CAN/DGSI 100-10 / HRSO 300.03

NORME NATIONALE DU CANADA

Première édition

2025-09

Gouvernance des données dans la recherche avec des êtres humains

03.100.02 03.100.40 35.020 35.030

ONRH

Organisme de normalisation de la recherche humaine

ccn scc

Table des matières

Avant-propos

L'Institut des normes de gouvernance numériques (INGN) élabore des normes de gouvernance de la technologie numérique adaptées à une utilisation planétaire. Il collabore avec des experts, avec des partenaires au pays et à l'étranger et avec le public pour établir des normes nationales visant à réduire les risques pour la population et les organisations canadiennes qui adoptent et utilisent des technologies novatrices dans l'économie numérique d'aujourd'hui.

L'INGN élabore ses normes conformément aux *Exigences et lignes directrices – Accréditation des organismes d'élaboration de normes* (13 juin 2019) du Conseil canadien des normes (CCN).

Il est à noter que certains éléments de la présente norme peuvent faire l'objet de droits de brevet. L'INGN ne saurait être tenu responsable de ne pas avoir indiqué ces droits. Les droits de brevet identifiés lors de l'élaboration de la présente norme figurent dans l'introduction.

Pour en savoir plus sur l'INGN :

Institut des normes de gouvernance numérique
1000, promenade Innovation, bureau 500
Ottawa (Ontario) K2K 3E7
www.dgc-cgn.org/fr/

Une Norme nationale du Canada est une norme qui a été élaborée par un organisme d'élaboration de normes (OEN) titulaire de l'accréditation du Conseil canadien des normes (CCN) conformément aux exigences et lignes directrices du CCN. On trouvera des renseignements supplémentaires sur les Normes nationales du Canada à l'adresse: https://ccn-scc.ca/.

Le CCN est une société d'État qui fait partie du portefeuille d'Innovation, Sciences et Développement économique Canada. Dans le but d'améliorer la compétitivité économique du Canada et le bien-être collectif de la population canadienne, l'organisme dirige et facilite l'élaboration et l'utilisation des normes nationales et internationales. Le CCN coordonne aussi la participation du Canada à l'élaboration des normes et définit des stratégies pour promouvoir les efforts de normalisation canadiens.

En outre, il fournit des services d'accréditation à différents clients, parmi lesquels des organismes de certification de produits, des laboratoires d'essais et des organismes d'élaboration de normes. On trouvera la liste des programmes du CCN et des organismes titulaires de son accréditation à l'adresse: https://ccn-scc.ca/.

L’Organisme de normalisation de la recherche humaine (ONRH) est un organisme canadien d’élaboration de normes sans but lucratif qui élabore des normes de recherche humaine pertinentes pour les Canadiens qui mènent, supervisent et participent à la recherche humaine.

Les normes de recherche humaine assurent que les droits et le bien-être des Participants à la recherche sont sauvegardés et que la recherche humaine soit menée dans un environnement qui favorise l’efficacité, atténue les risques et produit des données fiables vérifiables et crédibles. L'adoption des normes de recherche humaine assure l'harmonisation, la collaboration et la croissance de ce secteur d’activités économiques dans notre pays et à l’échelle internationale.

L'ONRH adhère au Code de pratique pour l'élaboration, l'adoption et l'application des normes de l'Accord de l'OMC sur les obstacles techniques au commerce dans le développement des normes de service et de gestion pour la recherche humaine.

Le calendrier pour l’élaboration de NNC CAN/DGSI 100-10 / HRSO 300.03 Gouvernance des données dans la recherche avec des êtres humains était comme suit:

Publication d’un avis d’intention : 2022-10-20
Première réunion du comité technique : 2023-03-16
Période de consultation publique : 2025/01/23 – 2025/03/28
Réunion finale du comité technique : 2025/06/19
Publication de la première version :2025-09-11

Toutes les unités de mesure utilisées sont exprimées conformément au Système international d’unités (SI).

La norme sera soumise à l’examen du Comité technique au plus tard deux ans après sa date de publication, après quoi elle pourra être rééditée, révisée, confirmée ou abandonnée.

