Manuel sur la protection de la vie privée et sur la confidentialité et le stockage sécurisé des données

Konrad Czechowski et John Sylvestre

8 janvier 2018 (révision : août 2019)

Centre de recherche sur les services éducatifs et communautaires (CRSEC)
613-562-5800, poste 1856 | crsec@uottawa.ca
crsec.uOttawa.ca

uOttawa

Table des matières

Remerciements

Nous aimerions remercier Catherine Paquette et son équipe du Bureau d’éthique et d’intégrité de la recherche, nos bibliothécaires Susan Mowers, Jessica McEvan et leur équipe, ainsi que l'architecte en sécurité Sandeep Gupta de l'Université d'Ottawa pour leurs précieux commentaires et suggestions sur les versions antérieures du présent document.

Introduction

Le présent manuel décrit les procédures recommandées par le Centre de recherche sur les services éducatifs et communautaires (CRSEC) pour la collecte, la protection et le traitement des données confidentielles. En tant qu'établissement de recherche situé à l'Université d'Ottawa, le CRSEC doit se conformer aux normes les plus élevées en matière de protection des renseignements personnels et renseignements confidentiels. Les chercheurs, les étudiants et les stagiaires postdoctoraux du CRSEC ont régulièrement accès à des renseignements confidentiels tels que des renseignements personnels identifiables, des renseignements sur la santé et d'autres types de renseignements non publics.

Il est essentiel que le CRSEC, dans son rôle de centre de recherche, soit en mesure d'assurer ses partenaires institutionnels et les participants à la recherche de la sécurité et de la confidentialité des données qu'ils fournissent. Le moindre écart de vigilance peut avoir des conséquences pour les participants, le CRSEC, l'Université d'Ottawa ou nos partenaires communautaires et institutionnels. Il est de la responsabilité de chacun au CRSEC de traiter la sécurité des données comme une partie vitale de son travail.

Le présent manuel commence par une justification du maintien de la protection de la vie privée, de la confidentialité et de la sécurité des données. Suit une brève description de la façon dont l'information pour ce manuel a été recueillie. Ensuite, un examen des lois provinciales et fédérales applicables en matière de protection de la vie privée ainsi que des codes de conduite professionnelle est présenté. À la suite de cet examen, une liste de recommandations concernant la protection de la vie privée, la confidentialité et la sécurité des données est fournie.

Principes généraux

- Les recommandations concernant la collecte, la protection et l'utilisation des données confidentielles s'appliquent à tout le personnel du CRSEC, y compris les professeurs, les employés, les associés de recherche, les chercheurs invités, les stagiaires postdoctoraux, les étudiants et les stagiaires. Les professeurs et les autres personnes qui ont un rôle de supervision du personnel et des étudiants du CRSEC ont quant à eux la responsabilité de s'assurer que les personnes qu'ils supervisent connaissent, comprennent et suivent ces recommandations.

- L'approbation éthique des comités d'éthique de la recherche (CER) de l'Université est requise pour les études avec des participants humains. Les chercheurs doivent obtenir une approbation éthique avant de commencer toute activité de recherche auprès d'êtres humains.

    - Tout projet de recherche comportant l'acquisition directe de données auprès de participants humains (p. ex. au moyen d'entrevues, de groupes de discussion, de sondages, etc.).

    - Les projets dont le but premier est l'assurance de la qualité (comme l'évaluation de programmes) et pour lesquels il n'y a aucune intention de publier les résultats dans

une revue évaluée par des pairs peuvent ne pas nécessiter l'approbation du CER. Toutefois, les lignes directrices de l'*Énoncé de politique des trois conseils* (EPTC 2) sur l'éthique de la recherche doivent toujours être suivies. Les chercheurs devraient consulter le Bureau d'éthique et d'intégrité de la recherche (BEIR) pour déterminer si une évaluation par un CER est nécessaire pour leur projet.

- Les projets comportant l'utilisation de données secondaires peuvent nécessiter l'approbation du CER, selon la nature et la source des données. Les chercheurs devraient consulter le Bureau d'éthique pour déterminer si une évaluation par un CER est nécessaire pour leur projet.

- On trouvera un complément d'information à l'adresse https://recherche.uottawa.ca/deontologie/

- La Bibliothèque offre à la communauté de l'Université d'Ottawa des services d'accès et de consultation de données secondaires à usage public et des services connexes, comme l'accès à faible risque aux données confidentielles de Statistique Canada par le biais d'un service d'accès à distance en temps réel, en complément à un centre de données de recherche sécurisé situé à la Bibliothèque. Prière de contacter la bibliothèque pour plus d'informations.

Méthode

Les étapes décrites ci-après ont été suivies pour l'élaboration du manuel :

1. Recherche en ligne sur des termes comme « politique de sécurité des données », « politique de confidentialité » et « sécurité des données ».
2. Examen des codes d'éthique pertinents à l'échelle nationale et par discipline.
3. Examen des sites Web des commissaires à la protection de la vie privée de l'Ontario et du Canada.
4. Consultation de bibliothécaires spécialisés dans la gestion des données.
5. Consultation de l'architecte de la sécurité des données de l'Université d'Ottawa.
6. Consultation du conseiller juridique de l'Université d'Ottawa et du Bureau d’éthique et d’intégrité de la recherche.
7. Présentation de l'ébauche des conclusions aux chercheurs, aux étudiants et aux agents du protocole d'éthique de la recherche de l'Université.

Constatations

Lois et codes de déontologie professionnelle applicables

Les lois et codes d'éthique professionnelle ont fait l'objet d'un examen visant à extraire l'information propre à la protection de la vie privée, à la confidentialité et à la sécurité des données pertinentes à la recherche reliée au CRSEC. Voici les résultats de l'examen de six sources pertinentes aux activités de recherche menées au CRSEC. Bien que les chercheurs du CRSEC puissent aussi être affiliés à des organismes professionnels étrangers (p. ex. l'American Evaluation Association), seules les sources canadiennes les plus pertinentes ont été incluses dans cette section du manuel. D'autres principes éthiques peuvent s'appliquer au travail au CRSEC, et chaque chercheur du Centre devrait connaître tous les codes d'éthique qui lui sont applicables. Le présent manuel vise à résumer les renseignements les plus pertinents à la protection de la vie privée, à la confidentialité et à la sécurité des données dans les situations qui se présentent le plus souvent aux chercheurs du CRSEC. Il n'a pas pour but de remplacer ou de supplanter de quelque façon que ce soit les lois ou les codes d'éthique de portée plus étendue.

Voici donc ce que nous avons résumé : (i) la *Loi sur la protection des renseignements personnels et les documents électroniques*, (ii) la *Loi sur la protection des renseignements personnels sur la santé*, (iii) l'*Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains*, rédigé au nom des trois principaux organismes de financement de la recherche au Canada, (iv) les lignes directrices en matière d'éthique de la Société canadienne d'évaluation, (v) les lignes directrices en matière d'éthique de la Société canadienne de psychologie et (vi) les lignes directrices en matière d'éthique de l'Ordre des psychologues de l'Ontario.

Loi sur la protection des renseignements personnels sur la santé (LPRPS) et *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

La LPRPDE est une loi fédérale en cinq parties qui régit la gestion des renseignements personnels. La LPRPS est une loi provinciale de l'Ontario qui a été déclarée « essentiellement similaire » à la loi fédérale (LPRPDE) en ce qui concerne les dépositaires de renseignements sur la santé. Ainsi, les dépositaires de renseignements sur la santé n'ont qu'à se conformer à la LPRPS pour la collecte, l'utilisation et la communication des renseignements personnels qui ont lieu dans la province de l'Ontario (Commissaire à la protection de la vie privée du Canada, 2013). La LPRPDE s'applique tout de même aux dépositaires de renseignements sur la santé en Ontario dans certaines situations, comme la divulgation de renseignements sur la santé à des agents à l'extérieur de l'Ontario, aux renseignements personnels qui ne sont pas liés à la santé et aux activités visées aux parties 2 à 5 de la LPRPDE (p. ex. l'utilisation de documents électroniques; Ordre des psychologues de l'Ontario, 2004; Commissaire à l'information et à la vie privée de l'Ontario, 2015).

La LPRPDE a été résumée en dix « principes relatifs à l'équité dans le traitement de l'information » (Ordre des psychologues de l'Ontario, 2013; Commissariat à la protection de la vie privée du Canada, 2015) :

1. **Responsabilisation** : L'organisation [Université d'Ottawa] est responsable des renseignements personnels dont elle assure la gestion et doit désigner une personne responsable de la conformité à la LPRPDE.

2. **Détermination des fins de la collecte** : Les fins auxquelles les renseignements personnels sont recueillis doivent être précisées au moment de la collecte ou avant.

3. **Consentement** : Le consentement éclairé de la personne est requis pour la collecte, l'utilisation ou la communication de ses renseignements personnels, à moins d'indication contraire.

4. **Limitation de la collecte** : La quantité et le type de renseignements personnels recueillis se limitent à ce qui est nécessaire aux fins déterminées.

5. **Limitation de l'utilisation, de la communication et de la conservation** : Les renseignements personnels ne doivent pas être conservés plus longtemps qu'il n'est nécessaire pour atteindre les fins auxquelles ils ont été recueillis et ne doivent être communiqués ou utilisés qu'à ces fins, sauf avec le consentement de la personne concernée ou si la loi l'exige.

