Lignes directrices en matière de protection des données de recherche à l'intention des équipes de recherche

Université de Montréal
Bibliothèques
Service des bibliothèques de l'Université de Montréal

1 La collecte

Cette étape comprend la collecte, la création et l'accès aux données de recherche, incluant l'accès temporaire à des données à des fins de constitution d'échantillons ou de dépersonnalisation.

Lignes directrices

- Collecter uniquement les renseignements personnels nécessaires et pertinents.
- Informer les participants de la collecte de données ainsi que de l'utilisation et de la conservation des renseignements personnels, en utilisant des formulaires adaptés à la nature des données recueillies (voir 2.2 de la ligne directrice).
- Utiliser la trousse de collecte d'une approuvée par le comité d'éthique de la recherche institutionnelle, au besoin.
- Lorsque cela est possible, maintenir l'anonymat des participants en utilisant des numéros de participants plutôt que leurs noms et prénoms.

Exemples

- Pour des entrevues de chercheur hautement confidentiel, bien que des données relatives à la santé soient recueillies, le chercheur ne connaît pas l'identité des participants, mais seulement leur numéro de participant.
- Par des discours avec un collègue des données de recherche, le chercheur ne connaît pas l'identité des sujets ayant un niveau profond, du type à catégorie.

Ressources

- Politique de protection des renseignements personnels
- Politique sur la gestion des documents et des archives
- Exemples de renseignements et de documents de consentement
- Trello/Kanban/ Google

2 L'utilisation

Cette étape comprend l'analyse, le traitement ainsi que **le partage et l'utilisation au sein de l'équipe de recherche** des données de recherche.

Lignes directrices

- Nommer des agents ayant des sur nous qu'ils/ elles puisse ils/ ainsi.
- Les données confidentielles doivent être chiffrées lorsque leur transmission est jugée sensible par l'Unité - Sources de données institutionnelles **Transmission des données**.

Transmission par courriel :

- Transmettre les renseignements par un mot de passe fort et envoyer le mot de passe par un autre moyen que le courriel (par exemple, par téléphone).
- Transmettre le mot de passe nécessaire par un autre moyen que le courriel (par exemple, par téléphone). Ne pas inclure le mot de passe dans le corps du courriel ou dans l'objet du courriel.
- Choisir des mots de passe longs et complexes (au moins 12 caractères, incluant majuscules, minuscules, chiffres et caractères spéciaux) et ne pas les réutiliser.
- Vérifiez l'identité du destinataire du courriel avant d'appuyer sur « envoyer » ou « répondre ».
- Limiter autant que possible l'utilisation des renseignements personnels dans le corps du courriel et privilégier l'utilisation d'un lien avec le projet de recherche.

Exemples

- Pour plusieurs des données relatives à l'identité du participant, le chercheur utilise des numéros de participants plutôt que leurs noms et prénoms. Le lien entre les deux est conservé dans un fichier sécurisé.
- Pour des données sensibles, le chercheur ne peut pas utiliser des chiffrement après le transfert, mais il peut utiliser des mots de passe temporaires (Twitter, Zoom).
- Dans des cas plus sensibles, le chercheur ne peut pas utiliser des chiffrement des données confidentielles et doivent être stockées sur un disque dur externe, ou encore de l'Z:\ou un utilisant un mot de passe.

Ressources

- Politique de protection des renseignements personnels
- Procédure pour protéger les informations sensibles lors du partage de documents sur la plateforme Google Drive
- Procédure pour protéger les informations sensibles lors du partage de documents sur la plateforme Microsoft Teams
- Procédure pour protéger les informations sensibles lors du partage de documents sur la plateforme Zoom
- Tableau de gestion des accès
- Tableau de gestion des accès
- Tableau de gestion des accès