Son but premier est énoncé sous la rubrique « Portée ». Il importe de retenir qu’il incombe à l’utilisateur de juger si la norme convient à une application donnée.

La norme est conçue pour être utilisée dans l’évaluation de la conformité.

ICS:
03.100.02 03.100.40 35.020 35.030

THIS NATIONAL STANDARD OF CANADA IS AVAILABLE IN ENGLISH AND FRENCH.

Comité technique

Membres et contributeurs

Clarissa Alberti Fleck, BSc; Québec

Sassan Azad, BSc, MSc; Ontario

Alexander Bernier, BCL, JD, LLM, SJD; Québec

Andria Bianchi, BA, MA, PhD; Ontario

Shamir Charania, BEng; Alberta

Liseanne Cadieux, BS, BASc, MIS; Nouvelle-Écosse

Colleen Cochran, BA; Saskatchewan

Natalie Comeau, BA, MHSc; Ontario

Sean Gowing, CISSP; Alberta

Kiren Handa, BSc, MSc, MBA; Ontario

Courtney Heisler, BSc, MSc; Nouvelle-Écosse

Cassie Hill, BA, MHA; Nouvelle-Écosse

Karey Iron, BA, MHSc, CIPM; Ontario

Alexander Karabanow, BSc, BAA; Ontario

Tatiana Kawakami, BA, MBA, MBA; Colombie-Britannique

Jude Dzevela Kong, BEd, BSc, MSc, PhD; Ontario

Diana Kulpa, BA, MA; Ontario

Michael McDonald, BA, MA, PhD; Colombie-Britannique

Erica Monteferrante, BA, MA; Québec

Waqar Mughal, BSc, MSc; Ontario

Janice E. Parente, BSc, PhD; Québec

Dimitri Patrinos, BSc, LLB, JD, LLM; Québec

Mikayla Redden, BA, MLIS; Ontario

Katie Roposa, BScN, MEd, RN; Ontario

Eric Sutherland, BMath, MMath; Ontario

Kristi Thompson, BA, MLIS; Ontario

Marie-Laurence Tremblay, BSc, PhD; Nouvelle-Écosse

Jeffrey Webster, BSc, MEnvSc; Ontario

Donald Willison, BSc, MSc, ScD; Ontario

Lee Wilson, BA, MLIS; Nouvelle-Écosse

Agents de normes

Martin Letendre, BA, LLB, LLM; Québec (ONRH)

Darryl Kingston, BA; Ontario (INGN)

Cherlene Tay, BComm; Ontario (INGN)

Introduction

La gouvernance des données dans la recherche avec des êtres humains sert plusieurs objectifs. Elle optimise l'utilisation des données de recherche pour répondre aux besoins de l'Entreprise de recherche (ER, comme une institution ou une société qui, dans le cadre d'une partie ou de la totalité de ses activités, mène ou facilite la recherche humaine) et elle en garantit une utilisation conforme aux obligations éthiques et légales, et elle permet d'appliquer des mesures pour assurer un accès et une protection appropriés contre la corruption des données ou d'autres problèmes. Lorsqu'une bonne gouvernance des données est palpable, les parties – y compris les Participants à la recherche – ont l'assurance que les données de recherche sont utilisées de manière responsable et dans l'intérêt du public.

De plus en plus, les promoteurs et les éditeurs de recherche demandent aux Investigateurs/Chercheurs de diffuser plus largement leurs données finales de recherche. Les ER et les Investigateurs/Chercheurs doivent donc tenir compte des répercussions de la transmission de données sur leur gouvernance tout au long du cycle de vie des données de recherche, par exemple aux étapes suivantes :

- planification de l'étude;
- collecte de données (les Investigateurs/Chercheurs doivent se pencher sur la disposition et la réutilisation des données de recherche dans le cadre du processus de consentement éclairé);
- traitement des données (les dossiers de métadonnées doivent être suffisamment exhaustifs et révélateurs pour les utilisateurs subséquents);
- stockage et archivage des données (les données doivent être stockées de façon appropriée, c'est-à-dire que les données pertinentes sont repérables et qu'il existe des processus pour juger et traiter les demandes d'accès externes).