6. **Exactitude** : Il faut veiller à ce que les renseignements personnels soient aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils ont été recueillis.

7. **Mesures de sécurité** : Les renseignements personnels doivent être protégés par des mesures de sécurité correspondant à leur degré de sensibilité.

8. **Transparence** : Des renseignements précis sur les politiques et les pratiques relatives à la gestion des renseignements personnels doivent être facilement accessibles aux particuliers. Il peut s'agir d'informations contextuelles sur les méthodes et les objectifs des études auxquelles les individus ont participé.

9. **Accès aux renseignements perso**nnels : Sur demande, une personne doit être informée de l'existence, de l'utilisation et de la divulgation de ses renseignements personnels et doit avoir accès à ces renseignements. Une personne doit être en mesure de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections qui s'imposent.

10. **Possibilité de porter plainte à l'égard du non-respect des principes** : Une personne doit être en mesure de s'adresser, au moyen de procédures facilement accessibles, à la personne responsable de l'application de la LPRPDE pour s'assurer qu'elle se conforme aux principes énoncés ci-dessus.

Renseignements personnels. Les « renseignements personnels » se rapportent aux clients, aux clients potentiels ou au personnel contractuel (p. ex., les non-employés, les bénévoles, les étudiants) et comprennent les renseignements factuels ou subjectifs au sujet de la situation d'une personne identifiable (Ordre des psychologues de l'Ontario, 2004) :

- caractéristiques personnelles (p. ex. le sexe, l'âge, la race, l'origine ethnique, le pays d'origine, l'éducation ou la formation, la situation de famille, la religion, la profession, les antécédents sexuels ou l'orientation sexuelle);

- santé (p. ex. antécédents médicaux, états de santé ou services reçus).

Renseignements personnels sur la santé. Les renseignements personnels sur la santé sont définis au sens large et comprennent (Ordre des psychologues de l'Ontario, 2004; Commissaire à l'information et à la protection de la vie privée de l'Ontario, 2015) :

- les renseignements sur une personne identifiable (y compris des données qui peuvent être combinées à d'autres données pour l'identifier);

- les renseignements verbaux ou enregistrés (le fait de poser une question peut constituer une collecte de renseignements personnels sur la santé, même si les renseignements ne sont pas consignés);

- les renseignements relatifs à l'individu :

    i. les antécédents personnels ou familiaux associés à son état physique ou mental;

    ii. les soins de santé (y compris l'entretien et les mesures préventives ou palliatives);

    iii. les fournisseurs de soins de santé;

    iv. les paiements pour les soins de santé ou le numéro de carte d'assurance-maladie;

    v. le décideur substitut;

    vi. d'autres renseignements (p. ex., numéro de téléphone) combinés à d'autres renseignements personnels sur la santé.

Voici des exemples de renseignements personnels sur la santé provenant de l'Ordre des psychologues de l'Ontario (2004) :

- **Caractéristiques personnelles** : Nom, coordonnées du domicile, numéro d'identification (p. ex. carte de crédit, assurance sociale, témoins de sites Web), couverture d'assurance, caractéristiques d'identification (p. ex. empreintes digitales, groupe sanguin), sexe, âge, race, langue, origine ethnique ou nationale, éducation, état civil, antécédents sexuels, orientation sexuelle, revenu et statut social.

- **Information sur la santé** : Antécédents médicaux, mesures, échantillons ou résultats d'examen, conditions, résultats d'évaluation, diagnostics, services reçus, renseignements recueillis au cours de la prestation de services, pronostic ou autres

opinions formées au cours de l'évaluation et du traitement, conformité à l'évaluation et au traitement, motifs du congé et conditions de congé et recommandations, et activités ou plans de dons de corps.

Divulgation, stockage et sécurité des renseignements personnels sur la santé. Les dépositaires de renseignements sur la santé (habituellement un hôpital) ont la responsabilité de protéger les renseignements personnels sur la santé contre le vol, la perte, l'utilisation non autorisée, la divulgation, la copie, la modification ou la destruction. Les gardiens ont l'obligation positive d'aviser les personnes de toute atteinte à leur vie privée.

La LPRPS prévoit la divulgation de renseignements personnels sur la santé à des fins de recherche dans certaines conditions. À la lumière du paragraphe 1 de l'article 44 de la LPRPS (intitulé « Divulgation relative à une recherche »), les lignes directrices suivantes sont présentées :

Un dépositaire de renseignements sur la santé peut divulguer des renseignements personnels sur la santé concernant un particulier à un chercheur qui,

a) d'une part, présente ce qui suit au dépositaire :

(i) une demande écrite;

(ii) un plan de recherche qui satisfait aux exigences du paragraphe (2);

(iii) une copie de la décision d'une commission d'éthique de la recherche d'approuver le plan de recherche;

b) d'autre part, conclut l'accord exigé par le paragraphe (5).

Le paragraphe 2 (intitulé « Plan de recherche ») fait référence à un plan écrit qui doit contenir les éléments suivants :

a) l'affiliation de chaque personne qui participe à la recherche;

b) la nature et les objets de la recherche, et les avantages que prévoit le chercheur pour le public ou la science;

c) les autres questions prescrites ayant trait à la recherche.

Le paragraphe 5 (intitulé « Accord de divulgation ») se lit comme suit :

Un dépositaire de renseignements sur la santé, avant de divulguer des renseignements personnels sur la santé à un chercheur en vertu du paragraphe (1), conclut avec ce dernier un accord selon lequel le chercheur convient de se conformer aux conditions et aux restrictions, le cas échéant, qu'impose le dépositaire relativement à l'utilisation, à la protection, à la divulgation, au retour ou à l'élimination des renseignements.

Il est important de noter que si un chercheur du CRSEC obtient de l'information d'un autre établissement, le CRSEC est assujetti aux mêmes exigences de protection de la vie privée et de confidentialité que l'établissement d'où proviennent les données.

Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains.

L'Énoncé de politique des trois Conseils a été élaboré à l'initiative des présidents des différents organismes de financement de la recherche (Instituts de recherche en santé du Canada (IRSC), Conseil de recherches en sciences naturelles et en génie (CRSNG) et Conseil de recherches en sciences humaines (CRSH)). L'objectif de l'énoncé de politique était d'assurer que les établissements financés par les conseils de recherche fédéraux et leurs chercheurs se conforment aux politiques en matière d'éthique établies par les trois Conseils pour la recherche auprès d'êtres humains. Les lignes directrices sont mises à jour de temps à autre, et la version la plus récente de l'Énoncé a paru en décembre 2014 (EPTC 2, 2014). Le chapitre 5 traite expressément de la protection de la vie privée et de la confidentialité.

Selon l'EPTC 2, il est important que toute exception à l'égard de la vie privée ou de la confidentialité, qu'elle soit d'ordre légal ou éthique, soit décrite dans le processus de consentement libre et éclairé et approuvée par le CER avant le début de la collecte des données, sauf si l'information est accessible au public. Lors de l'évaluation d'un programme, l'approbation d'un CER peut ne pas être nécessaire, mais les mêmes normes en matière de protection de la vie privée et de confidentialité devraient être maintenues. Les chercheurs qui comptent exclusivement sur l'utilisation secondaire de renseignements non identifiables ne sont pas tenus d'obtenir le consentement des participants, mais doivent demander l'évaluation du CER. L'identifiabilité peut dépendre du contexte (p. ex. l'utilisation de renseignements codés est considérée comme non identifiable seulement si le chercheur n'a pas accès à la clé) et le consentement des participants à l'utilisation secondaire de renseignements identifiables n'est pas toujours nécessaire si le CER donne son approbation (pour en savoir plus sur l'utilisation secondaire de renseignements, voir les articles 5.5 et 5.6 de l'EPTC 2, 2014).

En plus de l'Énoncé de politique général des trois Conseils, l'un des trois organismes (IRSC) a également produit un document sur les pratiques exemplaires en matière de protection de la vie privée dans la recherche en santé (Instituts de recherche en santé du Canada, 2005; http://www.cihr-irsc.gc.ca/f/29072.html). Selon ce document, l'évaluation des données devrait prendre la forme d'une évaluation de la vulnérabilité à la menace et au risque, ce qui comprend sept étapes (c.-à-d., déterminer quels actifs doivent être protégés, déterminer contre quoi il faut se protéger, évaluer la probabilité que la menace se produise, évaluer l'ampleur de l'impact si la menace se produit, évaluer les mesures de protection existantes, recommander des mesures supplémentaires appropriées et les mettre à jour régulièrement).

Société canadienne d'évaluation.

La Société canadienne d'évaluation fournit des lignes directrices générales en matière d'éthique à ses membres qui effectuent des recherches en évaluation. Les lignes directrices sont divisées en trois sections : compétence, intégrité et imputabilité. Ces lignes directrices générales indiquent que les évaluations devraient être conçues et menées de manière à protéger les droits (y compris le droit à la vie privée) et le bien-être de tous les participants. En général, les évaluateurs devraient agir avec intégrité et s'entretenir avec les clients au sujet des décisions contractuelles comme la confidentialité, la protection de la vie privée et la propriété des conclusions et des rapports (Société canadienne d'évaluation, 2014).

