsabilités et les ressources nécessaires en vue de bien gérer les données numériques de recherche.

Voici les sections principales d'un PGD selon l'Alliance de recherche numérique du Canada :

Section du PGD	Ce qu'il faut prévoir
Collecte des données	Les types de données qui seront collectées, les formats de fichiers ainsi que les conventions de nommage et de versionnage.
Documentation	Les informations nécessaires pour permettre aux membres de votre équipe, ou à d'autres personnes, de comprendre et d'interpréter correctement les données.
Stockage et sauvegarde	Les lieux et environnements où les données seront stockées, les modalités de sauvegarde ainsi que les mesures de contrôle des accès et de prévention des pertes de données.
Conservation	Les moyens prévus pour assurer l'accès à long terme aux données qui doivent être archivées après la phase active du projet ou en fin de projet.
Partage et réutilisation	Les modalités prévues pour partager les données et permettre leur réutilisation, lorsque cela est possible.

Responsabilités et ressources	La répartition des responsabilités liées à la gestion des données ainsi que les ressources humaines, techniques et financières nécessaires.
Exigences éthiques et juridiques	Les exigences légales et éthiques applicables aux données et les moyens prévus pour les respecter. Ceci peut inclure l'obligation de réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) lorsque celle-ci est requise en vertu du cadre légal applicable (voir sous-section suivante).

Pour vous accompagner : l'Assistant PGD est un outil canadien, bilingue et gratuit qui fournit des conseils et des guides pour élaborer, réviser et partager un PGD.

3.3 Faut-il réaliser une Évaluation des facteurs relatifs à la vie privée (EFVP)?

L'EFVP est une démarche visant à protéger les renseignements personnels et la vie privée des personnes concernées par votre recherche. Réalisée dès la planification d'un projet, elle permet d'évaluer adéquatement les risques associés à votre projet et de prévoir des mesures pour les éviter ou pour les réduire.

Il est important de vous référer aux politiques et procédures de votre établissement afin de déterminer si une EFVP est requise et de connaître la démarche à suivre, ainsi qu'aux indications de Santé Québec.

Cependant voici quelques points à considérer :

Avant d'entreprendre un projet impliquant la collecte, l'utilisation, la communication ou la conservation de renseignements personnels, **il est important de déterminer si une évaluation EFVP est requise.** Les obligations applicables varient selon le contexte du projet, la nature des renseignements concernés et le cadre juridique applicable.

Plusieurs situations peuvent notamment nécessiter la réalisation d'une EFVP, notamment :

- la communication de renseignements personnels à l'extérieur du Québec;
- l'acquisition, le développement ou la refonte d'un système d'information impliquant des renseignements personnels;
- certaines communications de renseignements personnels sans le consentement des personnes concernées;
- certaines collectes de renseignements personnels réalisées pour le compte d'un autre organisme;

- certains projets de recherche ou de communication de renseignements de santé et de services sociaux visés par la législation applicable;

Pour en savoir plus

4. COLLECTER ET DOCUMENTER LES DONNÉES

Une fois ces éléments planifiés et les exigences applicables identifiées, vous pouvez maintenant passer à la collecte des données. Les choix effectués en amont guideront alors la façon dont les données seront recueillies, saisies et documentées tout au long de votre projet.

4.1 Les risques importants à considérer



Tout d'abord, rappelez-vous que la qualité de vos résultats de recherche dépend directement de la qualité de vos données. Dès la collecte et la saisie, il est donc important de **limiter les risques d'erreurs et de préserver l'intégrité et la traçabilité des données numériques de recherche**.

En effet, plusieurs problèmes peuvent survenir : des erreurs de saisie ou de transcription, des données manquantes ou incohérentes, des modifications non documentées ou encore la multiplication des versions d'un même fichier.

Si vous utilisez un formulaire électronique (par exemple, un *electronic case report form*, (« eCRF »), fréquemment utilisé en recherche clinique) ou encore un système de gestion des données (EDC), **portez bien attention aux mécanismes de vérification et de validation des données**. La gestion des requêtes (*queries*) et la documentation des corrections vous permettront notamment de repérer et de corriger les erreurs tout en conservant une trace des modifications effectuées.

Enfin, si vous collectez des renseignements personnels ou des renseignements de santé et de services sociaux, vous devez également tenir compte des obligations applicables en matière de confidentialité et de protection de la vie privée des participants. Les questions de la sous-section suivante vous aideront à bien identifier les risques associés à ces renseignements et à mettre en place des mesures pour les atténuer.