Voir à l'annexe B des exemples de cycles de vie de données de recherche.

Les données de recherche sont de plus en plus recueillies, traitées et stockées en format numérique. Par conséquent, les répercussions d'actions délibérées ou accidentelles sont aussi plus importantes en raison des propriétés uniques de ce format. Par exemple, les données numériques sont associées à des risques de préjudices divers, car elles peuvent être copiées presque instantanément dans le monde entier. La gouvernance des personnes, des processus, des systèmes et des intervenants impliqués dans le traitement des données est donc importante. L'une des

grandes préoccupations est le risque de fuites de renseignements personnels et d'informations soumises aux droits de propriété intellectuelle à la suite d'un vol, d'une perte ou d'un accès non autorisé entraînant un vol d'identité, une fraude financière ou des dommages à la réputation ou autres aux personnes, organisations et groupes participants. Les lacunes des logiciels ou des systèmes d'exploitation peuvent représenter pour les cybercriminels des occasions d'intrusion au moyen du piratage, de maliciels et d'attaques d'hameçonnage. Cela démontre l'importance des mises à jour et des correctifs de sécurité technologiques. En outre, la disponibilité grandissante de services externes, dont le stockage infonuagique, exige une clarification des rôles et responsabilités des Fournisseurs et des protections fournies. Les tactiques de piratage psychologique, où l'attaquant manipule une personne pour qu'elle divulgue des renseignements personnels, accentuent par ailleurs la vulnérabilité des données numériques face aux cyberattaques. Les technologies évoluent rapidement; il faut donc déployer des efforts continus pour avoir une longueur d'avance en matière de vulnérabilités et de protection des actifs numériques.

L'objectif de la présente NNC est de proposer aux utilisateurs, comme les ER, les Investigateurs/Chercheurs ainsi que les auditeurs, des mesures tangibles d'évaluation de la qualité de leur gouvernance des données. Le document est un complément à de multiples textes normatifs, notamment la *Politique des trois organismes sur la gestion des données de recherche* et l'*Énoncé de politique des trois conseils (EPTC 2)*.

1. Portée

La NNC s'applique à toute personne participant à la réalisation d'une recherche avec des êtres humains ainsi qu'aux organismes à but lucratif et sans but lucratif, publics et privés. Dans le présent document, toute entité menant ou rendant possible des activités de recherche humaine est considérée comme une Entreprise de recherche (ER). Une ER peut faire partie d'un établissement (p. ex. une université) ou d'une société plus importants, ou alors d'un Programme de protection des Participants à la recherche (PPPR).

En réduisant la variabilité de l'interprétation des règlements, des politiques et des lignes directrices, cette NNC fournit une base pour l'implantation de documents procéduraux sans ambiguïté et conformes aux références normatives canadiennes et internationales.

La recherche sur les êtres humains intègre différents types de méthodes qualitatives et quantitatives, de disciplines (p. ex., santé, sciences sociales et humaines, arts, ingénierie) et d'approches (p. ex. interventionnelles, observationnelles) dans divers domaines (p. ex., biomédical, social, juridique, comportemental). Il est possible de faire de la recherche humaine avec des données, des spécimens, des images, des observations ou des enregistrements audio ou vidéo, numériques ou analogues, qu'ils soient existants ou recueillis préalablement. La présente norme s'applique à toutes les données numérisées et numériques.

Étant donné la diversité des disciplines et des méthodes de recherche, la présente NNC traite des problèmes, des pratiques et des processus de gouvernance des données

communs tout en tenant compte des exigences et des normes qui peuvent être propres aux disciplines, auxquelles le lecteur devrait se conformer.

