# RECOMMANDATIONS DU CÉR DU CIUSSS DE L'ESTRIE – CHUS EN MATIÈRE DE SÉCURITÉ DES DONNÉES EN RECHERCHE

# Conservation et partage des données dans le cadre de la recherche

PAR LE BUREAU D'AUTORISATION DES PROJETS DE RECHERCHE DE LA DIRECTION DE LA COORDINATION DE LA MISSION UNIVERSITAIRE ET LE COMITÉ D'ÉTHIQUE DE LA RECHERCHE DU CENTRE INTÉGRÉ UNIVERSITAIRE DE SANTÉ ET DE SERVICES SOCIAUX DE L'ESTRIE – CENTRE HOSPITALIER UNIVERSITAIRE DE SHERBROOKE

LE 10 DÉCEMBRE 2020

Québec

**Production, rédaction et révision**
Valery Lussier, conseillère en éthique de la recherche
*Bureau d'autorisation des projets de recherche*
Direction de la coordination de la mission universitaire
Et
Annabelle Cumyn, présidente
*Comité d'éthique de la recherche*
Centre intégré universitaire de santé et de services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke

**Remerciements**

Nous remercions d'abord Monsieur Thibaud Ecarot, membre du comité d'éthique de la recherche du CIUSSS de l'Estrie – CHUS et chercheur postdoctoral au Groupe de recherche interdisciplinaire en informatique de la santé (GRIIS) de l'Université de Sherbrooke, pour ses judicieux conseils et son soutien dans la rédaction d'une notre première ébauche des présentes recommandations.

Nous tenons ensuite à remercier Madame Myriam Bourque, responsable de la sécurité de l'information et Madame Julie Nadeau, conseillère en gouvernance de la sécurité de l'information du CIUSSS de l'Estrie - CHUS pour leur collaboration dans la rédaction et la mise en œuvre des recommandations énoncées.

Nous remercions Monsieur Pierre-Martin Tardif, directeur de la sécurité de l'information au rectorat de l'Université de Sherbrooke pour sa collaboration dans la rédaction des présentes recommandations.

Nous remercions spécialement Madame Carole Coulombe, coordonnatrice à l'éthique de la recherche de l'Université de Sherbrooke, pour son soutien dans la traduction et l'adaptation des documents de Madame Chandra Kavanagh.

Nous remercions également Madame Stéphanie McMahon, directrice de la DCMU du CIUSSS de l'Estrie – CHUS ainsi que Madame Josée Maffett, directrice de section pour le SARIC, Madame Maryse Marois, anciennement conseillère en gestion de la recherche, et Monsieur Sébastien Brochu, du Service des bibliothèques et des archives, de l'Université de Sherbrooke, pour leur participation à notre groupe de travail.

# TABLE DES MATIÈRES

# MISE EN CONTEXTE

Dans un monde moderne où la grande majorité de nos données sont informatisées, nous devons sans cesse innover pour trouver un moyen de bien les protéger. Actuellement, nous traversons une période particulièrement à risque pour les données personnelles et ces dernières ont une valeur de plus en plus importante sur le marché. D'ailleurs, plusieurs brèches de sécurité de l'information se sont produites dans les dernières années.

Les données de santé ne sont pas à l'abri de ces risques. L'amélioration de la protection de nos données informatiques passe notamment par nos méthodes de conservation ainsi que le lieu de stockage. Dans les faits, il semblerait que 96% des données volées soient des données n'ayant pas été chiffrées[1], et donc, prêtes à l'utilisation.

Le CIUSSS de l'Estrie – CHUS et l'Université de Sherbrooke, en collaboration avec les comités d'éthique de la recherche concernés, veulent aider les chercheuses et chercheurs à acquérir de bons standards en matière de sécurité des données. À cet effet, le CIUSSS de l'Estrie – CHUS s'est doté d'une Politique de la sécurité de l'information.

Ce guide se veut pratique. Il été organisé pour vous permettre de consulter directement une section particulière (par exemple, sur les mots de passe robustes) en utilisant la **TABLE DES MATIÈRES** et en cliquant sur les termes en **VERT** pour obtenir nos conseils sur un sujet nommé.

Un **LEXIQUE** complet se trouve à la fin du document pour définir les différentes expressions utilisées. Cliquez sur les termes en **BLEU-VERT FONCÉ** pour consulter les définitions.

Ce document sera appelé à évoluer dans le temps et fera donc l'objet d'une révision annuelle.

[1] GEMALTO, *The Breach Level Index*, [En ligne] : <https://breachlevelindex.com> (site consulté le 9 septembre 2019).

# GESTION DES DONNÉES DE RECHERCHE – VOTRE RESPONSABILITÉ

Les données de recherche et les données provenant des dossiers médicaux (contenant des **RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ**) sont soumises à des règles strictes de confidentialité[2]. Même si, désormais, la plupart de ces données sont informatisées, il faut que les mesures de protection utilisées permettent d'en préserver la confidentialité tout au long du projet de recherche et même au-delà, lorsque le projet est terminé. Il en va de l'imputabilité de la chercheuse ou du chercheur principal.

Avant l'ère numérique, les chercheuses et chercheurs étaient tenus de conserver les originaux (documents papier, cassettes d'enregistrement, CD, etc.) dans un classeur verrouillé se situant dans un bureau fermé à clé. À la fin du projet de recherche, les documents à conserver étaient envoyés en archivage chez une compagnie spécialisée et les autres étaient détruits de manière à en assurer la confidentialité (par exemple, en les déchiquetant).

Toujours avant l'ère numérique, s'il fallait que les chercheurs ou chercheuses envoient un document à un collaborateur ou au promoteur, le document était envoyé sous scellé par courrier recommandé ou remis en mains propres.

Aujourd'hui, la technologie nous permet d'être plus efficaces en envoyant les informations rapidement par courriel. Elle nous permet également de sauver de l'espace et des coûts d'archivage en préservant de l'information directement dans nos systèmes informatiques. Cependant, il faut user de prudence et s'assurer que nos pratiques permettent de protéger adéquatement la confidentialité des données que nous détenons.

En ce sens, le CÉR du CIUSSS de l'Estrie – CHUS vous invite à élaborer dès le début de la planification de votre projet de recherche un **PLAN DE GESTION DES DONNÉES**.

## ÉVALUATION PROPORTIONNELLE AUX RISQUES

Il est entendu que certaines des recommandations énoncées dans le présent document soient, par moment, difficiles à respecter. Sachez que le CÉR fait une évaluation de chaque projet, au cas par cas, afin de s'assurer que les mesures de protection mises en place sont proportionnelles au risque (pour plus d'information concernant les niveaux de risque, voir la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**).

[2] Ces règles sont prévues notamment par le *Code civil du Québec* (RLRQ, c. CCQ-1991) et la *Loi sur les services de santé et des services sociaux* (RLRQ, c. S-4.1).

# LES ÉLÉMENTS À SURVEILLER EN MATIÈRE DE GESTION DES DONNÉES DE RECHERCHE

## PROPRIÉTÉS FONDAMENTALES EN INFORMATIQUE

En matière de sécurité de l'information, pour s'assurer d'atteindre un bon niveau de protection des données, il faut viser l'atteinte de trois objectifs fondamentaux : la disponibilité, l'intégrité et la confidentialité (aussi connus sous l'acronyme « DIC »).

- La **disponibilité** a pour but de s'assurer qu'une information, un système ou une donnée soit accessible en un temps défini.
- L'**intégrité** a pour but de s'assurer qu'une donnée reste exacte et non altérée à travers son cycle de vie, et ce, de façon volontaire ou accidentelle.
- La **confidentialité** a pour but de s'assurer qu'une information n'est accessible qu'aux personnes autorisées.

Ces trois propriétés sont mises en œuvre par un ensemble de moyens, dont le tableau suivant fournit quelques exemples :

| Moyen | Soutient la ou les propriétés suivantes | | |
|---|---|---|---|
| | Intégrité | Confidentialité | Disponibilité |
| **Chiffrement / cryptage** | X | X | |
| **Contrôle des accès** | X | X | X |
| **Hachage** | X | | |
| **Journalisation** | X | X | |
| **Redondance** | | | X |

# MOT DE PASSE ROBUSTE[3]

Des programmes malveillants sont conçus spécifiquement pour permettre aux attaquants d'essayer toutes les combinaisons possibles de caractères afin de trouver vos mots de passe. Il est donc impératif d'utiliser des mots de passe robustes pour protéger vos informations.

Généralement, il y a 3 critères* fondamentaux pour assurer la robustesse d'un mot de passe:

- La **longueur**
- La **complexité**
- L'**unicité**

*La **facilité de mémorisation** est aussi à prendre en compte.

➲ La **longueur** du mot de passe est le critère le plus important.

En voici quelques exemples :

- GoauclubmedBahamas
- JaimejouerauHockey
- Surf!MonNouveauSport

***Il est toujours plus sécuritaire de chercher à augmenter la longueur d'un mot de passe plutôt que de chercher à utiliser le plus grand nombre de caractères différents.***

➲ La **complexité** du mot de passe est également fondamentale. Si le système informatique ne permet pas le mot de passe à plusieurs caractères, nous recommandons d'utiliser un minimum de 8 caractères comprenant majuscules, minuscules, chiffres, caractères spéciaux). Le mot de passe est plus fort lorsqu'il mélange des caractères diversifiés.

En voici quelques exemples :

- Thaamccé! (Très hâte d'aller à mon chalet cet été!)
- Mes$2$Fils
- Quatre*4=16!

***La complexité en temps pour « casser » un mot de passe augmente de manière exponentielle avec la longueur du mot de passe et avec la variété des caractères utilisés.***

Les mots de passe ne doivent jamais être basés sur des renseignements personnels (prénom et nom, date de naissance, adresse, prénoms de ses enfants, etc.) ou toutes autres informations ayant un rapport direct avec la vie privée.

➲ L'**unicité** du mot de passe signifie qu'il est préférable d'utiliser un mot de passe unique pour chaque service (messagerie professionnelle, messagerie personnelle, réseaux sociaux, sites d'achat en ligne, etc.), afin d'éviter des dégâts en cascade. Par exemple, si un site Web est victime d'une brèche de sécurité et que des mots de passe sont divulgués, ils peuvent être utilisés pour tenter d'infiltrer d'autres sites ou systèmes informatiques.

***Idéalement, un nouveau mot de passe est créé pour chaque document ou service.***

[3] Inspiré d'un document disponible dans l'onglet « Sécurité de l'information » de la « Boîte à outils » accessible dans l'Intranet du CIUSSS de l'Estrie – CHUS : <https://intranet.ciusss-estrie-chus.reg05.rtss.qc.ca/index.php?id=311>.