4.2 Les bonnes questions à se poser pour protéger les participants dès la collecte et la saisie des données

Au moment de la collecte et de la saisie des données, posez-vous les questions suivantes **afin de bien protéger les renseignements personnels des participants.** Cette réflexion devrait d'ailleurs être amorcée dès la planification du projet et être intégrée à votre Plan de gestion des données (PGD) :

- Les rôles et responsabilités de chaque membre de votre équipe en matière de gestion des données sont-ils clairement définis et documentés (par exemple, dans un registre de délégation des responsabilités)?
- Est-ce que seuls les renseignements nécessaires aux objectifs de votre projet seront collectés?
- Les renseignements personnels peuvent-ils être dépersonnalisés (par exemple, codés) dès leur collecte ou leur saisie afin de limiter les risques de bris de confidentialité ? Les clés de réidentification sont-elles conservées séparément des renseignements et protégées par des mesures de sécurité appropriées? (voir **Encadré 2**)
- Le formulaire de consentement décrit-il clairement la façon dont les données seront collectées, utilisées, protégées, conservées et, le cas échéant, partagées, réutilisées ou détruites?
- Les accès aux données identificatoires sont-ils limités aux seules personnes qui en ont besoin pour réaliser le projet de recherche?
- Les outils utilisés pour la collecte et la saisie offrent-ils un niveau de protection approprié à la sensibilité des renseignements?

Encadré 2 : Dépersonnaliser ou anonymiser les données : quelle différence?

Dépersonnaliser des renseignements personnels consiste à réduire le risque qu'ils permettent d'identifier directement la personne concernée. **En recherche chez l'humain, cela peut notamment consister à remplacer les identifiants directs, comme le nom ou le numéro d'assurance maladie, par un code.** Les renseignements demeurent toutefois des renseignements personnels puisqu'il est encore possible, dans certaines conditions, d'identifier la personne.

Lorsqu'un code est utilisé, **la clé de réidentification permet de faire le lien entre ce code et l'identité du participant**. Elle doit être conservée séparément des données dépersonnalisées et protégée par des mesures de sécurité appropriées. Son accès devrait être limité aux personnes qui en ont besoin et qui sont autorisées à voir des données identificatoires.

L'anonymisation va plus loin que la dépersonnalisation. Elle vise à faire en sorte qu'il ne soit plus possible d'identifier une personne, directement ou indirectement, selon les critères et les modalités prévus par la réglementation applicable. Retirer les noms ou les remplacer par des codes ne suffit donc pas à anonymiser des données.

Pour en savoir plus

4.3 Les bonnes pratiques pour assurer la qualité et la traçabilité des données

Bien documenter vos données numériques de recherche vous permet de mieux les comprendre et de pouvoir retracer leur évolution. C'est essentiel pour faciliter la collaboration entre les membres de votre équipe et rendre votre recherche reproductible au terme de votre projet. De plus, **pour assurer la qualité et la traçabilité des données numériques de recherche**, il est recommandé d'adopter des pratiques simples dès le moment de la collecte et de la saisie :

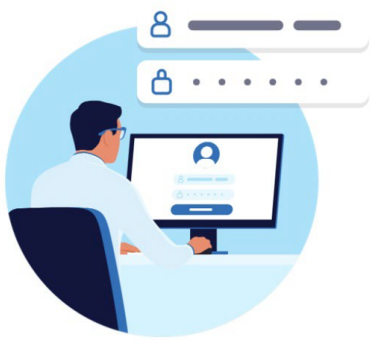
- **Utilisez des outils adaptés à votre projet** pour collecter et saisir vos données. Selon vos besoins, il peut notamment s'agir de formulaires électroniques (eCRF) ou de systèmes de gestion des données (EDC), comme REDCap.
- **Documentez vos données au fur et à mesure.** Décrivez les variables et les codes utilisés, les transformations effectuées, les algorithmes appliqués ainsi que les formats de fichiers et les logiciels utilisés, incluant leur version.
- **Concevez un fichier Lisez-moi (*Read me*).** Utilisez un fichier Lisez-moi pour présenter votre projet ou un ensemble de jeux de données et expliquer simplement son contenu et l'organisation des fichiers. Conservez-le avec les données et mettez-le à jour au besoin. Si vous avez plusieurs fichiers Lisez-moi, il est important de les structurer dans le même format.
- **Utilisez des métadonnées.** Utilisez des métadonnées pour décrire vos données : titre de la base de données ou d'un document, auteur, description, mots-clés, dates, format, langue, source, droits d'utilisation et toutes autres informations utiles pour les comprendre et les retrouver.
- **Adoptez des règles communes pour nommer et organiser vos fichiers.** Une convention de nommage et de versionnage vous permettra de retrouver plus facilement vos données et d'éviter la multiplication de versions difficiles à distinguer.
- **Effectuez des contrôles et des validations régulièrement.** Repérez les données manquantes, incohérentes ou erronées et assurez-vous que les corrections apportées sont documentées et traçables.

Pour en savoir plus

5. STOCKER ET SÉCURISER LES DONNÉES

À mesure que vos données numériques de recherche sont collectées, vous devez également prévoir où et comment elles seront entreposées. Voyons maintenant comment les stocker et les sécuriser adéquatement.

5.1 Les risques importants à considérer



Bien stocker vos données numériques de recherche est essentiel **pour préserver leur intégrité, leur confidentialité et leur disponibilité tout au long de votre projet.** Une mauvaise gestion du stockage peut notamment entraîner une altération ou une perte de données, ou encore un accès non autorisé à celles-ci.