Société canadienne de psychologie

La Société canadienne de psychologie dispose d'un ensemble de lignes directrices en matière d'éthique, qui sont présentées dans le *Code canadien d'éthique pour les psychologues (quatrième édition)*. Ce code de déontologie s'applique à toutes les activités professionnelles des psychologues affiliés à la SCP, y compris le travail clinique, la consultation et la recherche (Société canadienne de psychologie, 2017). Selon la SCP, les psychologues ne devraient chercher et recueillir que des renseignements pertinents aux fins pour lesquelles le consentement a été obtenu. Les renseignements personnels ne sont recueillis et documentés que s'ils sont nécessaires à la prestation de services futurs ou à la réalisation d'une étude de recherche, ou s'ils sont requis ou justifiés par la loi. De plus, les clients devraient être informés des mesures prises pour assurer la confidentialité de leurs renseignements personnels. Enfin, dans les milieux où les renseignements personnels sont partagés ou recueillis en groupe (p. ex. groupe de discussion, psychothérapie de groupe), tous les clients devraient être informés de leurs responsabilités quant au maintien de la confidentialité à l'égard des autres membres du groupe (Société canadienne de psychologie, 2017).

Ordre des psychologues de l'Ontario

L'Ordre des psychologues de l'Ontario (OPO) a des lignes directrices en matière de déontologie, énoncées dans ses Normes de conduite professionnelle. Ce code de déontologie s'applique à toutes les activités professionnelles des psychologues inscrits auprès de l'OPO, y compris le travail clinique, la consultation et la recherche (Ordre des psychologues de l'Ontario, 2005). Selon l'OPO, les psychologues devraient déployer des efforts raisonnables pour s'assurer que les dossiers sont complets et accessibles. Dans le cas des clients organisationnels (sociétés et organismes, p. ex.), il convient de tenir un dossier comprenant le nom du client organisationnel, le nom et le titre des personnes autorisées à divulguer des renseignements confidentiels sur le client organisationnel, la date et la nature de chaque service fourni au client organisationnel, une copie de toutes les ententes et de la correspondance avec le client organisationnel et une copie de chaque rapport préparé pour le client.

Recommandations

Les chercheurs principaux du CRSEC se livrent à la collecte de données sur le terrain, ce qui suppose parfois la collecte d'informations confidentielles. Par conséquent, il est important que les chercheurs soient conscients des risques qui peuvent survenir pendant la collecte et le traitement de leurs données et qu'ils prennent les mesures appropriées pour protéger la vie privée de leurs participants. L'absence de garanties et de mesures appropriées pour le traitement des données peut entraîner la perte de données, leur divulgation accidentelle à une partie non autorisée ou leur vol. Des pratiques appropriées de traitement des données sont donc essentielles pour chaque projet, et il incombe à tous les membres de l'équipe de recherche de suivre des procédures pour réduire au minimum le risque d'une atteinte à la protection des données (EPTC 2, 2014).

Comprendre les données d'identification et les données anonymes

Les chercheurs peuvent chercher à recueillir, utiliser, partager et consulter différents types d'information sur les participants. Ces renseignements peuvent comprendre des caractéristiques personnelles ou d'autres renseignements au sujet desquels une personne peut raisonnablement s'attendre à ce que sa vie privée soit protégée. Avant d'acquérir leurs données, les chercheurs devraient déterminer le type de données qu'ils utilisent au moment de planifier des mesures pour protéger ces données (voir le Tableau 1 pour plus de détails). L'EPTC 2 (2014) précise les cinq catégories suivantes pour évaluer la mesure dans laquelle l'information peut être utilisée pour identifier un participant.

- **Renseignements permettant l'identification directe** – Renseignements servant à l'identification de la personne par des identificateurs directs (le nom, le numéro d'assurance sociale ou le numéro personnel du régime de santé, par exemple).
- **Renseignements permettant l'identification indirecte** – Renseignements dont on présume qu'ils peuvent aider à identifier une personne par une combinaison d'identificateurs indirects (par exemple, la date de naissance, le lieu de résidence et des caractéristiques personnelles distinctives).
- **Renseignements codés** – Renseignements dont on a retiré les identificateurs directs pour les remplacer par un code. Selon le degré d'accès à ce code, on sera en mesure de réidentifier des participants (par exemple, dans le cas où le chercheur principal conserve une liste associant le nom de code des participants à leur nom véritable, ce qui permet de les relier à nouveau au besoin).
- **Renseignements rendus anonymes** – Renseignements dans lesquels les identificateurs directs sont irrévocablement retirés et pour lesquels **aucun code** permettant une future réidentification n'est conservé. Le risque de réidentification des personnes à partir des identificateurs indirects restants est faible ou très faible.
- **Renseignements anonymes** – Renseignements auxquels aucun identificateur n'a jamais été associé (enquêtes anonymes, par exemple). Le risque d'identification des personnes est faible ou très faible.

L'EPTC 2 explique comment les préoccupations éthiques concernant la protection de la vie privée diminuent à mesure qu'il devient plus difficile (ou impossible) d'associer des renseignements à une personne en particulier. Ces préoccupations varient également en fonction de la sensibilité des renseignements et de la mesure dans laquelle l'accès, l'utilisation ou la communication peuvent nuire à une personne ou à un groupe. La façon la plus simple de protéger les participants est de recueillir et d'utiliser des données anonymes ou rendues anonymes, bien que cela ne soit pas toujours possible ou souhaitable. Si l'information d'identification doit être rendue anonyme, il faut le faire le plus tôt possible après son acquisition, et bien souvent dans la plus grande mesure possible (à noter que les données n'ont pas toujours besoin d'être automatiquement dépersonnalisées; la décision de dépersonnaliser ou d'anonymiser les données dépend de facteurs comme ce à quoi les participants peuvent avoir consenti, le degré de sensibilité des données, etc.

Les données peuvent également être rendues anonymes en regroupant (et recodant) les données brutes en groupes à l'intérieur d'une certaine plage. Par exemple, les renseignements permettant une identification indirecte peuvent inclure une valeur aberrante telle qu'un âge de 89 ans, dans un contexte où l'âge moyen des participants est de 34 ans. Le regroupement de ces données dans une catégorie « 65 ans et plus » permet de masquer l'identité associée à la valeur aberrante. Cette forme d'anonymisation est pratique courante dans des organismes comme Statistique Canada, qui produit des fichiers de microdonnées à grande diffusion. La Bibliothèque de l'Université d'Ottawa offre quelques recommandations pour l'anonymisation des données et même des liens vers un outil d'aide (en anglais) à l'anonymisation (complément à MS Word) que pourraient trouver utiles les chercheurs utilisant des données qualitatives.

Lorsqu'il n'est pas possible d'utiliser des données anonymes ou rendues anonymes aux fins de la recherche (et il existe de nombreuses raisons pour lesquelles des données peuvent devoir être recueillies et conservées sous une forme identifiable), l'obligation éthique de confidentialité et le recours à des mesures appropriées pour protéger les renseignements deviennent primordiaux. On s'attend à ce que les chercheurs consultent leur CER s'ils ne sont pas certains que les données dont la collecte est proposée pour la recherche sont identifiables.

Aux États-Unis, la *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* considère que les données sont dépersonnalisées si **tous** les éléments suivants sont supprimés des données :

1. Noms.
2. Toutes les subdivisions géographiques plus petites qu'un État, y compris l'adresse municipale, la ville, le comté, la circonscription, le code postal et les géocodes équivalents, à l'exception des trois premiers chiffres du code postal si, selon les données publiques du Bureau du recensement actuellement disponibles :
    a. l'unité géographique formée en combinant tous les codes postaux comportant les mêmes trois chiffres initiaux contient plus de 20 000 personnes; et
    b. les trois premiers chiffres d'un code postal pour toutes les unités géographiques contenant 20 000 personnes ou moins sont remplacés par « 000 ».
3. Tous les éléments des dates (sauf l'année) dans le cas des dates directement liées à une personne, y compris la date de naissance, la date d'admission, la date de sortie, la date du décès, ainsi que tous âges supérieurs à 89 ans et tous éléments de dates (y

compris l'année) indiquant un tel âge, sauf que ces âges et éléments peuvent être regroupés dans une catégorie unique de « 90 ans ou plus ».

4. Numéros de téléphone.
5. Numéros de télécopieur.
6. Adresses de courrier électronique.
7. Numéros d’assurance sociale.
8. Numéros de dossier médical.
9. Numéros des bénéficiaires du régime d'assurance-maladie.
10. Numéros de compte.
11. Numéros de certificat ou de licence.
12. Identificateurs et numéros de série des véhicules, y compris les numéros de plaque d'immatriculation.
13. Identificateurs et numéros de série des appareils.
14. Localisateurs de ressources universelles Web (URL).
15. Numéros d'adresse IP (protocole Internet).
16. Identificateurs biométriques, y compris les empreintes digitales et vocales.
17. Photos de l'ensemble du visage et toutes images similaires.
18. Tout autre numéro d'identification, caractéristique ou code unique, à moins que la règle de confidentialité ne l'autorise autrement aux fins de la réidentification.

Selon l'HIPAA, les données ne sont pas considérées comme totalement anonymes à moins que toutes les informations ci-dessus ne soient supprimées d'un document. Toutefois, de façon générale, dans le contexte canadien, s’il y a par exemple un « grand » échantillon au niveau de la province et de la ville, l'information géographique à une échelle inférieure à celle de la province (p. ex., au niveau de la ville) peut être admissible.