## Testeurs de mot de passe

Pour vous aider, il existe de nombreux outils en ligne gratuits[4] pour tester la force relative des mots de passe. Ils peuvent produire des résultats légèrement différents, mais si vous en essayez plusieurs, vous aurez une bonne idée de la force du mot de passe que vous avez choisi.

## Gestionnaire de mots de passe

L'Université de Sherbrooke offre l'opportunité aux membres du personnel d'utiliser le gestionnaire de mots de passe **1Password**[5] sans frais. Cet outil sert à créer et conserver des mots de passe uniques différents pour chacun de ses comptes et à n'avoir que deux mots de passe à mémoriser : celui qui sert à accéder à 1Password et celui qui sert à se connecter à votre compte de messagerie/ordinateur de l'UdeS. Cet outil peut également être utilisé pour partager des mots de passe à des collaborateurs de manière sécuritaire.

# ÉQUIPEMENT INFORMATIQUE

**Dans un monde idéal, chaque personne impliquée dans un projet de recherche et devant travailler sur des DONNÉES BRUTES, soit pour les entrer dans une base de données, soit pour les analyser, serait en mesure d'utiliser de l'équipement informatique institutionnel par le biais du réseau Internet institutionnel; c'est-à-dire, en étant sur place, dans une installation du CIUSSS de l'Estrie – CHUS ou un bureau de l'Université de Sherbrooke.**

## ÉQUIPEMENT INFORMATIQUE PERSONNEL

### En pratique

Sachez que les équipements informatiques **personnels** (par exemple, un ordinateur portable) représentent des vecteurs importants d'attaques ou de propagation de virus informatiques. C'est pourquoi les ordinateurs professionnels (équipement informatique institutionnel) sont à privilégier. Dans tous les cas, assurez-vous que :

- Votre appareil – ainsi que tout appareil branché à votre réseau internet personnel – possède une solution antivirale, que celle-ci est à jour et qu'une analyse complète (scan) est faite périodiquement;
- Le système d'exploitation (ex. Windows) est à jour et que les mises à jour s'effectuent adéquatement)[6];
- Le **RÉSEAU SANS FIL**, le cas échéant, est sécuritaire.

Si vous devez exceptionnellement utiliser de l'équipement informatique personnel, nous vous suggérons aussi de vous assurer que le disque dur est chiffré. Pour des détails supplémentaires, consulter la

[4] Par exemple, nous vous proposons <https://password.kaspersky.com/fr/> ou <howsecureismypassword.net>.
[5] Pour plus d'information, veuillez consulter la page suivante : <https://www.usherbrooke.ca/services-informatiques/repertoire/acces/1password/> (consulté le 2020-11-23).
[6] Nous vous déconseillons **fortement** d'utiliser un ordinateur possédant un système d'exploitation avec une version Windows 7 ou antérieure, car ces versions ne sont plus supportées par Microsoft et n'offrent donc plus de protection.

section **CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE**. Vous pouvez consulter le STI si vous êtes affiliés à l'Université de Sherbrooke.

## Détails supplémentaires – mesures proportionnelles au risque

L'un des moyens les plus courants de collecte et de stockage de données consiste à utiliser un ordinateur portable protégé par mot de passe. Bien que cette méthode puisse être suffisamment sécurisée pour les données à **FAIBLE RISQUE**, ce n'est pas suffisant pour les données à risque **MOYEN risque** ou **HAUT risque**. Ainsi, des mesures supplémentaires doivent être prises pour protéger les données, notamment en chiffrant le disque dur sur lequel les données sont hébergées et en conservant l'équipement informatique dans un bureau fermé à clé.

Dans certains cas, le stockage de données sur un **PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF** est une bonne option pour ajouter un niveau de protection. Certains périphériques, comme les clés USB, ne sont pas connectés à Internet et, en tant que tels, sont moins sujets à un accès à distance sans autorisation. Cependant, ces petits appareils peuvent être plus facilement perdus ou volés. Pour plus d'information concernant ces appareils, veuillez consulter la section **PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF**.

Même si vous collectez des données à **FAIBLE RISQUE**, il existe des moyens de sécuriser le stockage sur un ordinateur protégé par mot de passe. Par exemple, chiffrer le disque dur, utiliser régulièrement des logiciels anti-virus et anti-malware, mettre à jour votre ordinateur dès que les mises à jour sont disponibles. Aussi, évitez les situations courantes où votre ordinateur pourrait être volé comme le laisser dans la voiture ou un lieu public sans surveillance. Le plus important est de sauvegarder régulièrement et de sécuriser vos données.

## CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE

**Le CHIFFREMENT est une méthode d'encodage de vos DONNÉES afin que seul vous, ou quelqu'un que vous autorisez, puissiez y accéder. L'ÉPTC 2 (2018) stipule ce qui suit : « En règle générale, les [RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES obtenus] dans le cadre de la recherche qui sont [conservés] sur un ordinateur branché à Internet doivent être [chiffrés]. »[7] Différentes méthodes de chiffrement des données existent, incluant le chiffrement de fichiers numériques individuels ou le chiffrement d'un appareil complet (par ex. un disque dur).**

***ATTENTION :*** Pour que le chiffrement soit efficace, il faut utiliser un **MOT DE PASSE ROBUSTE** et le conserver en un lieu sûr. Il est important que le lieu sûr soit un dossier différent de celui qui contient les fichiers de renseignements sensibles.

À mesure que la technologie avance, les normes et recommandations applicables en matière de chiffrement minimalement sécuritaire sont appelées à évoluer. Plusieurs références sur le sujet sont disponibles, notamment les recommandations du Centre canadien pour la cybersécurité du Gouvernement du Canada[8] pour les informations confidentielles.

Pour des conseils précis à ce sujet, veuillez vous référer aux ressources disponibles dans l'intranet du CIUSSS de l'Estrie – CHUS ou communiquez avec le STI de l'Université de Sherbrooke.

[7] ÉPTC 2 (2018), p. 71, Application de l'article 5.3.
[8] CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, Programme de validation des modules cryptographiques (PVMC), Gouvernement du Canada, [En ligne] : <https://cyber.gc.ca/fr/programme-de-validation-des-modules-cryptographiques-pvmc> (site consulté le 6 mai 2020). Voir l'onglet « Pour les acheteurs ».

## Avantages et inconvénients des différentes méthodes de chiffrement

### Chiffrement de fichiers numériques individuels

**Avantages :** Le **CHIFFREMENT** de certains fichiers seulement, tels que ceux liés à votre projet de recherche ou contenant des **RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES**, protège vos **DONNÉES** sans aucune complication supplémentaire.

**Inconvénients :** Si quelqu'un a accès à l'ordinateur sur lequel vos données sont stockées, il peut y pénétrer et afficher facilement tous les fichiers non chiffrés. Vous devez également vous souvenir de chiffrer chaque nouveau fichier que vous créez.

### Chiffrement de votre disque dur

**Avantages :** Le **CHIFFREMENT** de l'intégralité de votre disque dur le protège contre quiconque qui tente d'accéder à vos **DONNÉES** sans votre autorisation (en cas de vol, par exemple). Le chiffrement de l'ensemble de votre appareil est également plus pratique et moins sujet à l'erreur, car tous les fichiers sont automatiquement chiffrés.

**Inconvénients :** Si vous rencontrez un problème de corruption sur votre disque dur, il peut être plus difficile, voire impossible, de récupérer les données. Le chiffrement protège le disque dur lors de l'ouverture de l'ordinateur, par contre si un ordinateur portable est laissé ouvert et sans surveillance, l'option du chiffrement du disque dur est inutile, à moins d'avoir chiffré les fichiers également.

### Méthodes à essayer

Pour chiffrer l'intégralité de votre disque dur, ou vos fichiers individuels, essayer :

- *Bitlocker* : Il s'agit d'un système de sécurité intégré à Windows (10), qui permet de chiffrer les données stockées sur votre ordinateur, ce qui permet d'assurer la confidentialité de vos données. Ce logiciel se trouve de base dans les ordinateurs portables récents.
- *VeraCrypt* (Windows, Linux ou OS);
- *GNU Privacy Guard* (Windows, Linux ou OS)
- *FileVault* (OS).

Il peut être intéressant aussi d'acheter un disque dur externe et de procéder à son chiffrement lors de la configuration, en le protégeant par un **MOT DE PASSE ROBUSTE**.

Pour chiffrer et compresser des fichiers que vous souhaitez envoyer par Internet, essayez *7-Zip*.

***ATTENTION :*** Lorsque les **DONNÉES** nécessitent un **CHIFFREMENT**, il peut être facile de commettre l'erreur de chiffrer certaines copies, mais pas d'autres. Assurez-vous de chiffrer toutes les copies, incluant les sauvegardes (backups) et les données stockées sur des **PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF** tels que les téléphones cellulaires.

## TYPE DE CONNEXION À INTERNET

En ce qui concerne la connexion à Internet, il existe plusieurs possibilités : les ordinateurs qui se connectent à un réseau sans fil (Wi-Fi), les ordinateurs qui se connectent via des réseaux filaires et les ordinateurs sans aucune connexion à l'Internet (plus rares). Ces trois types de connexion représentent

également trois niveaux différents de sécurité des **DONNÉES**. Enfin, l'utilisation d'un ordinateur qui n'est pas connecté à l'Internet est le moyen le plus sécuritaire pour stocker des données de recherche.

***ATTENTION :*** Il existe des risques même si vous utilisez un ordinateur sans connexion à Internet, par exemple si vous y branchez un média amovible sur lequel se trouve un virus.

## Accès au réseau filaire

### CIUSSS de l'Estrie – CHUS

Seul l'équipement informatique institutionnel, celui fourni par l'organisation, peut accéder à Internet via le réseau filaire de l'établissement.

### Université de Sherbrooke

« L'Université dispose d'une infrastructure réseau qui permet l'accès au réseau IntraRISQ pour offrir une connexion Internet à large bande aux membres de sa communauté. [...] L'accès à l'Internet par le réseau IntraRISQ est disponible sur tous les campus à partir d'un ordinateur branché au réseau filaire ou un appareil mobile connecté aux réseaux sans fil *aerius* ou *aeriusSecurise*.»[9]

## Accès au réseau sans fil

### CIUSSS de l'Estrie - CHUS

Dans l'Intranet du CIUSSS de l'Estrie – CHUS, vous trouverez un document[10] expliquant comment vous connecter au réseau sans fil « CIUSSSE - CHUS ».