Pour les besoins de la présente, les scénarios de recherche humaine utilisés comprennent, sans toutefois s'y limiter :

1. la collecte ou la création de données prospectives afin de traiter une question de recherche précise ou de tendre vers un objectif de recherche précis :
    a) lorsqu'il n'y a pas de plan explicite de réutilisation des données;
    b) lorsque l'Investigateur/Chercheur croit que les données pourraient être réutilisées (par lui-même ou par d'autres); ou
    c) lorsque le promoteur de la recherche demande que les données soient réutilisées;
2. l'utilisation de données existantes pour traiter une question de recherche précise, et où les données :
    a) ont été créées à des fins autres que la recherche; ou
    b) ont été créées à des fins de recherche en planifiant ou non leur utilisation ultérieure;
3. la collecte de données prospectives dans le but précis de les réutiliser à des fins de recherche indéterminées :
    a) où les données sont recueillies directement auprès des personnes (p. ex., biobanques et registres);
    b) où la collecte prospective vise des données longitudinales dérivées de donnes existantes ayant été créées à des fins autres que la recherche (p. ex., données administratives); ou
    c) où s'applique une combinaison de a) et de b);
4. la création de nouvelles données basées sur des données existantes.

« Doit » vs « Devrait »

Dans la présente NNC, «doit» indique que l'exigence est obligatoire et est étayée par des références normatives, tandis que «devrait» indique que l'exigence est recommandée, ou un énoncé de bonnes pratiques.

2. Références normatives

Cette NNC a été élaborée tout en conformité avec les documents normatifs énumérés ci-dessous, accessibles au public. L'utilisateur de cette NNC doit se référer à la dernière édition ou révision des documents normatifs.

2.1 Législation canadienne

Commissariat à la protection de la vie privée du Canada : Lois et organismes de surveillance provinciaux et territoriaux en matière de protection de la vie privée

https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/lois-et-organismes-de-surveillance-provinciaux-et-territoriaux-en-matiere-de-protection-de-la-vie-privee/

Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) https://laws-lois.justice.gc.ca/fra/lois/p-8.6/page-1.html

Loi sur les aliments et drogues de Santé Canada https://laws-lois.justice.gc.ca/fra/lois/f-27/page-1.html

2.2 Règlements canadiens

Règlement sur les aliments et drogues de Santé Canada, partie C, titre 5 https://www.canada.ca/fr/sante-canada/services/medicaments-produits-sante/conformite-application-loi/bonnes-pratiques-cliniques/documents-orientation/guide-drogues-destinees-essais-cliniques-sujets-humains-gui-0100.html

Règlement sur les instruments médicaux de Santé Canada, partie 3 https://laws-lois.justice.gc.ca/fra/reglements/DORS-98-282/page-9.html

Règlement sur les produits de santé naturels de Santé Canada, partie 4 https://laws-lois.justice.gc.ca/fra/reglements/DORS-2003-196/page-7.html

2.3 Politiques et directives

Découvertes fortuites significatives – Énoncé de politique des trois conseils : Éthique de la recherche avec les êtres humains – EPTC 2 https://ethics.gc.ca/fra/incidental_findings.htmlhttps://ethics.gc.ca/eng/incidental_findings.html

Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains – EPTC 2 https://ethics.gc.ca/fra/policy-politique_tcps2-eptc2_2022.htmlhttps://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2022.html

Good Clinical Data Management Practices (GCDMP) https://scdm.org/gcdmp/

International Council for Harmonization (ICH) of Technical Requirements for Pharmaceuticals for Human Use Good Clinical Practice Guideline https://www.ich.org/page/efficacy-guidelines

Interprétations – Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains – EPTC 2 https://ethics.gc.ca/fra/policy-politique_interpretations.html

Politique des trois organismes sur la gestion des données de recherche https://www.ic.gc.ca/eic/site/063.nsf/fra/h_97610.html

Principes de propriété, de contrôle, d'accès et de possession des Premières Nations PCAP® https://fnigc.ca/fr/les-principes-de-pcap-des-premieres-nations/https://fnigc.ca/ocap-training/

2.4 Normes nationales du Canada et normes mondiales

CAN/DGSI 104:2021 / Rev 1: 2024 Contrôles de base de la cybersécurité pour les petites et moyennes organisations https://dgc-cgn.org/fr/produit/can-dgsi-104/