Évaluation du risque associé aux données à recueillir, traiter ou stocker

Une première étape de la planification de la collecte, du traitement et du stockage sécuritaires des données consiste à déterminer le type de données recueillies et les risques associés à ces données. En nous fondant sur les cinq niveaux de sécurité des données de la *Harvard Information Security Policy* (Université Harvard, s.d., en anglais), nous avons établi quatre niveaux de risque associés aux données de recherche. Lorsqu'ils recueillent des données, les chercheurs devraient se limiter à ne recueillir que la quantité minimale de renseignements personnels et identifiables nécessaires à l'atteinte des objectifs de la recherche. La collecte de renseignements personnels non pertinents aux objectifs de la recherche peut inutilement accroître le niveau de risque d’une possible violation de la confidentialité, ce qui peut rendre les participants vulnérables à un risque accru de préjudice. Ce qui suit s'applique aux situations où,

compte tenu des conditions de participation à la recherche, les renseignements des participants ne seraient pas rendus publics et la confidentialité serait maintenue.

Données de recherche confidentielles à faible risque.

Les données de recherche confidentielles sont des renseignements qui, dans leur forme actuelle, ne causeraient pas de préjudice à une personne ou à un groupe s'ils étaient divulgués, mais que les chercheurs ont néanmoins décidé de garder confidentielles. Les informations à ce niveau peuvent inclure des informations anonymes, des informations anonymisées ou des informations codées qui, si elles étaient décodées et divulguées, ne causeraient pas de préjudice grave au participant.

Voici quelques exemples :

- Données d'enquête anonymes
- Données entièrement anonymisées (voir les lignes directrices sur l'anonymisation ci-dessous)
- Propriété intellectuelle non publiée (p. ex., ébauches de manuscrits)

Renseignements confidentiels de nature délicate.

Les renseignements confidentiels de nature délicate sont des renseignements qui, s'ils sont divulgués sous leur forme actuelle, risquent vraisemblablement de nuire à la réputation d'une personne ou de la mettre dans l'embarras. L'information à ce niveau peut comprendre des données à faible risque qui n'ont pas encore été rendues anonymes, ainsi que des renseignements codés qui, s'ils étaient décodés et divulgués, pourraient causer un préjudice grave au participant.

Voici quelques exemples :

- Numéros de compte bancaire
- Dossiers scolaires (p. ex., relevés de notes)
- Renseignements fournis à titre confidentiel (renseignements que le répondant croit fournir à titre confidentiel et confirmés comme tels)

Renseignements dont la divulgation causerait vraisemblablement un préjudice

Les renseignements à ce niveau comprennent l'information qui, si elle est divulguée, pourrait créer un risque de préjudice social, psychologique, réputationnel, financier, juridique ou autre pour une personne ou un groupe. Ce niveau peut comprendre des données qui n'ont pas encore été rendues anonymes ou qui ne peuvent l'être parce que des renseignements confidentiels sont nécessaires à l'analyse, mais qui, si elles sont divulguées, peuvent causer du tort au participant.

Voici quelques exemples :

- Renseignements sur la carte d'assurance-maladie
- Diagnostic de maladie mentale ou physique
- Numéros de carte de crédit

Renseignements dont la divulgation causerait un préjudice grave

Les renseignements à ce niveau comprennent l'information qui, si elle est divulguée, pourrait entraîner des risques de responsabilité criminelle, de perte d'emploi ou de préjudice grave pour une personne ou un groupe. Ce niveau est réservé aux données de nature très sensible, lesquelles devraient être rendues anonymes dès que possible. Les informations hautement confidentielles qui ne peuvent pas être totalement anonymisées parce qu'elles sont nécessaires à l'analyse doivent être traitées avec le plus grand soin.

Voici quelques exemples :

- Numéro d'assurance sociale
- Informations sur des activités illégales

Acquisition, manipulation et stockage de données comportant différents niveaux de risque

Le Tableau 1 donne un aperçu des étapes recommandées pour l'acquisition, la manipulation et le stockage des données en fonction des différents niveaux de risque décrits ci-dessus. Ces lignes directrices sont fondées sur les recommandations énoncées dans la *Harvard Information Security Policy* et sur des consultations auprès des experts en sécurité des données de l'Université d'Ottawa. Ce tableau a été conçu comme un outil pour aider les chercheurs à décider des mesures à prendre pour sécuriser leurs données. Au bout du compte, c'est à la chercheure ou au chercheur de juger du niveau de risque associé à ses données. Il est important de noter que les données peuvent passer d'une catégorie de risque à une autre aux différentes étapes d'un projet de recherche. Le plus souvent, il s'agira d'une diminution du niveau de risque (p. ex. une base de données contenant les noms et les numéros de carte d'assurance-maladie des participants pourra d'abord être de niveau 3, mais passer au niveau 2, voire au niveau 1, une fois les données rendues entièrement anonymisées).

Dans les sections suivantes, nous décrivons les mesures particulières qui peuvent être prises et qui conviennent aux diverses étapes du processus de recherche, de l'étape de l'acquisition des données à celle du stockage.

Tableau 1 : Niveaux de risque et mesures correspondantes pour le traitement sécuritaire des données

Niveau de risque	Étapes pour sécuriser les données
4 Renseignements dont la divulgation causerait un préjudice grave Si ces renseignements étaient divulgués, ils pourraient créer un risque de responsabilité criminelle, de perte d'emploi ou de préjudice grave à une personne ou à un groupe. Ce niveau est réservé aux données de nature très sensible, lesquelles devraient être anonymisées dès que possible. Les informations hautement confidentielles qui ne peuvent pas être totalement anonymisées parce qu'elles sont nécessaires à l'analyse doivent être traitées avec le plus grand soin.	Collecte sur le terrain : Les données doivent être recueillies sur un dispositif chiffré et protégé par mot de passe. Il est déconseillé d'utiliser du papier, mais s'il est utilisé, il doit être manipulé avec le plus grand soin et ne pas être laissé sans surveillance, sauf dans un environnement verrouillé et sécurisé. Stockage : Les données doivent être stockées dans une pièce physiquement verrouillée (de préférence sécurisée par une alarme) sur un disque dur protégé par mot de passe et chiffré ou sur un ordinateur protégé par mot de passe non connecté à un réseau informatique. Partage : Le partage à ce niveau devrait être limité, et les données n'être accessibles que dans un endroit sûr. Accès : Contrôlé par le chercheur principal, qui tient une liste des personnes à qui l'accès a été accordé.
3 Renseignements dont la divulgation causerait vraisemblablement un préjudice Si ces renseignements étaient divulgués, ils pourraient créer un risque de préjudice social, psychologique, réputationnel, financier, juridique ou autre pour une personne ou un groupe. Ce niveau peut comprendre des données qui n'ont pas encore été rendues anonymes ou qui ne peuvent pas l'être complètement parce que des renseignements confidentiels sont nécessaires à l'analyse et que leur divulgation à une partie non autorisée pourrait causer un préjudice au participant.	Collecte sur le terrain : Les données doivent être recueillies sur un dispositif chiffré et protégé par mot de passe. Il est déconseillé d'utiliser du papier, mais s'il est utilisé, il doit être manipulé avec le plus grand soin et ne pas être laissé sans surveillance, sauf dans un environnement verrouillé et sécurisé. Stockage : Les données doivent être chiffrées et protégées par mot de passe. Partage : Les données ne doivent pas être partagées par courriel. Les fichiers doivent être chiffrés lors de l'utilisation de Docushare. Accès : Devrait être contrôlé par le chercheur principal, qui tient une liste des personnes ayant obtenu l'accès.
2 Renseignements confidentiels de nature délicate S'ils sont divulgués sous leur forme actuelle, on peut raisonnablement s'attendre à ce qu'il y ait atteinte à la réputation d'une personne ou à ce que celle-ci se retrouve dans l'embarras. L'information à ce niveau peut comprendre des données à faible risque qui n'ont pas encore été anonymisées ou des renseignements codés qui, s'ils étaient décodés et divulgués, pourraient causer un préjudice grave au participant.	Collecte sur le terrain : Les données doivent être stockées sur un dispositif protégé par mot de passe. Stockage : Les données doivent être protégées par mot de passe, et le chiffrement est recommandé. Partage : Les fichiers envoyés par courrier électronique doivent être protégés par mot de passe et chiffrés. Le mot de passe doit être envoyé sur un autre support. L'utilisation de Docushare est cependant préférable au courriel.

1 Renseignements confidentiels de recherche à faible risque Renseignements qui, dans leur forme actuelle, ne causeraient pas de préjudice à une personne ou un groupe s'ils étaient divulgués, mais dont les chercheurs ont néanmoins décidé de restreindre l'accès. Cela peut inclure des informations anonymes, des informations entièrement anonymisées ou des informations codées qui, si elles étaient décodées et divulguées, ne causeraient pas de préjudice grave au participant.	Stockage : Les données doivent être stockées sur un ordinateur ou un lecteur protégé par mot de passe. Partage : Il est recommandé que les fichiers envoyés par courriel soient protégés par un mot de passe. Le mot de passe devrait être envoyé sur un autre support.

Note : Les niveaux de risque sont une adaptation de la politique de sécurité des données de recherche de l'Université Harvard.