Les causes associées à de tels risques peuvent être variées : une erreur humaine, une panne informatique, le vol d'un appareil, un logiciel malveillant ou encore une sauvegarde inadéquate. Ces actions et erreurs peuvent avoir des conséquences importantes sur le déroulement de votre projet et rendre certaines données difficiles, voire impossibles, à récupérer.

Il est donc important de planifier vos besoins et vos capacités de stockage dès le début du projet, notamment en fonction du volume et de la sensibilité des données, des types de personnes qui doivent y avoir accès et des ressources dont vous disposez.

Mise en garde : Ne confondez pas le stockage pendant la phase active du projet avec la conservation à long terme (archivage). Le stockage permet d'entreposer et d'utiliser vos données pendant vos activités de recherche. La conservation à plus long terme, quant à elle, ne permet plus d'activités sur les données. Elle sera abordée dans la section sur la clôture du projet.

5.2 Les bonnes questions à se poser avant de débuter le stockage

Avant de choisir vos solutions de stockage et d'y déposer vos données numériques de recherche, posez-vous, par exemple, les questions suivantes :

- Quel volume de données devrait être stocké pendant le projet et quelles sont les exigences en matière de capacité et de performance?
- Quels coûts et quelles ressources devez-vous prévoir pour répondre à vos besoins de stockage?
- Les données contiennent-elles des renseignements personnels, des renseignements de santé ou d'autres informations confidentielles nécessitant des mesures de protection particulières?
- La solution de stockage envisagée est-elle approuvée par mon établissement et répond-elle aux exigences du projet?
- Qui est le détenteur des données et où seront-elles hébergées (établissement, promoteur, Québec, Canada ou autre territoire)?
- Qui doit avoir accès aux données et comment ces accès seront-ils gérés tout au long du projet?
- Quelle stratégie de sauvegarde (*backup*) sera mise en place afin de protéger les données contre leur perte, leur altération ou un incident informatique?

5.3 Les bonnes pratiques pour stocker et sécuriser les données

Une fois vos besoins identifiés et votre solution de stockage choisie, quelques bonnes pratiques vous permettront de mieux protéger vos données tout au long du projet :

- **Centralisez vos données dans les espaces prévus à cet effet.** Évitez autant que possible les copies locales non contrôlées et la multiplication des données dans différents environnements de stockage, sans que cela soit justifié. Lorsque plusieurs environnements doivent être utilisés, assurez-vous de pouvoir identifier la version de référence et de maîtriser les différentes versions.
- **Maîtrisez la création et la circulation des copies de données.** Lorsque des données sont copiées, importées ou exportées, vérifiez leur complétude et leur concordance avec les données sources. Portez également attention aux doublons qui peuvent être créés lors de la synchronisation entre différents environnements.
- **Mettez en place une gestion des accès adéquate** pour minimiser les risques d'incidents de confidentialité. Accordez les accès en fonction des responsabilités de chacun et assurez-vous de les modifier ou de les retirer lorsqu'ils ne sont plus nécessaires, par exemple lors du départ d'un membre de l'équipe ou d'un changement de partenaire de recherche.
- **Assurez-vous que vos données peuvent être récupérées en cas de problème.** Prévoyez des sauvegardes (*backup*) adaptées à la nature de vos données et vérifiez qu'elles permettent de les restaurer en cas de perte, d'altération ou d'incident. Pour les données non sensibles, vous pouvez notamment suivre la règle 3-2-1 : trois copies des données, sur deux supports différents, dont une copie conservée dans un autre

emplacement. Le bon fonctionnement de la restauration d'une sauvegarde doit être régulièrement vérifié.

- **Réévaluez vos pratiques de stockage au cours du projet.** Les besoins peuvent évoluer avec le volume ou la sensibilité des données, la composition de l'équipe ou les modalités de collaboration. Assurez-vous que les solutions utilisées demeurent adaptées et conformes aux exigences de votre établissement.

Pour en savoir plus

6. UTILISER ET ANALYSER LES DONNÉES

Une fois vos données collectées et entreposées, elles peuvent être préparées pour l'analyse. Dans certains projets, notamment les essais cliniques, cette étape peut mener au gel ou au verrouillage de la base de données (*database lock*) afin d'éviter toute modification ultérieure non autorisée. Vous pouvez alors choisir les outils qui permettront d'utiliser et d'analyser vos données.

6.1 Les risques importants à considérer



L'analyse de vos données numériques de recherche nécessitent généralement différents outils selon la nature de votre projet. Il peut s'agir de logiciels statistiques, d'outils d'analyse qualitative, de plateformes spécialisées pour le code ou encore de systèmes d'intelligence artificielle (IA). **L'objectif n'est pas de vous recommander des outils en particulier mais de vous présenter des enjeux à considérer pour prendre des décisions éclairées.**

Le choix de ces outils peut d'abord présenter **des risques pour la confidentialité et la sécurité de vos données**. Certaines solutions peuvent héberger ou traiter les données dans des environnements qui ne répondent pas aux exigences de votre établissement ou de votre projet. Ce risque est particulièrement important lorsque vous utilisez des renseignements personnels, des renseignements de santé et de services sociaux ou d'autres informations confidentielles.