### Université de Sherbrooke

« L'Université [de Sherbrooke] dispose d'une infrastructure de réseaux sans fil qui rend accessibles les communications entre les différents systèmes informatiques. Six réseaux sans fil sont disponibles sur les campus. L'accès à ceux-ci est permis selon votre statut et votre emplacement à l'Université. » Pour des détails sur les noms des réseaux ainsi que leur procédure d'accès, veuillez consulter la page web des services informatiques[11] de l'Université.

### Travail à domicile

Si vous devez exceptionnellement travailler ailleurs que dans les locaux du CIUSSS de l'Estrie – CHUS ou de l'Université de Sherbrooke, assurez-vous de la sécurité de votre réseau sans fil:

- Protocole de sécurité WPA2/WPA3 et de **CHIFFREMENT** AES;
- **MOT DE PASSE ROBUSTE** pour accéder à la configuration du routeur;
- **MOT DE PASSE ROBUSTE** pour accéder au réseau Wi-Fi.

---

[9] <https://www.usherbrooke.ca/services-informatiques/repertoire/reseaux/reseau-internet/> (site consulté le 6 août 2020)

[10] Si vous êtes connectés à un réseau du CIUSSS de l'Estrie - CHUS, vous pouvez cliquer sur l'hyperlien suivant ou le copier dans votre navigateur Internet : <https://intranet.ciusss-estrie-chus.reg05.rtss.qc.ca/clients/CIUSSSE-CHUS/02_Boite_a_outils/Informatique/ProcedureConnection_Reseau_sans_fil.pdf>.

[11] Vous pouvez cliquer sur l'hyperlien suivant ou le copier dans votre navigateur Internet : <https://www.usherbrooke.ca/services-informatiques/repertoire/reseaux/reseau-sans-fil/>.

***ATTENTION :*** Nous déconseillons d'utiliser une connexion Internet publique gratuite (réseau Wi-Fi public), car les données échangées peuvent être utilisées à des fins malveillantes. Utilisez plutôt votre réseau cellulaire lorsque vous vous trouvez dans un lieu public.

D'autres approches pour faciliter le télétravail ont été développées par le CIUSSS de l'Estrie – CHUS (jetons d'accès) et par l'Université de Sherbrooke (accès par réseau privé virtuel).

# CONSERVATION DES DONNÉES

## DURÉE DE CONSERVATION DES DONNÉES

Il est généralement recommandé de conserver les **DONNÉES** de recherche lorsque l'analyse est terminée et ce, même, à la suite de la publication des résultats, selon les règles actuellement en vigueur[12]. À titre d'exemple, les IRSC demandent de « conserver les ensembles de données originaux pendant au moins cinq ans après la fin de la période de validité de la subvention (ou plus si d'autres politiques s'appliquent). »[13]

***ATTENTION :*** Les données étant conservées durant plusieurs années, il est important de retirer les accès aux données lorsqu'un membre du personnel de recherche quitte l'équipe.

### Quelques pistes de réflexion

La durée de conservation dépend du type de données que vous avez recueilli. Voici quelques éléments qu'il peut être opportun de regarder :

1. Il revient à la chercheuse ou au chercheur responsable de trouver un **équilibre entre les risques et les avantages** de la conservation ou de la suppression des données de recherche, en accordant une attention particulière de leur caractère **PERSONNELS OU IDENTIFICATOIRES** ou au niveau de risque associé. Pour plus d'information sur le niveau de risque, consultez la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**.

2. Il faut un **plan** pour gérer les données en toute sécurité sur une base continue, et ce, au-delà du projet de recherche. Demandez-vous quel est votre **PLAN DE GESTION DES DONNÉES** (PGD) si vous deviez quitter votre institution, votre domaine ou votre carrière.

3. Éventuellement, vous devrez **SUPPRIMER** vos données. Si vous avez de bonnes raisons de **conserver vos données** et un **PGD** robuste qui décrit vos plans pour la façon dont vous gérerez les données à l'avenir, il est possible, quoique rare, de les conserver indéfiniment. Cependant, cette possibilité sera à discuter avec le CÉR et devra prendre en compte le consentement obtenu.

4. La **durée de conservation** est variable selon le pays dans lequel vous vous trouvez. L'ÉPTC 2 (2018) au Canada[14] et la *Data Protection Act 2018* du Royaume-Uni[15] ne fixent aucune période

---

[12] Les normes en matière de durée de conservation sont appelées à évoluer dans le temps. Les CÉR de l'Université de Sherbrooke suggèrent de prévoir une durée de sept (7) ans puisque certains éditeurs de revues scientifiques exigent que les auteurs permettent un accès aux données brutes durant tout le processus de publication et, parfois, exigent également de les conserver cinq (5) après la publication de l'article. Aussi, actuellement, Santé Canada exige que les données obtenues dans le cadre d'essais cliniques soient conservées pour une durée de 25 à 30 ans.

[13] GOUVERNEMENT DU CANADA, *Politique des trois organismes sur le libre accès aux publications*, [En ligne] : <http://www.science.gc.ca/eic/site/063.nsf/fra/h_F6765465.html?OpenDocument> (site consulté le 29 novembre 2019).

[14] CONSEIL DE RECHERCHES EN SCIENCES HUMAINES, CONSEIL DE RECHERCHE EN SCIENCES NATURELLES ET EN GÉNIE DU CANADA ET INSTITUTS DE RECHERCHE EN SANTÉ DU CANADA, *Énoncé de politique des trois conseils: Éthique de la recherche avec des êtres humains*, décembre 2018 (ci-après, « ÉPTC 2 (2018) »), p. 69 à 71, article 5.3.

minimale ou maximale précise pour la conservation des données personnelles Cependant, le *Office for Human Research Protections* des États-Unis exige que les dossiers de recherche généralement détenus par les chercheuses et chercheurs tels que les formulaires de consentement ou les transcriptions d'entrevues **ANONYMISÉS** soient conservés pendant au moins trois (3) ans après la fin de la recherche[16].

5. Dans les cas où la recherche est soutenue par un **contrat** ou une subvention universitaire qui comprend des dispositions spécifiques concernant la conservation des données notamment, les dispositions de cet accord prévaudront.

## Destruction des données

Lorsque les données ont atteint la fin de leur vie utile, il est temps de les **SUPPRIMER**.

***ATTENTION :*** Il s'agit d'une étape **importante** qui ne doit pas être oubliée. Il faut porter une attention particulière à la date prévue de fin de conservation qui se trouve dans la lettre d'autorisation de la DSP, le cas échéant, ou dans les formulaires d'information et de consentement présentés aux personnes participantes.

Les plus hauts standards en matière de sécurité de l'information recommandent, pour des données très sensibles (**HAUT RISQUE**), de détruire physiquement le disque (à la masse, par exemple) et, ensuite, de le brûler afin d'être assurés d'une destruction complète.

### Données à haut risque

- Si le contenu du disque dur doit être supprimé et réutilisé par vous-même :

  Il est possible d'utiliser un logiciel tel que CCleaner qui supprime les données du disque dur.

- Si le contenu du disque dur doit être supprimé et réutilisé par un tiers :

  La solution est de le chiffrer avec un outil tel que cité précédemment (voir **CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE**) et d'utiliser la méthode *crypto-erase*. Ainsi personne ne pourra récupérer les données. Celle-ci varie cependant selon le modèle du disque dur et peut s'avérer difficile à effectuer.

### Données à faible risque

- Si le contenu du disque dur doit être supprimé et réutilisé par vous-même ou par un tiers :

  Il est possible d'utiliser un logiciel tel que *CCleaner* qui supprime les données du disque dur.

---

[15] UK Public General Acts, 2018 c. 12, article 39, [En ligne] : <http://www.legislation.gov.uk/ukpga/2018/12/part/3/enacted> (site consulté le 6 mai 2020).

[16] OFFICE FOR HUMAN RESEARCH PROTECTIONS, "What records should investigators keep, and for how long?" dans *Investigator Responisibilities FAQs*, U.S. Department of Health & Human Services, [En ligne] : <https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/investigator-responsibilities/index.html> (site consulté le 6 mai 2020). Voir également CFR-45, article 46.115 b) qui prévoit que le CÉR (IRB en anglais) doit conserver les documents relatifs à une étude pour une durée de trois (3) ans.

## SERVICES INFONUAGIQUES (CLOUD)

Les **SERVICES INFONUAGIQUES** permettent de stocker et partager des **DONNÉES** en les conservant sur des serveurs distants accessibles depuis Internet. Le service infonuagique approuvé par le CIUSSS de l'Estrie - CHUS et l'Université de Sherbrooke est le *OneDrive* (ou *SharePoint*) associé à votre adresse courriel attribuée par l'institution concernée. Les renseignements devraient être **ANONYMISÉS** ou **CODÉS** et les fichiers devraient être **CHIFFRÉS**, comme ceux envoyés par courriel, avant d'être transférés sur *OneDrive*. Pour plus de détails, **consultez la section CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE.**

Même si les services *OneDrive* (ou *SharePoint*) institutionnels offrent plus de sécurité que les services publics comme *GoogleDrive* ou *iCloud*, ils ne sont pas complètement sécuritaires[17]. **Les fichiers contenant des données à MOYEN risque et HAUT RISQUE devraient donc être protégés par un MOT DE PASSE ROBUSTE avant de se trouver sur des services infonuagiques.**

La possibilité d'utiliser les services infonuagiques dépend du niveau de risque associé à vos données. Pour en connaître davantage sur les différents niveaux de risque, nous vous invitons à consulter la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**.

***ATTENTION :*** L'utilisation de **SERVICES INFONUAGIQUES** publics tels que *Google Drive* ou *One Drive* associé à un compte Google ou Microsoft personnel est **à proscrire**.

***ATTENTION :*** Pour les étudiantes et étudiants, les données devraient être conservées ailleurs que dans le *OneDrive* (ou *SharePoint*) associé à leur adresse courriel USherbrooke, car le service n'est plus accessible à la fin des études. Il est de la responsabilité du professeur ou de la professeure qui dirige l'étudiant de veiller à la conservation des données par la suite.

***ATTENTION :*** À l'accès aux services tel que le *OneDrive* institutionnel sur les cellulaires intelligents par le biais des applications mobiles qui ne seraient pas protégées par un **MOT DE PASSE ROBUSTE**.

## PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF

Le niveau de sécurité associé à un **PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF** dépend de la possibilité ou non de connecter le périphérique à Internet, pensons notamment aux téléphones cellulaires intelligents et tablettes électroniques (oui) ou aux clés USB et disque durs externes (non).

Les médias amovibles, comme les clés USB, sont pratiques et faciles à utiliser. Ils s'échangent d'un appareil à l'autre et peuvent contenir une quantité impressionnante de données. Entre les mains d'une personne mal intentionnée, par contre, ils peuvent poser de grands risques.