Collecte de données

La collecte de données auprès de participants humains constitue un aspect important de la recherche et de l'évaluation. Les chercheurs principaux du CRSEC peuvent travailler avec deux types de données.

Les données primaires comprennent les données recueillies directement auprès des participants à des projets de recherche ou d'évaluation. Étant donné que la collecte de données vise souvent des renseignements confidentiels, les chercheurs devraient s'efforcer de disposer des moyens les plus sûrs pour recueillir ces données. Comme les enquêtes sur papier peuvent être perdues, il est recommandé de recueillir les données à l'aide de dispositifs plus sûrs, protégés par mot de passe et chiffrés (p. ex. ordinateurs portables ou tablettes; notez que les produits Apple sont généralement plus sûrs, que les iPads ont un chiffrement par défaut solide et que les autres tablettes peuvent être moins sûres). De plus, une tablette ou un appareil mobile n'est considéré comme sécurisé que s'il est protégé par un mot de passe fort et si seules des applications correctement validées sont installées (c'est-à-dire uniquement des applications certifiées provenant d'un magasin d'applications officiel).

Les données secondaires sont des données qui ont été recueillies à l'origine par un organisme communautaire, un hôpital ou un autre établissement et qui sont ensuite transférées aux chercheurs du CRSEC pour analyse.

L'utilisation des deux types de données doit se faire dans le respect des principes de protection de la vie privée, de confidentialité et de sécurité des données. À cet égard, les recommandations suivantes sont formulées.

Recommandations concernant la collecte de données primaires

- Toujours s'assurer que tous les projets de recherche impliquant des participants humains ou l'utilisation de leurs données ont reçu toutes les approbations requises du CER de l'Université d'Ottawa.

- Au besoin, s'assurer d'avoir obtenu le consentement de chaque participant à la recherche quant à la collecte de renseignements personnels, à leur utilisation et aux fins auxquelles ces renseignements sont recueillis. Chaque participant a le droit de savoir ce à quoi il consent et de choisir s'il veut participer.

- Au moment de recueillir des données, toujours s'assurer de ne recueillir que les données dont vous avez besoin et, une fois ces données recueillies et stockées en toute sécurité, ne retirez pas les données de votre lieu de travail sécurisé, sauf en cas de nécessité absolue. Si vous travaillez sous supervision, l'enlèvement des données doit se faire au su de votre superviseur.

- L'Université d'Ottawa fournit des lignes directrices utiles pour assurer la protection des dossiers lorsqu'ils doivent emmenés hors du campus. Voici des exemples.

    - Les dossiers conservés sur un appareil électronique portatif (p. ex., un ordinateur bloc-notes) ne devraient jamais être laissés sans surveillance. Lorsqu'ils ne sont pas utilisés, ils devraient être entreposés en lieu sûr.

- Un appareil électronique portable contenant des données devrait être protégé par un mot de passe et chiffré.

- Les mots de passe ne doivent pas être faciles à deviner, et ils doivent rester confidentiels.

Recommandations concernant l'acquisition de données secondaires

- Toujours s'assurer que tous les projets de recherche impliquant des participants humains ou l'utilisation de leurs données ont reçu toutes les approbations requises du CER de l'Université d'Ottawa.

- Toujours s'assurer que tous les projets comportant l'utilisation de données agrégées obtenues de partenaires de recherche (comme les hôpitaux et les organismes gouvernementaux) ont été approuvés par les autorités compétentes du partenaire de recherche et que les consentements requis ont été obtenus du partenaire de recherche et, si nécessaire, des participants individuels, pour la divulgation des données aux chercheurs du CRSEC.

- Ne jamais accepter de données contenant des renseignements d'identification, à moins que ces renseignements ne soient absolument nécessaires au projet et que des mesures appropriées ne soient mises en place pour protéger la confidentialité des données, y compris la protection par mot de passe et le chiffrement des fichiers. Lorsqu'il n'est pas nécessaire de fournir des renseignements d'identification, demander aux partenaires de recherche de les expurger des données avant de transmettre celles-ci aux chercheurs du CRSEC.

- Dans certains cas, le CER de l'Université d'Ottawa a renoncé à l'approbation déontologique pour l'accès aux données secondaires au niveau des dossiers, lorsque les mesures de protection des données en place étaient jugées entièrement conformes aux lois régissant la protection et la confidentialité des données. Les fichiers de microdonnées à grande diffusion fournis par Statistique Canada et disponibles sur odesi.ca ou archivés par l'*Inter-University Consortium of Political and Social Research*, ou CIPRSS (Consortium interuniversitaire de recherche politique et sociale) ne nécessitent aucun processus préalable d'approbation ou de renonciation du CER de l'Université d'Ottawa.

Utilisation, manipulation et transport des données

Le CRSEC compte des chercheurs et des membres du personnel qui travaillent à divers titres à différents projets de recherche. Les données de ces nombreux projets doivent à l'occasion être recueillies à l'extérieur du site et peuvent devoir être retournées au CRSEC et sécurisées après les heures normales de bureau. De plus, du fait de contraintes de ressources et d'espace et compte tenu du grand nombre de chercheurs, les ordinateurs et les bureaux sont souvent partagés entre de nombreux chercheurs du CRSEC. Comme dans le cas de l'acquisition des données, ci-dessus, ces questions présentent des défis qu'il faut relever avec des solutions qui assurent le respect des principes de la vie privée, de la confidentialité et de la sécurité des données. À ce titre, les recommandations suivantes sont formulées.

Recommandations concernant l'utilisation et la manipulation des données

- Minimiser l'utilisation de données contenant des renseignements d'identification. Pour limiter le plus possible le risque de violation accidentelle de la confidentialité :
    - dans la mesure du possible, utiliser un ensemble de données anonymisées ou anonymes;
    - lorsque des données d'identification sont nécessaires, toujours conserver les renseignements d'identification dans une liste d'identification distincte (p. ex. une feuille de calcul ou une base de données contenant des codes d'identification uniques);
    - l'assurer que les ordinateurs et les fichiers sont protégés par mot de passe et chiffrés.
- N'utiliser les données qu'aux fins approuvées.
- Ne jamais procéder à l'entrée de données en dehors des espaces prescrits à cette fin. Le déplacement de copies papier des données dans le CRSEC augmente le risque de violation accidentelle de la confidentialité;
- Entreposer en toute sécurité les documents papier dans des classeurs verrouillés, dans des bureaux fermés à clé dont l'accès est limité aux membres du personnel.
- Le traitement des données (p. ex. les données d'enquête) sur support papier est déconseillé. Les outils de collecte de données électroniques sécurisés (chiffrés et protégés par mot de passe), tels que les ordinateurs portables ou les tablettes, sont préférables.
- Ne jamais partager ses identifiants d'authentification personnels (ID utilisateur, mots de passe, etc.) et ne jamais utiliser ses identifiants pour donner à une autre personne l'accès à des systèmes d'information ou des ordinateurs contenant des informations confidentielles.

Partage de données

- Les chercheurs ne devraient partager les données qu'avec des groupes et chercheurs externes approuvés et devraient s'assurer d'utiliser une méthode de partage suffisamment sûre.

    - Les courriels ne sont pas sécurisés par nature et le chiffrement des courriels est très difficile et souvent peu pratique. Il est recommandé aux chercheurs d'utiliser DocuShare, qui offre un moyen plus sûr de partager des fichiers, bien que les informations confidentielles affichées sur Docushare doivent être chiffrées. Le stockage en nuage (p. ex., DropBox, Google Drive) ne devrait pas être utilisé pour le stockage ou le partage de données confidentielles. Bien que le courriel ne devrait pas être utilisé pour le partage de données confidentielles, il peut l'être pour communiquer avec des chercheurs ou des participants, ou pour partager des données anonymes à très faible risque.

    - Les clés USB ne devraient pas être utilisées, à moins que les données ne soient considérées comme présentant un risque très faible, car les clés USB peuvent facilement être perdues ou égarées, et même après la suppression des données, il existe des moyens de les récupérer, ce qui rend très difficile la suppression définitive des données d'une telle clé. Lorsqu'une clé USB est utilisée, les fichiers de données doivent être chiffrés et protégés par mot de passe.

    - Ne communiquer des données confidentielles à des groupes externes approuvés qu'après avoir obtenu l'autorisation de la source originale et, le cas échéant, l'approbation du CER.

    - Ne communiquer les données aux organismes qu'après avoir confirmé le caractère adéquat de leurs politiques en matière de protection de la vie privée, de confidentialité et de sécurité des données.

    - S'assurer que les organismes reconnaissent par écrit leur responsabilité et celle du CRSEC de préserver la confidentialité de tous les renseignements échangés.

Transport de données

- Éviter, dans la mesure du possible, de sortir des données hors des locaux du CRSEC, que ce soit sur papier ou sous forme électronique.

- Lors du transport de données, toujours assurer la sécurité des données recueillies hors site, ce qui suppose de :

    - ne jamais laisser des données sans surveillance ou dans des endroits non sûrs (p. ex. une voiture verrouillée), car cela augmente le risque de violation accidentelle de la confidentialité;

    - s'assurer que les ordinateurs et les fichiers sont protégés par un mot de passe;

    - veiller à ce que les données électroniques qui contiennent des renseignements d'identification soient chiffrées.