Des risques concernent également **l'intégrité des données et la fiabilité des résultats**. Des erreurs de paramétrage, des transformations inadéquates ou non documentées ou encore certaines limites propres aux outils peuvent affecter les analyses réalisées. Un manque de traçabilité peut également rendre difficile la vérification ou la reproduction des résultats.

Enfin, dans le contexte des essais cliniques, **une validation inadéquate des systèmes informatisés peut compromettre la fiabilité des résultats** et, selon leur usage, la sécurité des participants. Selon les principes ICH E6(R3), la validation doit être adaptée à l'usage prévu du système et proportionnelle aux risques associés.

Pour en savoir plus

6.2 Les bonnes questions à se poser avant de choisir et d'utiliser un outil d'analyse

Au moment de choisir un outil d'analyse de données numériques, voici quelques questions qui pourront vous guider :

- L'outil est-il autorisé ou recommandé par mon établissement ou par le promoteur de la recherche?
- Où les données fournies à l'outil sont-elles hébergées ou traitées?
- L'outil permet-il de protéger adéquatement les renseignements personnels ou confidentiels?
- Les accès aux données analysées par l'outil sont-ils limités aux personnes autorisées?
- Est-il possible de conserver une trace des analyses réalisées (scripts, journaux, historique des modifications)?
- Les résultats produits sont-ils reproductibles et peuvent-ils être validés par un membre de l'équipe?
- L'outil permet-il d'exporter les données dans des formats pérennes et interopérables?
- L'utilisation de l'outil nécessite-t-elle une évaluation préalable des risques pour la vie privée, notamment une EFVP (voir 3.3)?
- Une validation de l'outil pour l'usage prévu est-elle nécessaire et, si oui, quel niveau de validation est requis?
- Le promoteur qui fournit un outil peut-il en confirmer la validation?

6.3 Utiliser l'IA générative pour analyser les données de recherche : enjeux spécifiques et bonnes pratiques



De plus en plus d'outils utilisés en recherche intègrent des fonctionnalités d'IA générative. Ces technologies offrent de nouvelles possibilités pour traiter et analyser les données, mais elles comportent également des enjeux spécifiques, notamment concernant la fiabilité des résultats, le respect de la propriété intellectuelle et la protection des renseignements personnels.

Face à ces risques, **le ministère de la Cybersécurité et du Numérique (MCN)** propose plusieurs bonnes pratiques pour guider l'utilisation des outils d'IA générative dans les administrations publiques tels que les établissements de santé et de services sociaux. Ces bonnes pratiques s'ajoutent bien sûr aux lois, aux normes éthiques ainsi qu'aux politiques et règles de votre établissement et, lorsqu'applicable, du promoteur du projet de recherche.

Si vous choisissez d'utiliser un outil d'IA générative pour analyser vos données de recherche, retenez ces sept réflexes recommandés par le MCN :

- **Ne divulguez jamais de renseignements personnels ou de renseignements de santé et de services sociaux,** à moins d'en avoir l'autorisation (par consentement notamment ou à la suite d'une EFVP);
- **Vérifiez les résultats produits.** Même s'il est performant, un outil d'IA peut produire des erreurs ou des informations imprécises;
- **Consultez et respectez les conditions d'utilisation de l'outil**;
- **Assurez-vous que votre utilisation respecte les lois et les normes éthiques applicables**, notamment concernant la protection de la propriété intellectuelle;
- **Assurez-vous que le canal de communication réseau avec l'IA est chiffré** et vérifiez toujours l'adresse du site utilisé;
- **Signalez rapidement toute situation laissant croire à une fuite d'information ou à la production d'informations trompeuses, erronées ou diffamatoires** concernant votre projet ou votre organisation;
- **Soyez prudent dans le choix de vos outils et restez informé de leurs mises à jour**, de leurs améliorations et de leurs limites.

Pour en savoir plus

En cas de doute, référez-vous toujours aux règles de votre établissement avant d'utiliser un outil d'IA avec vos données numériques de recherche.

7. TRANSFÉRER LES DONNÉES ET DONNER ACCÈS

Au cours de votre projet, vos données de recherche ne resteront pas toujours dans le même environnement ni entre les mêmes mains. Leur transfert et leur accès doivent donc eux aussi être encadrés avec soin. C'est l'objet de la présente section.

7.1 Ce que signifie transférer des données ou donner accès

Au cours d'un projet de recherche, vous pourriez avoir besoin de transférer vos données de recherche numérique ou de permettre à d'autres personnes d'y accéder. C'est notamment le cas lorsque vous devez transmettre des données à un promoteur ou à une

organisation de recherche sous contrat (CRO), ou que vous voulez permettre à un collaborateur ou à un partenaire d'accéder à votre environnement de recherche numérique.