CAN/DGSI 129 / HRSO 100.01/ Rev 1:2024 Développement d'un Programme de protection des Participants à la recherche (PPPR) https://www.hrso-onrh.org/francais/normes/normes-publiees/

CAN/HRSO-200.01-2021 Évaluation éthique et surveillance de la recherche avec des êtres humains https://www.hrso-onrh.org/francais/normes/normes-publiees/

CAN/HRSO-300.01-2022 La conduite de la recherche sur les êtres humains https://www.hrso-onrh.org/francais/normes/normes-publiees/

HRSO-100.02-2023 Développement d'un programme de formation pour la protection des Participants à la recherche https://www.hrso-onrh.org/francais/normes/normes-publiees/

ISO/IEC 27000:2018-02 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

2.5 Autres règlements

US Code of Federal Regulations Title 21 https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm

US Code of Federal Regulations Title 45 https://www.ecfr.gov/current/title-45

General Data Protection Regulation (GDPR) https://gdpr.eu/tag/gdpr/

3. Termes et définitions

Accès aux données : L'accès ouvert, homologué, contrôlé et privé aux données (définis ci-dessous).

- accès ouvert : Les données sont divulguées publiquement sans restriction des catégories d'utilisateurs pouvant y accéder ni imposition de limitations significatives quant aux objectifs d'utilisation acceptables.
- accès homologué : Les données sont directement mises à la disposition de tous les utilisateurs créant un compte ou demandant autrement accès aux données, ce qui cadre avec les politiques applicables en matière d'utilisation responsable des données.
- accès contrôlée : Les données sont mises à la disposition des utilisateurs s'étant authentifiés après avoir suivi un processus de demande rigoureux qui comprend souvent la signature d'ententes sur l'accès aux données, un examen des motifs d'utilisation des données par un comité d'experts ou un organisme de supervision, et la fourniture, par le demandeur, d'un justificatif de recherche et d'une preuve d'affiliation à un organisme de recherche reconnu.
- accès privé : Les données ne peuvent pas sortir des murs de l'organisation qui les a créées ou les détient autrement afin que des tiers les utilisent pour leurs propres recherches.

Banque de données : Tout ensemble structuré ou non de renseignements numériques ayant de la valeur pour une organisation ou une personne.

Comité d’éthique de la recherche (CER) : Un groupe constitué de manière appropriée qui applique des principes éthiques dans son examen et son évaluation continue de la recherche impliquant des humains. Un CER est également connu comme un comité d'examen indépendant ou institutionnel (IRB), un comité d'éthique indépendant (CEI), un comité d'éthique de la recherche (CER) ou un comité d'examen éthique (ERB).

Communauté : Un groupe de personnes ayant une identité ou un intérêt partagé qui a la capacité d'agir ou de s'exprimer en tant que collectif. Une Communauté peut être territoriale, organisationnelle ou définie par un intérêt commun. Une Communauté peut avoir des processus de gouvernance qui affectent la recherche sur les êtres humains, tels que l'engagement du leadership, le recrutement, le consentement, la diffusion et l'appropriation des résultats de la recherche.

Conflits de rôles : Une situation qui se produit lorsque des exigences incompatibles sont imposées à une personne relativement à son travail ou à son poste, comme des responsabilités fiduciaires conflictuelles (p. ex., un Investigateur/Chercheur évaluant sa propre recherche alors qu’il siège à un CER).

Conflits d’intérêts : Ensemble de conditions ou de facteurs (tels que l’argent, l’amitié, la réputation) dans lequel le jugement professionnel concernant un intérêt principal (tel que le bien-être d’un Participant à la recherche) est indûment influencé, ou raisonnablement perçu comme tel, par un intérêt secondaire (tel un gain financier). Les conflits d’intérêts ont les composantes suivantes :

- une relation – Une partie (le « fiduciant ») a le droit de croire que l’autre partie (le « fiduciaire ») promouvra ou protégera ses intérêts en ce qui concerne les questions relevant de la relation;
- un intérêt conflictuel – Il s’agit d’une influence qui tend à rendre le jugement du fiduciaire sur une décision donnée moins fiable dans la promotion ou la protection des intérêts du fiduciant qu’il ne le serait normalement;
- un exercice de jugement – Le fiduciaire doit être en mesure de prendre une décision qui a des répercussions sur les intérêts du fiduciant.