- Ne jamais sortir des locaux du CRSEC une liste d'identification ou d'autres renseignements d'identification.
- Ne jamais transporter des listes d'identification ou toute autre donnée ou information permettant d'identifier des personnes à partir d'un ensemble de données rendues anonymes en même temps que les données rendues anonymes.
- Toujours apporter les données recueillies hors site au CRSEC le plus tôt possible. En toutes circonstances, veiller à ce que ces données soient dépersonnalisées dès que possible.
- Si les données recueillies hors site ne peuvent être transmises directement au CRSEC, il faut appliquer les mesures de sécurité précitées. Les chercheurs travaillant sous supervision devraient toujours obtenir l'approbation écrite préalable de leur superviseur concernant le traitement des données et les procédures de sécurité.

Stockage de données

Les mesures suivantes doivent être prises lorsque des données très confidentielles sont stockées. Ces mesures seront probablement prises aux premières étapes du processus de recherche, avant que les données puissent être rendues anonymes.

Étape 1 : Trouver un ordinateur propre / créer un environnement sûr

D'abord et avant tout, il est essentiel que les ordinateurs soient à jour. Les fournisseurs de systèmes publient régulièrement des mises à jour du système d'exploitation pour protéger les utilisateurs contre les vulnérabilités que les pirates informatiques ont identifiées et exploitées.

Ensuite, il est important d'analyser les ordinateurs à la recherche de logiciels malveillants. Les ordinateurs sont facilement infectés par des logiciels malveillants. Même des sites Web dignes de confiance comme celui d'une agence de presse réputée peuvent, à l'insu des propriétaires, héberger des publicités infectées par des logiciels malveillants. Par conséquent, il est préférable qu'un ordinateur qui traite des données confidentielles (c.-à-d. des données préanonymisées) soit utilisé uniquement pour le traitement des données. Pour être considéré comme sûr, un ordinateur doit d'abord faire l'objet d'un scan visant à détecter les logiciels malveillants, et si des menaces sont détectées, elles doivent être rapidement nettoyées ou supprimées. Sophos Home a été recommandé par les experts en sécurité des données de l'Université d'Ottawa.

Étape 2 : Protéger et chiffrer

Une fois qu'un ordinateur a été scanné et que toutes les menaces ont été éliminées, un chercheur peut charger des données confidentielles sur l'ordinateur (c.-à-d. les enregistrements d'entrevues, les données non anonymisées, etc.). Une fois cela fait, il est recommandé de chiffrer l'ensemble du disque dur de l'ordinateur et de chiffrer les fichiers individuels (voir la section Ressources pour connaître les logiciels de chiffrement).

Étape 3 : Suppression permanente des fichiers

Les fichiers contenant des informations confidentielles ne doivent jamais être supprimés à l'aide des « corbeilles » standard installées sur les ordinateurs pour « supprimer » des fichiers. Cela ne fait que supprimer le répertoire de fichiers. Les fichiers mêmes et leur contenu sont toujours stockés physiquement sur le disque dur de l'ordinateur et restent accessibles. Des applications de « déchiquetage de fichiers » peuvent être utilisées pour supprimer définitivement des fichiers. Ces programmes écrasent les fichiers avec des lettres et/ou des chiffres aléatoires, souvent plusieurs fois, avant de les supprimer. Il est important de noter que cela s'applique aux fichiers qui contiennent des renseignements confidentiels et qui ne sont plus nécessaires, conformément à l'approbation du CER (p. ex. un enregistrement audio qui a été transcrit.) Un fichier qui a été rendu anonyme et qui servira plus tard à la recherche n'a pas besoin d'être détruit; il peut simplement être protégé par mot de passe et chiffré.

Créer un mot de passe fort pour protéger les comptes et les documents

Tous les mots de passe ne présentent pas le même degré de sécurité. Si un mot de passe n'est pas assez fort, le chiffrement n'aura pas d'importance. Un individu peut facilement contourner un mot de passe faible à l'aide d'une des nombreuses applications d'attaque par la force brute (*brute-force*) facilement accessibles en ligne. Ces applications peuvent deviner un mot de passe faible en quelques minutes, voire quelques secondes. Il est également important de ne jamais stocker un mot de passe sur le même ordinateur sur lequel des données confidentielles sont stockées, sauf si elles sont stockées dans un gestionnaire de mots de passe sécurisé (voir les exemples ci-après).

Un logiciel peut être utilisé pour essayer rapidement d'innombrables mots de passe possibles. Ces logiciels font l'objet d'améliorations constantes visant à tenir compte des mots de passe formés de :

- mots du dictionnaire;
- mots épelés à l'envers;
- renseignements personnels tels que noms, dates de naissance, noms de rues locales, etc.

L'Université d'Ottawa fournit des lignes directrices pour le choix de mots de passe plus forts. Voici un résumé de certaines de ces lignes directrices.

- Longueur : au moins 10 caractères (cela prendra plus de temps au pirate pour le déchiffrer)
- Complexité : au moins trois lettres majuscules / minuscules, des chiffres et des caractères spéciaux
- Variation : changer le mot de passe au moins tous les trois mois
- Variété : utiliser un mot de passe différent pour chaque site fréquenté (c'est-à-dire différents sites = différents mots de passe).

Si vous n'êtes pas sûr si votre mot de passe est fort, il existe différentes ressources en ligne pour en vérifier la force. Il existe également des générateurs de mots de passe aléatoires que certains chercheurs pourront trouver utiles.

Il peut être difficile de se remémorer des mots de passe forts. En fait, si les mots de passe sont suffisamment forts, il devrait être presque impossible de les retenir tous. Un gestionnaire de mots de passe peut être un outil utile pour garder une trace de tous les mots de passe compliqués. Voici une liste de gestionnaires de mots de passe (tous sont gratuits ou incluent une version gratuite) recommandés par l'architecte en sécurité de l'Université d'Ottawa :

- Dashlane
- KeePass (logiciel ouvert)
- Sticky Password
- LastPass
- Password Safe (logiciel ouvert)
- Gestionnaire de mots de passe RoboForm
- SplashData SplashID

Parmi les options ci-dessus, nous recommandons LastPass, qui offre un outil de génération de mot de passe complexe et le remplissage automatique des formulaires et des identifiants et mots de passe, est disponible pour les systèmes d'exploitation Windows et Mac, et peut également être téléchargé sur téléphone intelligent (y compris pour iOS d'Apple et Android). LastPass est gratuit, mais la version Premium est très abordable, à 2 $ par mois. La version premium inclut la possibilité de partager des mots de passe avec d'autres personnes grâce à la fonction de « Partage avec plusieurs » et 1 Go de stockage en nuage chiffré gratuit. LastPass est facile à utiliser et enregistre et mémorise automatiquement les mots de passe lorsque l'on se connecte à son compte sur son ordinateur ou son smartphone, et il inclut même un outil automatique de changement de mot de passe (en anglais). De nombreux tutoriels sont disponibles en ligne.

Recommandations supplémentaires concernant le stockage des données

- Veiller à toujours stocker les données et les listes d'identification sur des ordinateurs « sûrs ». La protection par mot de passe, le chiffrement des données, les pare-feu, la mise à jour de la protection antivirus et un nombre restreint d'utilisateurs réduiront au minimum le risque de violation accidentelle de la confidentialité.
- Éviter dans la mesure du possible de stocker des données confidentielles sur support papier. Si cela n'est pas possible, s’assurer que les documents papier sont stockés dans un environnement sécurisé et verrouillé.
- Ne jamais stocker de données anonymes au même endroit que des listes d'identification ou d'autres renseignements d’identification.

- Retirer toute information confidentielle lorsqu'elle n'est plus nécessaire et s'assurer qu'elle est correctement effacée de tout support de stockage électronique (y compris les supports portables) ou, si elle est sur papier, détruite de façon sécuritaire.

- Toujours archiver les données en fonction des besoins. Conserver les anciennes données dans un endroit sûr pendant une durée appropriée. Les besoins de préservation des données au-delà de la durée de vie d'un projet et des publications de recherche devraient être pris en compte. Il faut se demander si les données seront nécessaires à des fins de reproduction, de documentation supplémentaire ou de référence. Ces considérations et certaines autres, soulevées dans la Déclaration de principes des trois organismes sur la gestion des données numériques, pourraient nécessiter de prendre en compte un horizon allant au-delà des cinq années suivant l'achèvement d'un projet de recherche.

- Dans la mesure du possible, stocker les fichiers dans plus d'un format. Les fichiers QDA Miner et SPSS peuvent également être enregistrés au format Excel. Ceci est également utile si les données sont partagées avec un autre chercheur qui n'a peut-être pas QDA Miner. Alors que les données des progiciels tels que SPSS et QDA Miner peuvent être exportées et sauvegardées au format Excel, d'autres comme celles de NVivo ne peuvent pas être exportées.

L'Université d'Ottawa met de l'avant certaines pratiques exemplaires, dont les suivantes.