Dans ce guide, le **transfert** désigne le fait de transmettre ou de déplacer des données d'un environnement à un autre ou d'une organisation à une autre. **Donner accès** signifie plutôt permettre à une personne autorisée de consulter ou d'utiliser vos données dans l'environnement où elles se trouvent, sans nécessairement lui en transmettre une copie.

Ces activités sont à distinguer du dépôt des données aux fins de leur réutilisation par d'autres chercheurs ou utilisateurs, qui sera évoqué dans la section suivante qui aborde les bénéfices de la valorisation des données au-delà de la durée de votre projet.

7.2 Les risques importants à considérer en matière de transfert et d'accès

Chaque transfert ou accès à des données peut occasionner de nouveaux risques, notamment **la perte ou l'altération de données, un accès non autorisé ou un bris de confidentialité**. Ces risques peuvent augmenter lorsque les données sont transférées à l'extérieur de votre établissement ou rendues accessibles à des partenaires externes.

Des risques peuvent également survenir lorsque les données sont transférées ou rendues accessibles sans que les conditions applicables aient été suffisamment encadrées. Un transfert peut, par exemple, ne pas être conforme au consentement des participants, aux autorisations obtenues, aux ententes contractuelles ou aux exigences de votre établissement. Pour les renseignements personnels ou les renseignements de santé et de services sociaux communiqués à l'extérieur du Québec, des exigences supplémentaires peuvent s'appliquer, notamment la réalisation d'une **EFVP** (voir 3.3) et la conclusion d'une entente écrite.

Enfin, les risques ne dépendent pas uniquement du lieu où les données sont hébergées. Ils dépendent également des fournisseurs et organisations qui interviennent dans leur traitement, des personnes pouvant y accéder, des juridictions applicables et des mesures de protection en place. Une organisation demeure d'ailleurs responsable des renseignements personnels qui lui sont confiés lorsqu'elle les communique à un tiers.

Pour en savoir plus

7.3 Les bonnes questions à se poser avant de transférer des données ou de donner accès

Voici quelques questions qui pourront vous aider dans vos décisions de transfert et d'accès aux données :

- Les données qui seront transférées contiennent-elles des renseignements personnels, des renseignements de santé ou d'autres informations confidentielles?
- À qui les données seront-elles transférées ou rendues accessibles et pour quelle utilisation (membres de l'équipe, collaborateurs d'un autre établissement, promoteur, CRO, partenaire externe, etc.)?
- Le transfert ou l'accès est-il conforme au formulaire de consentement, aux autorisations obtenues et aux politiques de l'établissement?
- Une entente (contrat) de transfert ou d'accès doit-elle être signée?
- La solution de transfert envisagée est-elle autorisée par mon établissement et offre-t-elle un niveau de sécurité adapté à la sensibilité des données?
- Où les données seront-elles hébergées, traitées ou transiteront-elles (Québec, Canada ou autre territoire)? Est-ce qu'une EFPV est requise?
- Les accès sont-ils limités aux personnes autorisées et sont-ils révisés, modifiés ou retirés lorsque nécessaire, par exemple lorsqu'une personne quitte l'équipe, change de rôle ou n'a plus besoin d'accéder aux données?
- Le transfert ou l'accès est-il documenté et suffisamment traçable (journal des accès, historique des versions, registre des transferts, entente de partage, etc.)?

Pour en savoir plus

8. DÉPOSER ET PERMETTRE LA RÉUTILISATION DES DONNÉES

Les accès aux données accordés dans le cadre du projet répondent à des besoins immédiats de collaboration et de recherche. La réutilisation des données au-delà du projet soulève quant à elle des considérations différentes. Découvrons-les à présent.

8.1 Ce que signifie permettre la réutilisation des données

Une fois qu'elles ont été recueillies et analysées, des données numériques de recherche peuvent parfois être utilisées **au-delà de votre projet**. Cette étape est facultative et dépend des particularités du projet.

Lorsque possible, les données peuvent notamment servir à répondre à de nouvelles questions de recherche, à valider des résultats ou à soutenir de nouveaux projets de recherche. **On parle alors d'utilisation secondaire des données. Il s'agit d'un moment clé**

pour revaloriser les données et permettre la génération d'un maximum de connaissances et d'utilité, aujourd'hui et pour de futurs projets.

Une des options pour permettre l'accès et la réutilisation de certaines données de recherche à long terme est d'**envisager leur dépôt**. Mais attention, déposer des données ne signifie pas nécessairement rendre les données publiques. Selon leur sensibilité et les exigences applicables, elles peuvent être faire l'objet d'un accès contrôlé ou demeurer dans un environnement sécurisé. D'ailleurs, selon les Trois Conseils, **« les données de recherche doivent être aussi ouvertes que possible et aussi fermées que nécessaire. »**

Pour en savoir plus

8.2 Les bonnes questions à se poser avant de déposer des données ou d'en permettre la réutilisation

Avant de déposer vos données ou d'en permettre une nouvelle utilisation au-delà de votre projet de recherche, posez-vous les questions suivantes :