Connaissances traditionnelles : L’Information transmise entre générations, comme des langues, des histoires, des pratiques cérémoniales, des danses, des chansons; des méthodes artistiques, de chasse, de piégeage; des traditions de rassemblement; des techniques de préparation et d’entreposage d’aliments et de remèdes; et des croyances, croyances spirituelles et visions du monde. C’est l’une des formes de données des Populations autochtones.

Consentement collectif/communautaire : Un accord qui passe par l’adhésion à la structure de gouvernance de la Communauté en question. En l’absence d’une structure de gouvernance, un accord est obtenu par la consultation de groupes d'individus reflétant la diversité de la Communauté en question.

Consentement éclairé : Un accord libre, volontaire, éclairé et continu que donne une personne pour participer à une recherche.

Documents de procédure: Terme collectif utilisé pour décrire les politiques, les procédures (telles que les modes opératoires normalisés) et les lignes directrices.

Données : Tout ensemble de variables qualitatives ou quantitatives. Les données peuvent être enregistrées dans n'importe quel format (par exemple, électronique, papier) et inclues dans des collections de novo ou une utilisation secondaire des données existantes.

Données de recherche : Données utilisées à des fins de recherche. Pour cette NNC, le terme « données de recherche » est limité aux données sur les êtres humains, y compris leur matériel biologique.

Données de recherche identifiables : Selon un jugement raisonnable, les renseignements qui peuvent permettre d'identifier une personne, qu'ils soient utilisés seuls ou combinés à d'autres renseignements disponibles. On les appelle aussi des renseignements personnels.

Droits collectifs ou de groupes : Les droits éthiques ou légaux des groupes par opposition aux droits des personnes. Les titulaires de droits de groupes comprennent les sociétés, les associations bénévoles et les Communautés. Il s'agit de groupes aux intérêts communs, reconnaissant mutuellement les responsabilités associées à leur statut de membres, à la structure de gouvernance formelle ou informelle, et partageant souvent un patrimoine et des traditions. De tels droits définissent les domaines de contrôle et de gouvernance souverains. Lorsque la Population étudiée est un groupe ayant des droits collectifs, ceux-ci doivent entrer en ligne de compte dans la gouvernance de la recherche.

- **Droits collectifs des Populations autochtones :** Les droits collectifs des Populations autochtones du monde entier (voir la *Déclaration des Nations Uniques sur les droits des Populations autochtones*) intégrés à la loi canadienne et dans les lois et coutumes locales autochtones. Ces droits reconnaissent la souveraineté, le contrôle des terres, les ressources et l'accès de la Communauté autochtone.

Engagement de la Communauté et des Participants à la recherche : Un processus qui établit une interaction entre un Investigateur/Chercheur, ou une Équipe de recherche, et une Communauté ou des participants individuels. Cela signifie l'intention d'établir une relation de collaboration avec un objectif de responsabilisation commune, bien que le degré de collaboration puisse varier en fonction du contexte communautaire et de la nature de la recherche.

Entreprise de recherche (ER) : Une entité, telle qu'une institution ou une société, qui, dans le cadre de toutes ses activités, mène ou facilite la recherche humaine. Une ER peut exister en tant que composante d'un PPPR

Équipe de recherche : Un groupe d'individus travaillant ensemble de manière engagée vers un objectif de recherche commun.

Évaluation de la conformité : Un processus utilisé pour démontrer qu'un produit, un service, un système de gestion ou un organisme satisfait à des procédures ou à des exigences spécifiées.