### Avantages et inconvénients de l'utilisation de périphériques portatifs

#### Périphérique de sauvegarde portatif connecté à Internet

**Avantages :** La collecte de **DONNÉES** sur un périphérique de sauvegarde portatif connecté à Internet tel qu'un téléphone cellulaire ou une tablette électronique peut être un bon choix, car la technologie est disponible en tout temps, familière, pratique. Elle est également rapide, précise et portable. Son utilisation requiert peu d'énergie et représente un coût relativement faible pour l'équipe de recherche.

[17] En fait, le service infonuagique du RSSS (associé à l'adresse @ssss.gouv.qc.ca) assure un niveau de sécurité acceptable pour le partage des fichiers seulement entre les adresses du RSSS. Autrement, il est préférable de procéder par courriel chiffré et pièces jointes protégées par mot de passe.

**Inconvénients :** Lorsque les données sont stockées sur un périphérique de sauvegarde portatif, elles peuvent potentiellement être volées ou mal utilisées. Il en va de même lors du **TRANSFERT DE DONNÉES**. Cependant, le **CHIFFREMENT** au niveau de l'appareil et pendant la transmission peut considérablement atténuer ces risques[18]. Pour plus de détails sur les méthodes de chiffrement, consultez la section **CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE**.

### Périphérique de sauvegarde portatif non connecté à Internet

**Avantages** : Un périphérique de sauvegarde portatif non connecté n'a pas les mêmes vulnérabilités que les périphériques connectés, mais offre tout de même des options de stockage et de transfert des données.

**Inconvénients** : Considérant qu'il n'est pas connecté à l'Internet, le transfert des données à partir de ce type de périphérique peut être moins pratique. En outre, certains périphériques sont facilement corruptibles et ne sont pas conçus pour le stockage long terme comme, par exemple, les lecteurs flash peu coûteux. Si une clé USB a déjà transigé par un poste informatique connecté à internet, celle-ci peut contenir des virus ou vulnérabilités.

## Conseils pour une utilisation sécuritaire des médias amovibles (clés USB)

La clé USB est discrète et fait partie du quotidien. Elle est cependant à l'origine de la majorité des incidents liés à la fuite d'informations sensibles ou à l'infection des systèmes informatiques de par l'introduction de logiciels malveillants.

1. Éviter de copier des informations confidentielles sur les médias amovibles;
2. Si, malgré tout, des informations confidentielles doivent y être stockées :
    - Chiffrer les documents avec un **MOT DE PASSE ROBUSTE**;
    - Utiliser une clé USB chiffrée (soit une clé USB pour laquelle un mot de passe est requis afin d'accéder au contenu);
3. Supprimer les données des médias amovibles aussitôt qu'elles ne sont plus requises, surtout pour les médias non chiffrés.

# TRANSFERT DE DONNÉES

## PARTAGE DE DONNÉES AVEC LES COCHERCHEUSES ET COCHERCHEURS

Avant de partager des **DONNÉES** collectées auprès de personnes participantes de quelque manière que ce soit, il est essentiel de rendre ces données aussi peu risquées que possible, par exemple en les codant ou en les rendant anonymisées. L'idéal serait que les personnes responsables de la recherche suppriment toutes les informations personnelles permettant d'identifier les personnes participantes avant que les données ne soient partagées avec les partenaires de recherche d'autres institutions, en particulier ceux des États-Unis, car ils sont soumis à la loi américaine *Patriot Act/Domestic Security Enhancement Act* qui ne traite pas les **RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES** de la même manière qu'ici.

[18] TRUCANO, Michael. "Using mobile phones in data collection: Opportunities, issues and challenges." Edutech. April 18, 2014. Accessed August 28, 2017, en ligne : <http://blogs.worldbank.org/edutech/using-mobile-phones-data-collection-opportunities-issues-and-challenges> [Anglais seulement]

Choisissez une méthode de communication de vos données qui soit conforme à son niveau de risque (**FAIBLE RISQUE**, **MOYEN RISQUE** ou **HAUT RISQUE**). Pour en savoir plus sur le niveau de risque de vos données, consultez la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**.

Pour les fichiers protégés par mots de passe, nous vous suggérons d'utiliser un **GESTIONNAIRE DE MOTS DE PASSE** pour les échanger avec vos cochercheuses et cochercheurs.

### Données à faible risque

Ces données peuvent être partagées en utilisant votre adresse courriel institutionnelle, soit le service Office365 offert par le CIUSSS de l'Estrie – CHUS ou l'Université de Sherbrooke, et tous les **SERVICES INFONUAGIQUES (CLOUD)** associés.

### Données à risque moyen

Les documents qui contiennent des données à risque moyen devraient se trouver dans des fichiers **CHIFFRÉS** (pour des détails concernant la procédure, référez-vous à la section **CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE** du présent document) et protégés par un **MOT DE PASSE ROBUSTE**. Une fois protégés, les fichiers peuvent être partagés qu'en ayant recours au service de courrier électronique du CIUSSS de l'Estrie – CHUS ou de l'Université de Sherbrooke et les services infonuagiques associés. En fait, le service infonuagique du RSSS (associé à l'adresse @ssss.gouv.qc.ca) assure un niveau de sécurité acceptable pour le partage des fichiers seulement entre les adresses du RSSS. Autrement, il est préférable de procéder par courriel chiffré et pièces jointes protégées par mot de passe.

### Données à haut risque

Ces données à accès restreint doivent faire l'objet d'une grande vigilance. Elles pourraient être partagées de main à main sur un dispositif de stockage de données chiffré et protégé par un mot de passe. Les fichiers chiffrés et protégés par un mot de passe pourraient être partagés par le biais des services infonuagiques approuvés par les responsables de la sécurité informationnelle. Le CÉR devra prendre connaissance et approuver les mesures proposées. Un transfert de données à haut risque entre les institutions peut nécessiter des stratégies individualisées, notamment la signature d'entente de transfert de données (DTA). Contactez le CÉR/BAPR pour plus d'informations.

# PLATEFORMES ET LOGICIELS INFORMATIQUES

## SONDAGES EN LIGNE

Les données doivent être hébergées au Canada et colligées avec un outil professionnel sécurisé qui respecte un haut niveau de conformité et pour lequel des ententes de confidentialité et de sécurité sont signées avec le fournisseur.

Il est fortement déconseillé d'utiliser les outils de sondages publics et surtout les versions gratuites ou non-institutionnelles (par exemple, SurveyMonkey, GoogleForms) qui comportent des risques de sécurité pouvant notamment causer des violations de la confidentialité. Même si vous ne prévoyez pas collecter de données sensibles, il est possible que les gens fournissent des réponses qui le sont. Aussi, ces outils peuvent utiliser les adresses courriel pour les distribuer à des tiers faisant en sorte que les gens reçoivent des polluriels par la suite.

Si vous désirez procéder à un sondage en ligne, les services informatiques de nos établissements offrent certaines plateformes, par exemple :

- L'Université de Sherbrooke et le CIUSSS de l'Estrie - CHUS offre *Microsoft Forms* qui vient avec la suite Office365;
- *LimeSurvey* est aussi disponible pour les chercheurs de l'Université de Sherbrooke (mais la FMSS n'offre plus de soutien dédié exclusivement à ce logiciel);
- Le logiciel *RedCap*;
- Le logiciel *Simple Sondage* est utilisé par le CIUSSS de l'Estrie – CHUS;
- Autres stratégies proposées par l'Université de Sherbrooke.

## VIDÉOCONFÉRENCE

Pour assurer la confidentialité des échanges pendant l'entrevue, nous recommandons d'utiliser des logiciels qui offrent des mesures de protection adéquates, surtout si les sujets discutés sont sensibles (voir la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**).

Pour les rencontres d'équipe ou les entrevues qui ont lieu par support audiovisuel, il est recommandé d'utiliser les logiciels tels que *Zoom* et *Teams* en prenant soin de sélectionner les versions institutionnelles et en appliquant toutes les précautions habituelles. L'accès à *Teams* est fourni par l'Université de Sherbrooke et par le CIUSSS de l'Estrie – CHUS par le biais de l'adresse courriel (compte Office365).

Les membres du corps professoral de l'Université de Sherbrooke ont également accès à la plateforme *Adobe Connect.*

Des documents de référence sont disponibles sur le site web de l'Université de Sherbrooke et dans l'Intranet du CIUSSS de l'Estrie – CHUS (accessible à l'interne seulement ou par le biais d'un jeton). Pour les liens complets, aller à la section **RÉFÉRENCES**.

# LEXIQUE[19]

Tout au long du présent document, nous utilisons certains termes spécifiques à la gestion des données et au domaine de la sécurité de l'information. En voici les définitions :

- **Chiffrement :** « Il s'agit d'une opération par laquelle un texte clair est substitué par un texte inintelligible et inexploitable pour quiconque ne possède la clé (une sorte de code) permettant de le ramener à sa forme initiale. »[20] Autrement dit, le contenu chiffré est un contenu converti de texte brut lisible à un texte brouillé chiffré; seul le destinataire peut le lire. Le mot « **chiffrement** » et souvent confondu avec « **cryptage** » qui correspond à la science du chiffrement. Pour des conseils à ce sujet, voir la section « **CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE** ».

- **Couplage de données[21] :** Fusion ou analyse de deux ou plusieurs ensembles de données (p. ex. renseignements sur la santé et renseignements sur la formation académique des mêmes personnes) à des fins de recherche. Voir également l'expression « **ENSEMBLE DE DONNÉES** ».

- **Cryptage** : Voir « **CHIFFREMENT** ».

- **Cycle de vie des données[22] :** Le **: CYCLE DE VIE** des données fait référence à toutes les étapes de l'existence des données, de leur collecte à leur destruction. Une vue globale du cycle de vie est utile pour permettre une gestion active des données dans le temps, en préservant ainsi la sécurité de l'information.

- **Données :** Dans le présent document, le terme « données » réfère, entre autres, aux données cliniques issues du dossier médical des usagers, aux données administratives du CIUSSS de l'Estrie – CHUS, aux données issues d'une recherche documentaire, aux résultats d'analyses faites à partir d'un échantillon biologique ainsi qu'aux données collectées directement auprès des personnes participantes dans le cadre d'un projet de recherche (par exemple, lors d'une entrevue). Pour des détails sur les types de renseignements, voir « **RENSEIGNEMENTS (TYPES DE)** ».