- Est-ce que des exigences spécifiques de dépôt de données s'appliquent à mon projet de recherche (ex. exigences d'une revue scientifique, exigences d'un organisme subventionnaire, politiques institutionnelles, etc.)?
- Les données peuvent-elles être réutilisées ou certaines restrictions s'appliquent-elles? Par exemple, le formulaire de consentement, le comité d'éthique et les règles de votre établissement permettent-ils cette réutilisation? **Sachez par exemple que des données obtenues à travers une EFVP ne peuvent pas être réutilisées (pas même dans une banque de données).**
- Les données contiennent-elles des renseignements personnels, des renseignements de santé et de services sociaux ou d'autres informations confidentielles qui nécessitent des mesures de protection ou des limitations particulières?
- Les données doivent-elles être transformées avant leur dépôt ou leur réutilisation, par exemple à travers des processus tels que la dépersonnalisation (codage) ou l'anonymisation?
- Des exigences particulières du promoteur, de l'organisme subventionnaire, ou une entente conclue avec un partenaire encadrent-elles le dépôt ou la réutilisation des données?
- Quelle licence, quelles conditions d'utilisation et quel cadre de gestion devraient accompagner les données afin d'encadrer leur réutilisation?
- Le dépôt ou l'environnement choisi permet-il d'appliquer le niveau d'accès approprié aux données?
- Les données sont-elles suffisamment documentées pour être comprises et réutilisées? (voir **Encadré 2**).

- Le format des fichiers est-il adapté à une conservation et à une réutilisation à long terme?

Pour en savoir plus

8.3. Choisir où et comment déposer ses données

Il existe différentes façons de déposer des données numériques de recherche pour favoriser leur réutilisation à long terme. Toutefois, il n'y a pas à ce jour un dépôt adapté à toutes les données et à tous les projets de recherche. Le bon choix du dépôt dépend avant tout de la nature de vos données et des conditions dans lesquelles elles pourront être réutilisées. Avant de faire votre choix, vérifiez si votre établissement, votre promoteur, votre organisme subventionnaire ou votre discipline prévoit une solution ou des exigences particulières.

Dès lors, si vous êtes amenés à devoir choisir un dépôt de données, portez notamment attention aux éléments suivants :

- **les types et les volumes de données acceptés**, qui peuvent varier d'un dépôt à l'autre;
- **la nature et la sensibilité de vos données**, incluant les restrictions qui pourraient limiter leur dépôt ou leur accès;
- **les possibilités de contrôler l'accès aux données déposées**, afin que les données puissent être rendues accessibles selon les conditions appropriées;
- **la capacité du dépôt à assurer la préservation des données à long terme**, pour maintenir notamment leur accessibilité et leur lisibilité dans le temps, malgré l'évolution des technologies et des formats de fichiers;
- **la documentation demandée par le dépôt**, afin que les données déposées puissent être comprises et, lorsque cela est permis, être réutilisées.

Il faut bien garder que l'esprit que le dépôt n'est nullement équivalent à un archivage, lequel est abordé dans la section suivante.

Pour en savoir plus

9. CLÔTURER UN PROJET

Que vos données soient destinées ou non à être réutilisées, leur gestion se poursuit jusqu'à la fin du projet. Voyons maintenant les dernières étapes à prévoir pour bien le clôturer.

9.1 Les risques importants à considérer



La fin de votre projet de recherche ne signifie pas nécessairement la fin du cycle de vie de vos données. Certaines données numériques de recherche devront encore être archivées pendant une période déterminée, tandis que d'autres pourront éventuellement être anonymisées ou détruites.

Une mauvaise gestion de cette étape peut entraîner **la destruction prématurée de données qui doivent encore être archivées ou, au contraire, leur archivage au-delà de la période nécessaire.** Dans le premier cas, la perte de données peut nuire à la traçabilité de la recherche et au respect de certaines exigences. Dans le second, leur archivage inutile peut augmenter les risques de perte, d'accès non autorisé ou de bris de confidentialité, en particulier lorsqu'elles contiennent des renseignements personnels ou des renseignements de santé et de services sociaux.

La façon dont les données sont archivées peut également présenter des risques. Des données incomplètes, mal documentées ou archivées dans des formats ou des environnements inadéquats peuvent devenir difficiles à retrouver, à comprendre ou à réutiliser éventuellement dans le futur.

9.2 Les bonnes questions à se poser au moment de clôturer un projet

Au moment de clôturer votre projet, prenez le temps de déterminer quelles sont les données de votre projet de recherche qui doivent être archivées ou non. Les questions suivantes peuvent ainsi vous guider :

- Quelles données de recherche doivent être archivées à la fin du projet?
- Les données qui ne doivent plus être archivées seront-elles détruites de façon sécuritaire ou anonymisées lorsque cela est approprié? (voir **Encadré 3**)
- Pendant combien de temps les données doivent-elles être archivées, et quelles exigences s'appliquent (par exemple, des exigences réglementaires, des demandes

du promoteur du comité d'éthique ou des organismes subventionnaires)? Par exemple, certains dossiers relatifs aux essais cliniques doivent être archivés pendant 5, 15 ou même 25 ans conformément aux exigences applicables.
- Les données sont-elles suffisamment documentées pour pouvoir être comprises et éventuellement réutilisées ultérieurement (métadonnées, dictionnaire de données, fichier lisez-moi, scripts d'analyse, etc.)?
- Les accès aux données, aux plateformes de stockage et aux outils d'analyse ont-ils été révisés et retirés lorsque nécessaire?