- L'utilisation d'espaces et de caractères spéciaux (?, &, !) est déconseillée au moment de nommer les fichiers. Les traits d'union, les tirets de soulignement et les majuscules constituent de meilleurs choix pour séparer les éléments d'un nom de fichier. Le nom d'un fichier doit comprendre des renseignements clés sur le projet, comme l'étape où en est le projet, l'équipe de recherche qui travaille sur le projet, la langue utilisée dans le fichier, etc. (on trouvera un complément d'information sur la structure des fichiers et des dossiers ici (en anglais))

    - Exemples : Liste-Codes-Projet-Logement-Dec2016
Proposition_Recherche_CRSEC2_Fr

- Les formats de fichiers doivent être soigneusement choisis en gardant à l'esprit la possibilité de partage et l'accès à long terme (voir ici la liste des formats de fichiers privilégiés).

- Afin de réduire au minimum le risque de travailler accidentellement sur une version désuète d'un fichier, les chercheurs sont encouragés à pratiquer le « versionnage des fichiers ». Voici quelques méthodes suggérées :

    - Inclure des informations sur la version dans le nom du fichier ainsi que dans le document;

    - L'utilisation de la numérotation séquentielle est encouragée (p. ex. 0.1, 0.2, 0.3 pour les ébauches; 1.0 pour une version finale; 1.1, 1.2 peuvent signifier des révisions à une version finale jusqu'à la version 2.0).

- Les données doivent être sauvegardées régulièrement, et un calendrier de sauvegarde périodique doit être suivi. Il est recommandé de sauvegarder régulièrement au moins trois copies séparées géographiquement, soit une copies originale, une copie externe locale (par exemple, disque dur externe dans une pièce verrouillée) et une copie externe distance (par exemple, sauvegarde à distance des données sur une plate-forme sécurisée et approuvée telle que DocuShare).

Formation et supervision

Le CRSEC est un centre multidisciplinaire qui emploie un grand nombre de chercheurs, y compris des employés, des étudiants postdoctoraux, des étudiants des cycles supérieurs et des étudiants de premier cycle ou avec spécialisation. Ainsi, les chercheurs qui commencent à travailler au CRSEC peuvent avoir des antécédents variés en matière d'éthique et de formation en recherche. Cette variété de connaissances fondamentales en éthique et en recherche indique que la formation joue un rôle important pour assurer que les principes de protection de la vie privée, de confidentialité et de sécurité des données sont respectés au CRSEC. De plus, le CRSEC fonctionne à la fois comme centre de recherche et comme centre de formation pour de nombreux étudiants de l'Université d'Ottawa. À ce titre, la supervision des chercheurs est importante pour assurer à la fois la qualité du travail et le respect des principes éthiques de la vie privée, de la confidentialité et de la sécurité des données. Afin d'assurer qu'une formation et une supervision adéquates sont offertes au CRSEC, les recommandations suivantes sont formulées.

Les employés et les étudiants qui auront accès aux données et les utiliseront doivent :

- lire le présent manuel sur la vie privée, la confidentialité et le stockage des données au CRSEC;

- suivre le Didacticiel sur l'Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains (EPTC 2) ainsi que tout programme de formation supplémentaire que l'Université d'Ottawa ou le CRSEC peut exiger de temps à autre pour assurer une connaissance de base en éthique de la recherche;

- remplir l'entente de confidentialité et de non-divulgation, fournie à l'Annexe 1, qui décrit les lignes directrices en matière d'éthique pour la protection des renseignements personnels, la confidentialité et le stockage des données au CRSEC.

Autres recommandations :

- La supervision de chaque projet doit inclure la surveillance des procédures liées à la protection de la vie privée ainsi qu'à la confidentialité et la sécurité des données.

- Toutes les questions d'éthique doivent être soulevées auprès d'un superviseur le plus tôt possible. Toutes les décisions éthiques doivent être prises en consultation avec un superviseur du CRSEC et être documentées dans le dossier du projet, avec l'approbation écrite du superviseur du CRSEC.

- Toute utilisation, tout accès ou toute perte non autorisés de renseignements confidentiels doivent être signalés dès que possible au superviseur immédiat (pour les personnes travaillant sous supervision) et au Bureau d'éthique et d'intégrité de la recherche, qui doit également être informé si l'information en question permet une identification directe.

Documentation des services

Avec les nombreux chercheurs du CRSEC qui travaillent à divers titres sur plusieurs projets de recherche, la documentation des services est essentielle au bon fonctionnement du CRSEC. S'assurer que les tâches sont exécutées correctement, que les principes d'éthique (liés notamment à la protection de la vie privée, la confidentialité et la sécurité des données) sont respectés et que le travail est mené à bien sont autant d'aspects importants du travail du CRSEC qui doivent être bien documentés. Pour garantir que les services sont bien documentés au CRSEC, les recommandations suivantes sont formulées.

1. Tous les services offerts aux clients institutionnels seront documentés conformément aux normes de l'OPO résumées précédemment dans le présent manuel (Ordre des psychologues de l'Ontario, 2005).

2. Chaque chercheur et superviseur doit tenir un dossier confirmant que les questions liées à la protection de la vie privée, à la confidentialité et à la sécurité des données ont fait l'objet de discussions par rapport au projet auquel il travaille et aux décisions qui ont été prises.

3. Dans le cas d'un travail sous supervision, toute dérogation aux lignes directrices relatives à la protection de la vie privée, à la confidentialité et à la sécurité des données doit être approuvée par écrit par le superviseur du CRSEC (et éventuellement par le CER).

Élaboration de plans de gestion des données

Un plan de gestion des données (PGD) est un aperçu, souvent sous forme écrite, qui résume la façon dont les données sont traitées avant, pendant et après un projet de recherche. L'utilité d'un plan de gestion des données (PGD) est reconnue dans la Déclaration de principes des trois organismes sur la gestion des données numériques, qui prévoit rendre obligatoires dans l'avenir les plans de gestion des données pour les demandes de subvention de recherche. L'élaboration d'un PGD peut aider à répondre à beaucoup des préoccupations soulevées dans le présent manuel et à mettre en œuvre bon nombre des recommandations énoncées ci-dessus. Il est fortement recommandé que les chercheurs du CRSEC élaborent un PGD avant d'entreprendre un nouveau projet. L'Université d'Ottawa a consacré une section de son site Web aux PGD afin d'aider les chercheurs à élaborer et adapter des PGD adéquats pour leur projet de recherche. On y trouve des conseils utiles, des exemples, des liens vers des articles pertinents et même un outil de PGD en ligne. Tel que le décrit ce site Web, un PGD

typique comprend des renseignements sur ce qui suit :

- Comment les données seront recueillies ou acquises
- Conventions et procédures à utiliser pour structurer, stocker, sauvegarder et préserver les données
- Attribution de la responsabilité de la production de la documentation ou des métadonnées
- Mesures de sécurité, le cas échéant, pour protéger les données confidentielles
- Dimensions juridiques, éthiques ou de propriété intellectuelle, le cas échéant, et la façon dont elles seront traitées
- Ressources nécessaires à la mise en œuvre du PGD

Le site Web sur les PGD de l'Université contient également une section sur le stockage à long terme (archivage) des données, où sont décrits les divers dépôts de données utilisés pour fournir l'infrastructure nécessaire au stockage et à l'archivage des données.

La bibliothèque de l'Université d'Ottawa offre de l'aide pour la préparation des PGD (rdm@uOttawa.ca).

Ressources

On trouvera ci-dessous une liste de ressources qui pourraient être utiles pour assurer la sécurité des données de recherche.

> *Nota* : Les liens vers les ressources peuvent cesser de fonctionner avec le temps ou peuvent évoluer vers d'autres logiciels (ou versions). La plupart des logiciels que nous recommandons offrent des fonctions de base, et il existe d'innombrables solutions de remplacement acceptables et une multitude d'options de didacticiels. Veuillez consulter le service des TI de l'Université d'Ottawa ou un bibliothécaire spécialisé en gestion de données pour obtenir de plus amples renseignements sur des ressources spécifiques.

Application de détection et de suppression de logiciels malveillants

Sophos Home est l'application que nous recommandons. Notez que la version « Home » est gratuite. L'Université d'Ottawa peut installer gratuitement Sophos Business sur les ordinateurs connectés au domaine de l'Université. Pour de plus amples renseignements, communiquez avec le Service des technologies de l'information.

Chiffrement

Le chiffrement complet d’un disque dur est très simple. Les utilisateurs d’ordinateurs Macintosh (Apple) peuvent utiliser FileVault, tandis que les utilisateurs Windows peuvent utiliser BitLocker. Ces logiciels sont installés par défaut sur la plupart des ordinateurs et peuvent être démarrés d'un simple clic. Nous attirons toutefois votre attention sur le fait que le chiffrement du disque

dur peut donner un faux sentiment de sécurité. Une fois connecté, le disque est déchiffré et accessible par un hacker. C'est pourquoi le chiffrement au niveau des fichiers est essentiel pour les données très sensibles.

Microsoft Word permet aux utilisateurs de chiffrer un fichier avec un mot de passe. Ce chiffrement est fort, mais il est important de ne pas oublier d'utiliser un mot de passe fort.

VeraCrypt (anciennement connu sous le nom de TrueCrypt) est recommandé pour un niveau plus élevé de chiffrement de fichiers. Il s'agit d'un logiciel de chiffrement à code source ouvert largement reconnu comme la référence en matière de chiffrement à code source ouvert. Très facile à utiliser, VeraCrypt crée un « conteneur » sécurisé à chiffrement fort, c'est-à-dire un fichier dans lequel les autres fichiers peuvent être stockés en toute sécurité.