- **Données à faible risque :** Les données à faible risque nécessitent des contrôles contre les modifications non autorisées dans un souci de préservation de l'intégrité des données plutôt que pour prévenir les risques pour les chercheurs, les membres de l'équipe de recherche ou les personnes participantes. Des données à faible risque, pour lesquelles aucune ou peu de restriction est nécessaire, sont, par exemple, des renseignements **ANONYMES** ou **ANONYMISÉS**, des formulaires de consentement et des fiches d'information vierges (p. ex. questionnaires ou grille d'évaluation), et des renseignements recueillis sur un site web auquel le public a librement accès sur Internet. Voir la « **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE** » pour obtenir des conseils sur la gestion de ces données.

---

[19] Inspiré du document *Research Data Management Glossary* développé par le *Ethical Digital Data Management Working Group*, traduit et adapté avec la permission de Chandra Kavanagh. Nous vous invitons également à consulter le *Research Data Management Glossary* de la CASRAI (disponible en anglais seulement).

[20] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Chiffrement » dans *Terminologie en sécurité informatique*, Gouvernement du Québec, m.à.j. février 2013, [En ligne] : <https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/chiffrement.html> (site consulté le 29 nov. 2019).

[21] Tel que défini dans le « Glossaire » de CONSEIL DE RECHERCHES EN SCIENCES HUMAINES, CONSEIL DE RECHERCHE EN SCIENCES NATURELLES ET EN GÉNIE DU CANADA ET INSTITUTS DE RECHERCHE EN SANTÉ DU CANADA, *Énoncé de politique des trois conseils: Éthique de la recherche avec des êtres humains*, décembre 2018 (ci-après, « ÉPTC 2 (2018) »), p. 217.

[22] Voir également la définition se trouvant sur le site de l'OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, En ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8354209> (consulté le 2020-10-09).

- **Données à haut risque :** Les données à haut risque nécessitent des contrôles très rigoureux contre la divulgation, la perte et la modification non autorisées. La divulgation, perte ou modification non autorisée de ces renseignements peut entraîner un risque important pour la personne participante, le chercheur et les membres de l'équipe de recherche, notamment des atteintes à la réputation, une perturbation importante sur les plans professionnel et personnel, des conséquences financières ou, encore, une responsabilité juridique. Les données à haut risque, nécessitant des contrôles rigoureux, comprennent, par exemple, l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou autres croyances similaires, l'appartenance à un syndicat, l'état de santé physique ou mentale, la vie sexuelle, la commission présumée ou avérée d'une infraction (casier judiciaire). Voir la « **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE** » pour obtenir des conseils sur la gestion de ces données.

- **Données à moyen risque :** Les données à moyen risque nécessitent des contrôles rigoureux contre toute divulgation, perte ou modification non autorisée. La divulgation, perte ou modification de ces renseignements confidentiels peut entraîner des risques pour la personne participante. Ces renseignements confidentiels incluent notamment des enregistrements audio ou vidéo selon la nature du contenu, le fichier contenant la clé du code ou des formulaires d'information et de consentement signés. Voir la « **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE** » pour obtenir des conseils sur la gestion de ces données.

- **Données brutes :** « Ensemble de données présentées sous la forme où elles ont été collectées, avant d'avoir subi un quelconque traitement ou une interprétation. »[23] Bien que ces données aient le potentiel de devenir intéressantes, elles nécessitent une extraction sélective, un nettoyage, une organisation et, parfois, une analyse ainsi qu'un formatage à des fins d'utilisation. Les données brutes sont des renseignements qui n'ont pas encore été **ANONYMISÉS**. À cette étape du **CYCLE DE VIE DES DONNÉES**, vos données contiennent encore des **RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES**.

- **Données non-identificatoires :** Ces données ne peuvent pas conduire à l'identification d'une personne en particulier, à distinguer une personne d'une autre ou à des **RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES**. Il peut s'agir de renseignements **ANONYMISÉS** ou de renseignements **ANONYMES** qui n'ont jamais pu conduire à l'identification d'une personne en particulier. Néanmoins, il faut demeurer vigilants, car certains renseignements non-identificatoires, lorsque **COUPLÉS** avec un autre **ENSEMBLE DE DONNÉES**, peuvent devenir identificatoires.

- **Ensemble de données[24] :** Collection de renseignements servant à la recherche, y compris du matériel biologique humain.

- **Gestion des données de recherche (GDR)** : « [L]'ensemble des processus appliqués tout au long du cycle de vie d'un projet de recherche pour guider la collecte, la documentation, le stockage, le partage et la préservation des données de recherche. »[25] Les processus incluent l'organisation active et la maintenance des données tout au long de leur **CYCLE DE VIE des données**. La saine gestion des données de recherche permet d'augmenter l'efficience et la possibilité de réutilisation des données.

- **Hachage[26] :** Il s'agit d'une opération qui consiste à appliquer une fonction mathématique permettant de créer l'empreinte numérique d'un message, en transformant un message de taille

[23] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Fiche terminologique : données brutes », *dans Le grand dictionnaire terminologique (GDT),* Gouvernement du Québec, En ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26521863.
[24] Tel que défini dans le « Glossaire » de l'ÉPTC 2 (2018), p. 218.
[25] PORTAGE, *Introduction à la gestion des données de recherche*, août 2019, [En ligne] : <https://portagenetwork.ca/wp-content/uploads/2019/08/Introduction_GDR_Aout2019_FR.pdf> (site consulté le 30 avril 2020).
[26] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Chiffrement » dans *Terminologie en sécurité informatique*, Gouvernement du Québec, m.à.j. février 2013, [En ligne] :

variable en un code de taille fixe, en vue de son authentification ou de son stockage. Cette opération est notamment utilisée pour la signature électronique ou numérique d'un document.

- **Journalisation[27] :** Il s'agit de l'enregistrement, dans un journal, des opérations informatiques effectuées dans un système (lecture, saisie, modification, suppression, etc.). Cet enregistrement permet de garder une trace de certains événements en vue de vérifications ultérieures.

- **Logiciel de SONDAGES EN LIGNE** : Outil en ligne qui permet de créer des questionnaires auxquels les personnes participantes peuvent répondre directement par le biais d'Internet. Ces outils sont généralement des formulaires web accompagnés d'une base de données contenant les réponses transmises. Ces outils peuvent inclure un logiciel statistique fournissant des analyses.

- **Métadonnées[28]** : « Donnée qui renseigne sur la nature de certaines autres données dans le but d'en faciliter la compréhension et la gestion. […] Le nom d'un fichier, sa taille, sa date de création ou de modification sont des exemples de métadonnées. »[29] D'autres exemples de métadonnées sont :

    - Les métadonnées **techniques** qui incluent les noms de table et de colonne de base de données physiques, les propriétés de colonne et les propriétés d'autres objets de base de données, y compris la façon dont les données sont stockées.

    - Les métadonnées de **processus** qui sont des données qui définissent et décrivent les caractéristiques d'autres éléments du système (processus, règles métier, programmes, travaux, outils, etc.).

    Pour une représentation visuelle, voir la **FIGURE 2: INFOGRAPHIE ILLUSTRANT LA MÉTADONNÉE**.

- **Partage des données** : Pratique qui consiste à rendre les **DONNÉES** de recherche accessibles pour une réutilisation. Cela se fait notamment en versant les données dans un dépôt[30] ou par le biais de la publication des données.

- **Périphérique de sauvegarde portatif** : Les périphériques de stockage portatifs sont tout périphérique ou support facilement transportable sur lequel des données peuvent être stockées. Cette définition n'est pas limitée aux périphériques spécialement conçus pour le stockage tels que les CD et DVD, les disques durs amovibles et les lecteurs flash USB, mais peut également inclure les ordinateurs portables, les tablettes électroniques, les téléphones (cellulaires) intelligents, les assistants numériques personnels (p. ex. Siri, Alexa et Cortana) ainsi que tout autre équipement informatique portatif. Les périphériques de sauvegarde portatifs peuvent être connectés à Internet ou non, différentes mesures de sécurité des données s'appliqueront dans chaque cas.

- **Plan de gestion des données de recherche (PGD)[31] :** Un PGD est une déclaration officielle décrivant comment les **DONNÉES** de recherche seront gérées et documentées tout au long du

---

<https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/hachage.html> (site consulté le 29 nov. 2019).

[27] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Chiffrement » dans *Terminologie en sécurité informatique*, Gouvernement du Québec, m.à.j. février 2013, [En ligne] : <https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/journalisation.html> (site consulté le 29 nov. 2019).

[28] Voir également les explications données dans la Foire aux questions de la *Politique des trois organismes sur la gestion des données de recherche*, en ligne : <https://www.ic.gc.ca/eic/site/063.nsf/fra/h_97609.html> (consulté le 2020-10-09), question 3 (g) « En quoi consistent les métadonnées? ».

[29] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Fiche terminologique : métadonnée », *dans Le grand dictionnaire terminologique (GDT),* Gouvernement du Québec, En ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8869869

[30] PORTAGE, « Expression en GDR en français et en anglais » dans *Ressources de formation par Portage*, En ligne : <https://portagenetwork.ca/fr/ressources-de-formation-par-portage/expressions-gdr-francais-anglais/> (consulté le 2020-10-09).

projet de recherche. Presque tous les PGD contiennent les éléments essentiels suivants : métadonnées, politiques d'accès et de partage, politiques de réutilisation et de destruction. Le CÉR du CIUSSS de l'Estrie – CHUS encourage l'utilisation de l'Assistant PDG de Portage, un outil bilingue, pour préparer un PDG qui suit les meilleures pratiques en matière de gestion des données et guide les chercheurs pas à pas à travers les questions clés sur la **GESTION DES DONNÉES DE RECHERCHE**.

- **Redondance**[32] : Il s'agit de la duplication d'un élément essentiel au fonctionnement d'un système informatique en vue de pallier la défaillance éventuelle de cet élément et d'assurer ainsi la continuité d'une fonction informatique vitale. Elle s'applique autant à un système complet qu'à des éléments d'information.

- **Renseignements (types de)** [33]

    - **anonymes** : Renseignements auxquels aucun identificateur n'a jamais été associé (p. ex. réponse à un sondage anonyme). Le risque d'identification des personnes est faible ou très faible.

    - **anonymisés :** Renseignements dont tous les identificateurs directs sont irrévocablement retirés et pour lesquels aucun code permettant une réidentification ultérieure n'est conservé. Le risque de réidentification de la personne à partir des identificateurs indirects restants est faible ou très faible.

    - **codés**[34] **:** Renseignements dont les identificateurs directs ont été retirés et remplacés par un code. Si le code est accessible, il peut être possible de réidentifier des participants précis (p. ex. si le chercheur principal conserve une liste permettant d'associer, au besoin, le nom de code des participants à leur vrai nom).