9.3 Les bonnes pratiques à adopter pour archiver les données à long terme

Une fois que vous avez déterminé quelles données de recherche doivent être archivées et pendant combien de temps, vous devez vous assurer qu'elles seront entreposées dans des conditions appropriées. Voici quelques bonnes pratiques à adopter en la matière :

- **Archivez la version finale des données, accompagnée de l'ensemble de la documentation nécessaire à leur compréhension.**
- **Privilégiez des formats de fichiers ouverts**, largement utilisés et pérennes lorsque cela est possible afin de faciliter la consultation et la réutilisation futures.
- **Vérifiez l'intégrité et la complétude des données avant leur archivage** afin de s'assurer qu'aucun fichier essentiel ne manque ou n'est corrompu.
- **Archivez les données dans un environnement institutionnel offrant des garanties** de sécurité et de préservation à long terme et qualifiez tout fournisseur de service (coir ICH E6(R3)).
- **Sauvegardez les informations nécessaires à la traçabilité des données**, notamment les versions finales, les dates, les responsables et les principales transformations réalisées au cours du projet.
- **Documentez les modalités d'archivage,** notamment les délais de stockage, les restrictions d'accès, les conditions de réutilisation ainsi que les décisions relatives à la destruction ou à l'anonymisation des données.

Encadré 3 : Détruire ou anonymiser les renseignements personnels?

Les données recueillies dans le cadre de votre recherche ne doivent pas nécessairement être détruites lorsque votre projet prend fin. La durée pendant laquelle les données doivent être archivées dépend de votre projet et des exigences qui s'y appliquent, notamment lorsque vous avez collecté des renseignements personnels. L'EPTC 2 rappelle notamment que cette durée peut varier selon la nature des données, le domaine de recherche et les objectifs du projet.

À la fin de la période pendant laquelle vous devez conserver des renseignements

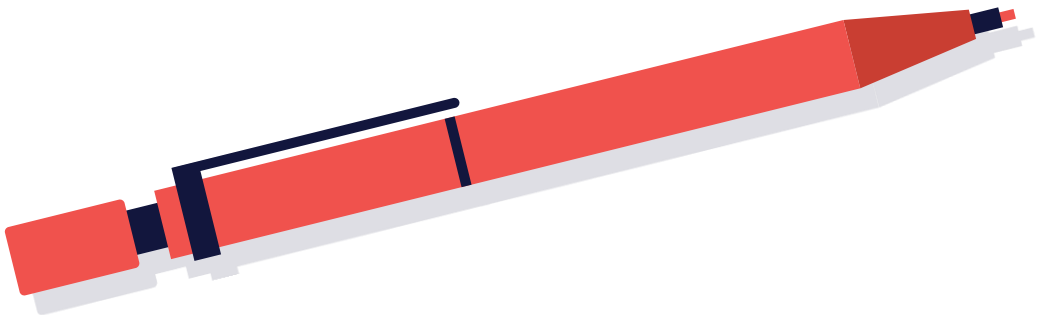
personnels, deux options s'offrent à vous : les détruire de façon sécuritaire ou les anonymiser. Au Québec, ces obligations sont prévues par les lois sur la protection des renseignements personnels, notamment la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, la *Loi sur la protection des renseignements personnels dans le secteur privé*, la *Loi sur les renseignements de santé et de services sociaux*, et le *Règlement sur l'anonymisation des renseignements personnels.*

Il est également à noter qu'anonymiser des données ne consiste pas simplement à retirer le nom des participants. Une donnée anonymisée est une donnée qui ne permet plus d'identifier une personne, directement ou indirectement, et pour laquelle le risque de réidentification a été réduit à un niveau permettant de considérer l'anonymisation comme irréversible. Au Québec, ce processus est encadré par le *Règlement sur l'anonymisation des renseignements personnels*.

Pour en savoir plus



La clôture de votre projet marque ainsi la dernière étape de ce guide, mais pas nécessairement la fin du cycle de vie de vos données numériques de recherche. Rappelez-vous pour finir qu'une gestion réfléchie tout au long de votre projet vous permettra de préserver leur intégrité et leur valeur, tout en respectant les personnes qui ont contribué à la recherche. Il s'agit de considérations essentielles en recherche clinique.