Il est important de voir le Tutoriel du débutant (en anglais) avant d'utiliser le logiciel. Après quelques essais pratiques, les chercheurs verront que ce logiciel est très facile à utiliser. Il existe de nombreux autres guides étape par étape qui peuvent être trouvés en faisant une recherche sur Google.

Les dernières versions d'autres logiciels (par exemple, SPSS) ont également des capacités de chiffrement, et il existe de nombreux tutoriels et guides pratiques faciles à trouver sur Google.

Suppression permanente de fichiers

File Shredder est une application très simple à utiliser et efficace pour les utilisateurs Windows.

Les utilisateurs Mac peuvent utiliser des applications comme Incinerator ou Permanent Eraser. Ce dernier est gratuit, et Incinerator ne coûte que 1 $. La plupart préfèrent Incinerator car il est plus facile à utiliser (il suffit de glisser-déposer le fichier que vous voulez supprimer sur l'icône dans votre panneau de contrôle). De son côté, Permanent Eraser efface tout dans sa corbeille. Cependant, des applications plus puissantes comme AweEraser peuvent être nécessaires pour supprimer des fichiers plus volumineux.

Glossaire

Anonymisation – Processus consistant à modifier de façon permanente des données pour en retirer les renseignements d'identification de manière à assurer la protection de la vie privée. Dans le cas des échantillons de données, cela comprend des méthodes pour supprimer les valeurs aberrantes et pour agréger et recoder les renseignements d'identification, comme l'âge exact des participants, le revenu, les groupes professionnels et les adresses.

Chiffrement – Processus consistant à encoder l'information de manière à ce que seules les personnes autorisées puissent y avoir accès. Pour accéder à un fichier chiffré, une personne devra posséder une « clé » générée par un algorithme complexe. Cette clé est accessible à l'aide d'un mot de passe.

Confidentialité – Responsabilité éthique et/ou légale des individus ou des organisations de protéger l'information qui leur est confiée contre l'accès, l'utilisation, la divulgation, la modification, la perte ou le vol non autorisés. (EPTC 2)

Dépersonnalisation – Processus consistant à retirer des données les renseignements d'identification dans le but de protéger la vie privée. Les données peuvent tout de même être repersonnalisées. Les identificateurs directs sont supprimés de l'information et remplacés par un code, et une liste maîtresse des codes et identités est conservée.

Logiciel malveillant – Terme désignant tout logiciel conçu pour perturber le fonctionnement normal d'un ordinateur, recueillir des informations sensibles ou permettre à un tiers non autorisé d'accéder à un ordinateur infecté.

Renseignements confidentiels (ou données confidentielles) – S'entend de l'information protégée en raison de considérations d'exclusivité, éthiques ou de protection de la vie privée. (Règlement sur la classification et la manutention de l'information de l'Université d'Ottawa).

Renseignements personnels – Renseignements dont on peut raisonnablement s'attendre à ce qu'ils permettent d'identifier une personne, seuls ou en combinaison avec d'autres renseignements disponibles. Ils sont également appelés des renseignements permettant l'identification (EPTC 2).

Utilisation secondaire (données secondaires) – Utilisation de renseignements ou de matériel biologique humain recueillis à l'origine dans un but autre que celui du projet de recherche en question. (EPTC 2)

Vie privée – Droit d'une personne de ne pas subir d'ingérence ou d'interférence de la part d'autrui. (EPTC 2).

Plusieurs des définitions qui précèdent sont tirées directement du Glossaire de l'EPTC 2.

Bibliographie

Commissaire à l'information et à la protection de la vie privée de l'Ontario (2015). *La Loi sur la protection des renseignements personnels sur la santé - Votre vie privée*. Extrait de : https://www.ipc.on.ca/wp-content/uploads/2017/09/phipa-f.pdf

Commissariat à la protection de la vie privée du Canada (2013). *Lois provinciales réputées essentiellement similaires à la LPRPDE*. Extrait de : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/lois-provinciales-essentiellement-similaires-a-la-lprpde/

Commissariat à la protection de la vie privée du Canada (2015). *Guide à l'intention des particuliers. La protection de vos renseignements personnels*. Extrait de : https://www.priv.gc.ca/fr/a-propos-du-commissariat/publications/guide_ind/

Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains, décembre 2014. Extrait de : http://www.pre.ethics.gc.ca/fra/policy-politique_tcps2-eptc2_2018.html

Harvard Information Security (s.d.). *Data Classification Table.* Extrait de : https://security.harvard.edu/dct

Instituts de recherche en santé du Canada (2005). *Pratiques exemplaires des IRSC en matière de protection de la vie privée dans la recherche en santé*. Extrait de : http://www.cihr-irsc.gc.ca/f/29072.html

Ordre des psychologues de l'Ontario (2016). *The personal health information protection act, 2004: A guide for regulated health professionals.* Extrait de : http://www.cpo.on.ca/WorkArea/DownloadAsset.aspx?id=1591

Ordre des psychologues de l'Ontario (2005). *Normes de conduite professionnelle*. (révisées en mars 2009) Extrait de : http://www.cpo.on.ca/WorkArea/DownloadAsset.aspx?id=1485

Ordre des psychologues de l'Ontario (2013). *Privacy code of the College of psychologists of Ontario.* Extrait de : http://www.cpo.on.ca/WorkArea/DownloadAsset.aspx?id=653

Société canadienne d'évaluation (2014). *Lignes directrices en matière d'éthique.* Extrait de : https://evaluationcanada.ca/fr/ethique

Société canadienne de psychologie (2017). *Code canadien d'éthique pour les psychologues (quatrième édition)*. Extrait de : https://cpa.ca/docs/File/Ethics/CPA_Code_2017_4thEdFR.pdf

Annexe

Centre de recherche sur les services éducatifs et communautaires
Faculté des sciences sociales et Faculté d'éducation
Université d'Ottawa

Entente en matière de confidentialité et de non-divulgation

Le présent document a pour but de clarifier et de reconnaître ce qu'il est convenu au sujet de la nature et du traitement des renseignements et documents confidentiels susceptibles d'être portés à la connaissance d'une personne (universitaire, membre du personnel, étudiant, bénévole ou autre) au Centre de recherche sur les services éducatifs et communautaires (CRSEC) de l'Université d'Ottawa.

Lorsque des contextes particuliers ne sont pas précisés dans la présente entente, l'intention générale du document est de protéger la confidentialité de l'information reçue par les chercheurs du CRSEC et d'assurer un comportement éthique dans la recherche. Des conditions plus spécifiques peuvent également s'appliquer, par exemple lorsque l'exigent les procédures du CRSEC ou les exigences des comités d'éthique de la recherche.

Je comprends et j'accepte que le respect de cette entente est une condition préalable à ma participation aux activités de recherche du CRSEC.

J'entreprends une tâche ou je participe à des activités de recherche qui peuvent comprendre des entrevues avec des participants humains, la transcription d'entrevues, la saisie de données ou d'autres activités liées à la recherche au CRSEC de l'Université d'Ottawa. Je comprends que mes activités appuieront les études de recherche auxquelles prennent part des participants humains.

En plus des connaissances acquises lors d'une séance d'orientation et d'information sur les activités de recherche du CRSEC, j'accepte de garder confidentielles toutes les questions qui sont portées à mon attention dans l'exercice de mes fonctions au CRSEC, y compris la documentation sur les participants à la recherche, les organismes communautaires et les clients.

J'accepte de respecter toutes les procédures du CRSEC concernant la collecte, la protection et le traitement des données confidentielles.

Je comprends que toute discussion verbale sur la recherche avec des participants humains se limite à l'équipe de recherche et se fera selon ce que décidera le chercheur principal. Le chercheur principal est la personne qui dirige un projet ou un programme de recherche et qui est responsable du bon déroulement du projet ou programme.

Je conserverai tous les renseignements découlant des activités de recherche en toute confidentialité. Je conviens que tous ces renseignements seront utilisés uniquement aux fins de la recherche ou de la thèse, et à aucune autre fin, et qu'ils ne seront pas divulgués à l'organisme parrain (assurant le financement) ou à tout autre tiers sans l'approbation du chercheur principal.

Je ne ferai ni ne conserverai pour mon usage personnel aucune copie de toute information originale, que ce soit sous forme électronique ou papier. Toute information qui est retirée des locaux doit toujours être anonyme, et toutes les caractéristiques susceptibles de permettre l'identification doivent être supprimées. Tout renseignement transféré de cette façon doit être approuvé par écrit par le chercheur principal, et l'autorisation doit être accordée par écrit. Cela comprend toutes les formes de données, y compris les données papier, électroniques et audio et les enregistrements visuels.

À la fin de mes activités au CRSEC, tous renseignements, données, mots de passe informatiques et autres documents connexes devront être retournés au Centre de recherche. J'effacerai également toutes les bases de données électroniques qui sont en ma possession ou sous mon contrôle.

J'accepte d'observer et d'appliquer rigoureusement les exigences du Comité d'éthique de la recherche ou d'autres organismes dans toutes les activités de recherche auxquelles je participerai.

Fait à Ottawa (Ontario), ce ___ jour de _____ 20__. Convenu et accepté par

_____

Signature

_____

Nom

_____

Superviseur / Employeur

_____

Signature

_____ _____ _____

Nom Adresse Profession