    - **d'identification directe :** Renseignements permettant d'identifier une personne en particulier par des identificateurs directs (p. ex. nom, numéro d'assurance sociale ou numéro d'assurance maladie).

    - **d'identification indirecte :** Renseignements qui peuvent vraisemblablement permettre d'identifier une personne par une combinaison d'identificateurs indirects (p. ex. date de naissance, lieu de résidence ou caractéristique personnelle distinctive).

- **Renseignements accessibles au public**[35] **:** Documents, fichiers ou publications existants, qui peuvent ou non contenir des renseignements identificatoires, dont l'utilisation ou la diffusion n'est soumise à aucune restriction ou qui peuvent être rendus publics sous réserve de certaines conditions légales.

---

[31] Voir également les explications données dans la Foire aux questions de la *Politique des trois organismes sur la gestion des données de recherche,* en ligne : <https://www.ic.gc.ca/eic/site/063.nsf/fra/h_97609.html> (consulté le 2020-10-09), question 3 (d) « Qu'est-ce qu'un plan de gestion des données (PDG)? » et question 3 (f) « Quelles sont les principales composantes du plan de gestion des données? »

[32] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Chiffrement » dans *Terminologie en sécurité informatique*, Gouvernement du Québec, m.à.j. février 2013, [En ligne] : <https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/redondance.html> (site consulté le 29 nov. 2019).

[33] Tel que défini dans le « Glossaire » de l'ÉPTC 2 (2018), p. 226.

[34] Conseil pratico-pratique : Pour diminuer davantage le risque de réidentification, il est possible également de transformer les identifiants indirects qui pourraient être utilisés seuls ou en combinaison pour réidentifier un individu (p. ex. date de naissance, détails géographiques, dates d'événements clés).

[35] Tel que défini dans le « Glossaire » de l'ÉPTC 2 (2018), p. 226.

- **Renseignements personnels *ou* identificatoires**[36] : « Renseignements qui, seuls ou en combinaison avec d'autres renseignements accessibles, risquent vraisemblablement de permettre d'identifier une personne. »[37] Ces renseignements peuvent être utilisés pour identifier, contacter ou localiser une personne en particulier. Ceux-ci se composent de renseignements **D'IDENTIFICATION DIRECTE** associés ou non avec des renseignements **D'IDENTIFICATION INDIRECTE** . Même lorsque des données sont agrégées, il peut devenir possible d'identifier une personne quand il y a très peu d'individus dans une catégorie en particulier ou qu'il s'agit de valeurs extrêmes. Le caractère identificatoire d'un **ENSEMBLE DE DONNÉES** dépend de la quantité de renseignements détenus ainsi que des compétences et de la technologie utilisée par le détenteur de ces données.

- **Renseignements personnels sur la santé (RPS)** : Les RPS sont des **RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES** liés aux soins de santé d'une personne. Cela peut comprendre des renseignements se rapportant à sa santé physique ou mentale, ses antécédents familiaux, des renseignements concernant le mode de paiement ou l'admissibilité à certains soins ou, encore, son numéro d'assurance-maladie.

- **Risques d'atteinte à la vie privée**[38] : Préjudices potentiels que peuvent subir les participants, ou les groupes auxquels ils appartiennent, à cause de la collecte, de l'utilisation ou de la divulgation de renseignements personnels dans le cadre de la recherche.

- **Sécurité des données :** « Mesures prises pour protéger les renseignements. Il peut s'agir de mesures de protection matérielle, administratives ou techniques. »[39] Ces mesures servent à s'assurer qu'on puisse accéder aux données lorsque requis (disponibilité), que ces dernières ne sont pas altérées (intégrité), que la confidentialité soit préservée (confidentialité), et que les données sont conservées, puis éliminées de manière appropriée (conservation/destruction). Pour plus de détails, consulter la section « **PROPRIÉTÉS FONDAMENTALES EN INFORMATIQUE** ».

- **Services infonuagiques (Cloud) :** Méthode de stockage et de partage de données permettant de conserver les données sur des serveurs distants accessibles depuis Internet. Les services infonuagiques sont maintenus, exploités et gérés par un fournisseur de services sur des serveurs de stockage. Ces services peuvent être publics ou privés. Les services infonuagiques publics incluent *DropBox*, *Google Drive*, *iCloud* et le *OneDrive.* Bien que toute utilisation de services infonuagiques comporte des risques inhérents, les risques sont différents pour les serveurs publics ou privés, principalement en ce qui concerne l'emplacement et le contrôle du serveur ainsi que la surface d'attaque. Avec le stockage dans un service public, les données peuvent être stockées n'importe où dans le monde et, donc, être soumises aux lois du pays d'accueil. Avec le service privé, vos données sont gérées par un contrat de licence et sont stockées sur des serveurs dont la localisation est connue. L'institution concernée contrôle alors les accès aux services et, parfois même, aux données. De plus, les services publics peuvent avoir une infrastructure tentaculaire comportant de nombreux points d'attaque. Généralement, les services privés sont moins ouverts à de telles attaques et offrent un meilleur niveau de protection. Pour des renseignements supplémentaires, consulter la section « **SERVICES INFONUAGIQUES (CLOUD)** ».

- **Suppression**[40] **:** Le processus de **DESTRUCTION DES DONNÉES** stockées sur des disques durs, des appareils mobiles et d'autres formes de supports électroniques afin qu'elles soient complètement illisibles et ne puissent être consultées ou utilisées.

---

[36] Voir également la définition se trouvant sur le site de l'OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, En ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26532706> (consulté le 2020-10-09).

[37] *Id.*

[38] Tel que défini dans le « Glossaire » de l'ÉPTC 2 (2018), p. 227.

[39] *Id*.

[40] Voir également la définition se trouvant sur le site de l'OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, En ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2071864> (consulté le 2020-10-09).

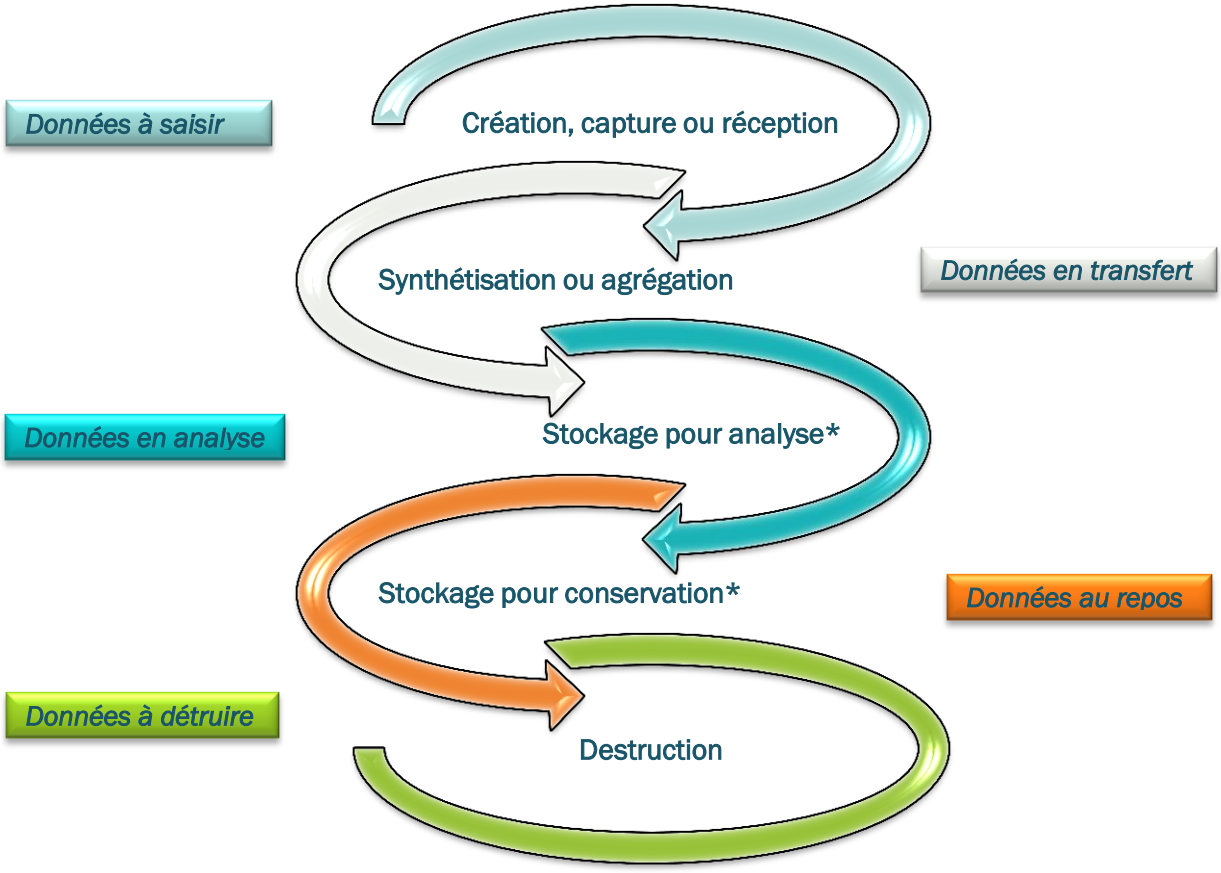
# ANNEXE 1 : CYCLE DE VIE DES DONNÉES

La Politique de la sécurité de l'information du CIUSSS de l'Estrie – CHUS définit le cycle de l'information ainsi :

> *« l'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisation ».*

Dans le contexte de la recherche, le cycle de vie des données doit être vu comme un schéma itératif, c'est-à-dire pour lequel l'ordre des boucles peut changer et pour lequel des boucles peuvent être refaites à plusieurs reprises.

Figure 1 : Cycle de vie des données




***L'objectif est de veiller à adopter les meilleures pratiques possibles en matière de sécurité de l'information, et ce, à chaque étape du cycle de vie de vos données de recherche.***

# ANNEXE 2 : AIDE-MÉMOIRE SUR LES BONNES PRATIQUES POUR LA SÉCURITÉ DES DONNÉES

Voici un document développé par l'Université de Québec à Montréal qui pourrait vous aider :

« Guide de bonnes pratiques pour la sécurité informatique des données de recherche ».

# ANNEXE 3 : QUESTIONS FRÉQUEMMENT POSÉES RELATIVEMENT À LA GESTION DES DONNÉES DE RECHERCHE (F.A.Q.)

1. **Est-ce qu'un ordinateur portable protégé par mot de passe est un endroit sécuritaire pour conserver mes données?**

   La réponse se trouve dans la section **ÉQUIPEMENT INFORMATIQUE** (p. 5).