ANNEXE : LISTE DES RESSOURCES UTILES EN GESTION DES DONNÉES DE RECHERCHE

Nom de la ressource	Source	Cycle de vie de la donnée	Lien vers la ressource
Glossaires sur la gestion des données de recherche	Alliance de recherche numérique du Canada	Transversal	Consulter
Politique des trois organismes sur la gestion des données de recherche – Foire aux questions	IRSC, CRSNG et CRSH	Transversal	Consulter
Matrice de risque lié aux données de recherche avec des êtres humains et bonnes pratiques associées	Portage	Transversal	Consulter
La gestion des données de recherche et les données sensibles	Université de Sherbrooke	Transversal	Consulter
Harvard Biomedical Data Management	Harvard Medical School	Transversal	Consulter
Introduction à la gestion des données de recherche	Portage / Conseil du leadership sur l'infrastructure de recherche numérique	Transversal	Consulter
Comprendre la gestion des données de recherche	Université Laval	Transversal	Consulter
Ressources de formation en gestion des données de recherche	Alliance de recherche numérique du Canada	Transversal	Consulter

Gestion des données de recherche	Alliance de recherche numérique du Canada	Transversal	Consulter
Guide de rédaction du plan de gestion des données	Université de Sherbrooke	Planifier et concevoir	Consulter
Outil d'aide pour le calcul des coûts liés à la GDR et liste de vérification	Université de Sherbrooke	Planifier et concevoir	Consulter
Data Management Checklist	UK Data Service	Planifier et concevoir	Consulter
Assistant PGD	Alliance de recherche numérique du Canada	Planifier et concevoir	Consulter
Modèles de plans de gestion des données	Alliance de recherche numérique du Canada	Planifier et concevoir	Consulter
Évaluation des facteurs relatifs à la vie privée : un guide plus convivial	Commission d'accès à l'information du Québec	Planifier et concevoir	Consulter
Guide d'accompagnement à la démarche d'EFVP et à sa documentation	Commission d'accès à l'information du Québec	Planifier et concevoir	Consulter
Langage en matière de gestion des données de recherche pour le consentement éclairé	Portage	Planifier et concevoir / Collecter et documenter	Consulter
Guide de nommage des fichiers numériques	CHU Sainte-Justine	Collecter et documenter	Consulter

Documentation et métadonnées	UQAC	Collecter et documenter	Consulter
Readme Files	Harvard Medical School	Collecter et documenter	Consulter
Traçabilité des activités de recherche et gestion des connaissances – Guide pratique	Réseau Qualité en recherche du CNRS	Collecter et documenter / Utiliser et analyser	Consulter
Pensez cybersécurité	Gouvernement du Canada	Stocker et sécuriser	Consulter
Protection des données, confidentialité et respect de la vie privée	Alliance de recherche numérique du Canada	Stocker et sécuriser	Consulter
La sécurité des données de recherche	Université de Sherbrooke	Stocker et sécuriser	Consulter
Infrastructures et services aux chercheurs	Calcul Québec	Stocker et sécuriser / Transférer et donner accès	Consulter
Outil interactif pour explorer les solutions de stockage des données de recherche	Université de Montréal	Stocker et sécuriser	Consulter
Stockage et accès	Université de Sherbrooke	Stocker et sécuriser	Consulter
Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics	Ministère de la Cybersécurité et du Numérique	Utiliser et analyser	Consulter

Guide des bonnes pratiques d'utilisation de l'intelligence artificielle générative	Ministère de la Cybersécurité et du Numérique	Utiliser et analyser	Consulter
Position sur l'utilisation de l'intelligence artificielle générative dans les processus des Fonds de recherche du Québec	Fonds de recherche du Québec	Utiliser et analyser	Consulter
Lignes directrices sur l'utilisation de l'intelligence artificielle dans l'élaboration et l'évaluation des propositions de recherche	Gouvernement du Canada / Trois organismes	Utiliser et analyser	Consulter
Analysis Ready Datasets	Harvard Medical School	Utiliser et analyser	Consulter
Utilisation et communication de renseignements personnels	Commission d'accès à l'information du Québec	Transférer et donner accès	Consulter
Informations sur le transfert de données	Alliance de recherche numérique du Canada	Transférer et donner accès	Consulter
Globus	Alliance de recherche numérique du Canada	Transférer et donner accès	Consulter
Politique des trois organismes sur la gestion des données de recherche	IRSC, CRSNG et CRSH	Planifier et concevoir / Déposer et permettre la réutilisation	Consulter
EPTC 2 (2022), chapitre 5 – Respect de la vie privée et confidentialité	Groupe en éthique de la recherche	Transversal	Consulter

Puis-je partager mes données?	Alliance de recherche numérique du Canada / Portage	Déposer et permettre la réutilisation	Consulter
FAIR Principles	GO FAIR	Déposer et permettre la réutilisation	Consulter
Partage et réutilisation des données	Université de Sherbrooke	Déposer et permettre la réutilisation	Consulter
Conservation et destruction des renseignements personnels	Commission d'accès à l'information du Québec	Clôturer	Consulter
Règlement sur l'anonymisation des renseignements personnels	Gouvernement du Québec	Clôturer	Consulter
Techniques d'anonymisation de données	Université de Montréal	Clôturer	Consulter
Guide d'évaluation pour la préservation des données de recherche	Université de Sherbrooke	Clôturer	Consulter