2. **Combien de temps devrais-je conserver mes données?**

   La réponse se trouve dans la section **DURÉE DE CONSERVATION DES DONNÉES** (p. 9).

3. **Qu'est-ce que le chiffrement (ou l'encryptage)? Quand et comment devrais-je chiffrer mes données?**

   La réponse se trouve dans la section **CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE** (p. 6).

4. **Qu'est-ce que le stockage en ligne (*cloud storage*)? Est-ce sécuritaire de conserver mes données dans un nuage?**

   La réponse se trouve dans la section **SERVICES INFONUAGIQUES (CLOUD)** (p. 11).

5. **Est-ce sécuritaire de conserver mes données sur des appareils mobiles tels qu'un téléphone cellulaire ou une clé USB?**

   La réponse se trouve dans la section **PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF** (p. 11).

6. **Quelle est la différence entre une connexion internet sans fil ou réseau (filaire, câblée)? Est-ce qu'une ou l'autre est plus sécuritaire?**

   La réponse se trouve dans la section **TYPE DE CONNEXION À INTERNET** (p. 7).

7. **Quelle plateforme de sondage en ligne est-ce que je devrais utiliser?**

   La réponse se trouve dans la section **SONDAGES EN LIGNE** (p. 13).

8. **Quel est le meilleur moyen de partager mes données avec mes cochercheurs et cochercheuses provenant d'autres établissements ou institutions de recherche?**

   La réponse se trouve dans la section **PARTAGE DE DONNÉES AVEC LES COCHERCHEUSES ET COCHERCHEURS** (p. 12).

À noter : Plusieurs réponses à ces questions dépendent du niveau de risque associé aux données que vous avez collecté dans le cadre de votre projet. Pour en savoir plus sur les niveaux de risques, consulter le document **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE** (annexe 4, p. 29).

# ANNEXE 4 : MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE

| | FAIBLE RISQUE | MOYEN RISQUE | HAUT RISQUE |
|---|---|---|---|
| **TYPES DE DONNÉES** | - Données de recherché ne contenant aucune information sensible ou identificatoire (par exemple, les renseignements ont été **ANONYMISÉS** ou **CODÉS**).<br>NB: En cas de doute, supposez que les données sont sensibles<br>- Documentation de recherche non sensible<br>- Renseignements accessibles au public | - Données de recherche pouvant contenir ou contenant des informations sensibles ou identificatoires<br>- Documentation de recherche sensible<br>- Renseignement permettant d'identifier une personne | - Données de recherche contenant des informations confidentielles, restreintes ou très sensibles<br>- **RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ**<br>- Renseignements financiers<br>- Données et protocoles de recherche lies à de la propriété intellectuelle hautement sensible |

| | FAIBLE RISQUE | MOYEN RISQUE | HAUT RISQUE |
|---|---|---|---|
| **EXEMPLES** | - Renseignements ont été **ANONYMISÉS** ou **CODÉS** ou qui sont complètement **ANONYMES**<br>- Formulaire d'information et de consentement (FIC) et fiches d'information vierges<br>- Renseignements recueillis sur un site web destiné au public | - Enregistrements audio ou vidéo d'entrevue, si le contenu ne comprend pas de renseignements jugés à haut risque<br>- Clés (codes) d'identification et FIC signés<br>- Renseignements financiers anonymisés ou codés associés aux paiements pour la participation à la recherche | - Renseignements relatifs à l'origine raciale ou ethnique, aux opinions politiques, aux croyances religieuses ou autres croyances similaires, à l'appartenance syndicale, à l'état de santé physique ou mentale, à la vie sexuelle, à la commission présumée ou avérée d'une infraction criminelle par la personne concernée (casier judiciaire) |

| | FAIBLE RISQUE | MOYEN RISQUE | HAUT RISQUE |
|---|---|---|---|
| **PROTECTION DES DONNÉES** | - Conservation des données de recherche conformément aux méthodes prévues au protocole de recherche approuvé par le Comité d'éthique de la recherche (CÉR) | - Collecte et stockage des données sur un dispositif protégé par un mot de passe; de préférence, sur un dispositif statique conservé dans un endroit protégé comme un ordinateur de bureau dans un bureau fermé à clé ou sur un serveur protégé de manière appropriée<br>- Toutes les données de recherches impliquant un être humain soumises à l'ÉPTC2 qui stipule que « les [**RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES** obtenus] dans le cadre de la recherche qui sont [conservés] sur un ordinateur branché à Internet doivent être [chiffrés]. »<br>- Voir ci-dessous pour plus d'information sur la conservation, l'accès et le transfert sécurisé de données | - Collecte et stockage des données sur un dispositif protégé par un mot de passe et **CHIFFREMENT**, de préférence sur un dispositif statique conservé dans un endroit protégé comme un ordinateur de bureau dans un bureau fermé à clé ou sur un serveur protégé de manière appropriée<br>- Toutes les données de recherche impliquant un être humain soumises à l'ÉPTC2 qui stipule que « les [**RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES** obtenus] dans le cadre de la recherche qui sont [conservés] sur un ordinateur branché à Internet doivent être [chiffrés]. »<br>- **SERVICES INFONUAGIQUES** institutionnel (privé) à utiliser pour le stockage ou le transfert de données; l'utilisation de services publics (Google Drive, DropBox, iCloud, Onedrive, etc.) sont strictement interdits; les restrictions sont détaillées ci-dessous. |

| | FAIBLE RISQUE | MOYEN RISQUE | HAUT RISQUE |
|---|---|---|---|
| **CONSERVATION DES DONNÉES** | - Tous les **PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF** ou non (dispositif de stockage), de partage de fichiers ou les **SERVICES INFONUAGIQUES** institutionnels (Office 365 du CIUSSS de l'Estrie – CHUS ou de l'Université de Sherbrooke) sont permis. | - Un ordinateur ou un périphérique de sauvegarde électronique externe qui répond aux exigences en matière de protection des données.<br>- **SERVICES INFONUAGIQUES** institutionnel (Office 365 du CIUSSS de l'Estrie – CHUS ou de l'Université de Sherbrooke) peuvent convenir si c'est spécifié au protocole de recherche soumis au CÉR; l'utilisation de services publics (Google Drive, DropBox, iCloud, Onedrive, etc.) sont strictement interdits. Des risques liés à la vie privée et à la sécurité existent, particulièrement pour les services externes avec lesquels il n'existe pas d'accord d'entreprise (licence institutionnelle).<br>- Dossiers partagés centraux, départementaux et de laboratoires qui répondent aux exigences de protection des données et qui ont été identifiés dans le protocole approuvé par le CÉR. | - Un ordinateur ou un périphérique de sauvegarde électronique externe qui répond aux exigences en matière de protection des données.<br>- Dossiers partagés centraux, départementaux et de laboratoires qui répondent aux exigences de protection des données et qui ont été identifiés dans le protocole approuvé par le CÉR. |

| | FAIBLE RISQUE | MOYEN RISQUE | HAUT RISQUE |
|---|---|---|---|
| **ACCÈS AUX DONNÉES** | - Aucune manipulation particulière n'est requise. | - L'accès aux renseignements confidentiels doit être limité aux personnes autorisées qui sont identifiées dans le protocole de recherche approuvé par le CÉR. | - L'accès aux renseignements confidentiels doit être limité aux personnes autorisées qui sont identifiées dans le protocole de recherche approuvé par le CÉR.<br>Note pour le CÉR : Le nombre de personnes autorisées devrait être le plus limité possible. |
| **TRANSFERT DE DONNÉES** | - Possible d'utiliser l'adresse courriel ou les **SERVICES INFONUAGIQUES** institutionnels (Office 365 du CIUSSS de l'Estrie – CHUS ou de l'Université de Sherbrooke), ainsi que les services publics (Google Drive, DropBox, iCloud, Onedrive, etc.). | - Les fichiers protégés par un **MOT DE PASSE ROBUSTE** peuvent être partagés en utilisant l'adresse courriel et l'option de **CHIFFREMENT** ou les **SERVICES INFONUAGIQUES** institutionnels (Office 365 du CIUSSS de l'Estrie – CHUS ou de l'Université de Sherbrooke). | - Les données restreintes devraient être conservées sur un périphérique de sauvegarde électronique externe protégé par un mot de passe robuste et chiffré, puis remis en mains propre.<br>- Les fichiers peuvent être transmis par le biais de liens qui ont les caractéristiques suivantes :<br>• correctement chiffrés;<br>• protégés par mot de passe robuste;<br>• ayant une durée limitée (expiration). |

# ANNEXE 5 : MATRICE DES RISQUES ASSOCIÉS AUX DONNÉES NUMÉRIQUES

| | RISQUES POUR LES PERSONNES PARTICIPANT À LA RECHERCHE | RISQUES POUR LES CHERCHEURS ET CHERCHEUSES | RISQUES POUR LES INSTITUTIONS | RISQUES POUR LES DONNÉES | GESTION DES RISQUES |
|---|---|---|---|---|---|
| **ACCÈS NON AUTORISÉ AUX DONNÉES** | La perte de contrôle, la divulgation ou l'accès à des **RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES** et/ou sensibles pourraient causer un préjudice important aux personnes participantes, selon le profil des données (**FAIBLE RISQUE**, **MOYEN RISQUE** ou **HAUT RISQUE**). | Il incombe au chercheur responsable d'évaluer « les risques d'atteinte à la vie privée et les menaces pour la sécurité de l'information pour toutes les étapes du cycle de vie de la recherche et [de] mettre en œuvre des mesures adéquates pour protéger l'information ». Ceux qui ne respectent pas cette obligation s'exposent à des risques psychologiques, sociaux, professionnels et juridiques. | « Les établissements ou les organisations où sont conservées des données de recherche ont la responsabilité d'établir des mesures de sécurité appropriées pour protéger ces données. » Les institutions qui ne respectent pas cette obligation s'exposent à des risques éthiques, juridiques et de réputation. | Le respect de l'obligation de contrôler l'accès aux données est essentiel pour l'intégrité du projet de recherche. Lorsque les données ont été consultées de manière non autorisée, leur intégrité et leur utilité sont remises en question. | - Protection par un **MOT DE PASSE ROBUSTE**<br><br>- **CHIFFREMENT DES DONNÉES ET DE L'ÉQUIPEMENT INFORMATIQUE**<br><br>- Évitez d'utiliser les **SERVICES INFONUAGIQUES** publics<br><br>- Évitez les transferts de données par courriel<br><br>Pour en savoir plus, consulter la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**. |

| | RISQUES POUR LES PERSONNES PARTICIPANT À LA RECHERCHE | RISQUES POUR LES CHERCHEURS ET CHERCHEUSES | RISQUES POUR LES INSTITUTIONS | RISQUES POUR LES DONNÉES | GESTION DES RISQUES |
|---|---|---|---|---|---|
| **VIOLATION DE LA CONFIDENTIALITÉ** | Selon le profil des données (**FAIBLE RISQUE**, **MOYEN RISQUE** ou **HAUT RISQUE**), les personnes participantes sont soumises, au mieux, à un abus de confiance et, au pire, à d'importants risques psychologiques, sociaux et physiques. | « Il est essentiel de s'acquitter [du] devoir éthique de confidentialité pour maintenir le lien de confiance entre le chercheur et le participant ». Outre l'abus de confiance, les chercheurs qui ne respectent pas cette obligation s'exposent à des risques psychologiques, sociaux, professionnels et juridiques. | « [Le devoir éthique de confidentialité] comporte l'obligation de protéger l'information contre l'accès, l'utilisation, la divulgation et la modification non autorisés, d'une part, et contre la perte et le vol, d'autre part. » Les institutions qui ne respectent pas cette obligation s'exposent à des risques éthiques, juridiques et de réputation. | « Il est essentiel de s'acquitter [du] devoir éthique de confidentialité pour maintenir [...] l'intégrité du projet de recherche. » Lorsque la confidentialité a été compromise, l'intégrité et l'utilité des données sont remises en question. | - Toutes les tactiques de gestion des risques associées à « accès non autorisé aux données »<br><br>- Séparation des **RENSEIGNEMENTS PERSONNELS OU IDENTIFICATOIRES** des autres renseignements<br><br>- Accès aux données limitées<br><br>Pour en savoir plus, consulter la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**. |

| | RISQUES POUR LES PERSONNES PARTICIPANT À LA RECHERCHE | RISQUES POUR LES CHERCHEURS ET CHERCHEUSES | RISQUES POUR LES INSTITUTIONS | RISQUES POUR LES DONNÉES | GESTION DES RISQUES |
|---|---|---|---|---|---|
| **CORRUPTION DES DONNÉES** | Les personnes participantes ont consacré leur temps et leurs ressources à la participation à un projet de recherche en espérant que leur participation aura un certain rôle à jouer dans la production de conclusions significatives. Lorsque les données sont corrompues, les personnes participantes peuvent se voir refuser ce droit. | Lorsque les données sont corrompues, les chercheurs risquent de perdre des données, de confondre les calendriers de recherche, d'abuser de la confiance des personnes participantes et même de devoir annuler le projet ou de ne pas être en mesure de le terminer entièrement. | Les projets de recherche qui sont interrompus, perturbés ou annulés en raison de la corruption des données entraînent un gaspillage des ressources institutionnelles. | La corruption des données peut potentiellement les rendre inutilisables partiellement ou totalement. | - Évitez l'utilisation de **PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF** de basse qualité<br><br>- Surveillez l'état de santé de votre disque dur, par exemple à l'aide d'un utilitaire d'analyse et d'étalonnage pour Windows[41] ou Mac[42]<br><br>- Créez une copie de sauvegarde[43]<br><br>Pour en savoir plus, consulter la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**. |

[41] Consulter le <https://recoverit.wondershare.com/hard-drive/how-to-fix-hard-drive-problems-with-chkdsk-in-windows.html?gclid=CjwKCAjwkJj6BRA-EiwA0ZVPVuicbUfFi65sJmSO5Abk9GVL1h34-JV78cXCdDAPwce3WD9o_ITAvhoC904QAvD_BwE>

[42] Consulter le <https://osxdaily.com/2012/05/24/check-hard-drive-health-mac-disk-utility/>.

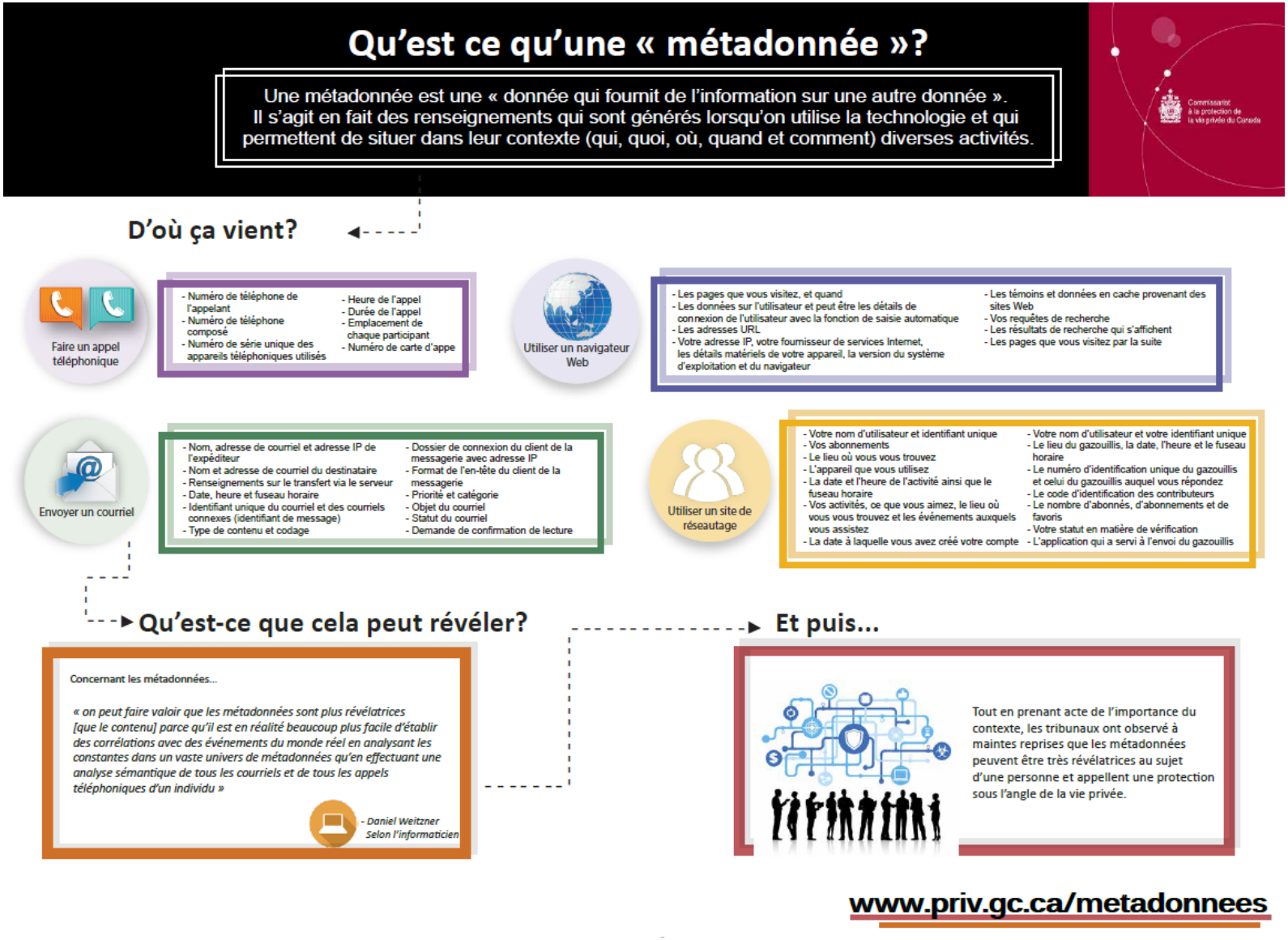
[43] « À noter qu'un back-up des données qui sont sauvegardées sur les serveurs institutionnels est fait quotidiennement. »

| | RISQUES POUR LES PERSONNES PARTICIPANT À LA RECHERCHE | RISQUES POUR LES CHERCHEURS ET CHERCHEUSES | RISQUES POUR LES INSTITUTIONS | RISQUES POUR LES DONNÉES | GESTION DES RISQUES |
|---|---|---|---|---|---|
| **PERTE DES DONNÉES** | Les personnes participantes ont consacré leur temps et leurs ressources à la participation à un projet de recherche en espérant que leur participation aura un certain rôle à jouer dans la production de conclusions significatives. Lorsque les données sont perdues, les personnes participantes peuvent se voir refuser ce droit. | Lorsque les données sont perdues, les chercheurs risquent de confondre les calendriers de recherche, d'abuser de la confiance des personnes participantes et même de devoir annuler le projet ou de ne pas être en mesure de le terminer entièrement.<br>. | Les projets de recherche qui sont interrompus, perturbés ou annulés en raison de la perte des données entraînent un gaspillage des ressources institutionnelles. | La perte des données les rend complètement inutilisables. | - Évitez l'utilisation de **PÉRIPHÉRIQUE DE SAUVEGARDE PORTATIF** de petit format, telles que les clés USB, qui peuvent être facilement égarées<br><br>- Créer une copie de sauvegarde[44]<br><br>Pour en savoir plus, consulter la **MATRICE DE LA GESTION DES DONNÉES DE RECHERCHE**. |

[44] « À noter qu'un back-up des données qui sont sauvegardées sur les serveurs institutionnels est fait quotidiennement. »

# ANNEXE 6 : MÉTADONNÉE

Figure 2: Infographie illustrant la métadonnée



# RÉFÉRENCES

## *Publication citée*

CONSEIL DE RECHERCHES EN SCIENCES HUMAINES, CONSEIL DE RECHERCHE EN SCIENCES NATURELLES ET EN GÉNIE DU CANADA ET INSTITUTS DE RECHERCHE EN SANTÉ DU CANADA, *Énoncé de politique des trois conseils: Éthique de la recherche avec des êtres humains* (ÉPTC 2 (2018)), décembre 2018.

## *CIUSSS de l'Estrie - CHUS*

Des documents de référence sont disponibles dans l'Intranet du CIUSSS de l'Estrie – CHUS (pour ceux qui y ont accès) : **Boîte à outils** > **Sécurité de l'information**.

- *Procédure pour chiffrer un courriel avec Outlook365*
- *Procédure pour chiffrer un document (Word, Excel, PDF ou autres formats)*
- *Définition d'un mot de passe robuste*
- *Guide d'utilisation des outils de communication*

## *Université de Sherbrooke*

Des capsules d'information sont disponibles sur le site web de l'Université de Sherbrooke : **Sécurité de l'information** > **Conseils et astuces**.

Dans le contexte de la pandémie de la COVID-19, des outils relatifs aux modalités de télétravail ont été mis en ligne sur le site web de l'Université de Sherbrooke : **Coronavirus** > **FAQ** > **Cybersécurité**.