Fournisseurs et Sous-traitants : Des entités qui vendent des produits et services à l'ER ou PPPR (Fournisseurs) ou fournissent des services sous contrat à l'ER ou PPPR

(Sous-traitants). Certains exemples importants de Sous-traitants comprennent, sans s'y limiter, aux CER externes, les Investigateurs/Chercheurs externes, les biobanques externes et les organismes de recherche sous contrat.

Gestionnaire/Coordonnateur/Propriétaire d'actifs informationnels : Une partie (personne ou entité) choisie comme Gestionnaire des données, donc chargée de gérer la sphère de protection connexe. Le Gestionnaire d'actifs informationnels est responsable d'établir et de maintenir en place toutes les mesures de protection applicables.

Gouvernance des données : Il en existe de nombreuses définitions. Voici deux définitions pour vous aider à comprendre certaines nuances :

- Exercice de l'autorité, du contrôle et de la prise de décision commune (planification, surveillance et application) concernant la gestion des banques de données (Ladley, 2020).
- Façon dont une organisation assure la sécurité, se conforme aux règlements et aux lois, et suit les normes éthiques lorsqu'elle gère l'information (Smallwood, 2019).

Investigateur/Chercheur : Dans le cadre d'une ER ou d'un PPPR, un individu qui effectue des recherches sur les êtres humains.

Matériels biologiques : Le terme comprend les tissus, les organes, le sang, le plasma, la peau, le sérum, l'ADN, l'ARN, les protéines, les cellules, les cheveux, les coupures d'ongles, l'urine, la salive et d'autres fluides corporels. Le terme comprend également les éléments liés à la reproduction humaine, y compris les embryons, les fœtus, les tissus fœtaux ainsi que les éléments reproductifs humains.

Méta-données : Les données mettant en contexte les données recueillies. Les métadonnées, qui proviennent de documents bibliographiques au sujet de livres, facilitent le repérage, l'utilisation et la gestion des données. Elles sont souvent plus générales que les données qu'elles mettent en contexte, et peuvent être de nature descriptive (caractéristiques des données et de leur créateur, Gestionnaire, Coordonnateur, ou Propriétaire), structurale (organisation des données) ou administrative (origine, type et droits et limitations d'accès).

Norme nationale du Canada (NNC) : Une norme élaborée par un organisme d'élaboration de normes accrédité par le Conseil canadien des normes (CCN) conformément aux exigences et aux directives établies par le CCN.

Participant à la recherche : Une personne dont les données, le matériel biologique ou les réponses aux interventions, aux stimuli ou aux questions peuvent être utilisés pour répondre à la ou aux questions de recherche.

Personnes qui jouent un rôle dans l'ER : Toute personne ou entité au sein d'une organisation dont les actions affectent directement ou indirectement l'intégrité des données de recherche, le bien-être, les intérêts ou les droits des Participants à la recherche, tels que les Investigateurs/Chercheurs, le personnel administratif, étudiants-chercheurs, coordonnateurs de recherche, moniteurs de recherche, associés de recherche et partenaires communautaires ou patients.

Populations autochtones : Dans le contexte du Canada, les personnes d'ascendance des Premières Nations, Inuite ou métisse, peu importe où elles résident et que leur nom figure ou non sur le registre du gouvernement canadien et quelles que soient les autres dispositions provinciales, territoriales ou régionales en ce sens.

Plan de gestion des données : Un document spécifique au projet qui décrit les stratégies, pratiques et processus de gestion des données tout au long du cycle de vie de la recherche, y compris les phases actives, de stockage et d'archivage/destruction. Le plan doit évoluer parallèlement au projet et être régulièrement mis à jour pour refléter les changements de conception, de méthodologie ou d'exigences liées aux données, garantissant ainsi une conservation et une gestion responsables et efficaces des données, du début à la fin, et au-delà.

Population étudiée : Une population bien définie comme sujet de la recherche. Par exemple, elle peut être délimitée par des traits physiologiques, psychologiques ou sociaux en commun. Dans certains cas, la population détient des droits collectifs qui ont des répercussions sur l'accès à ses données et sur leur contrôle.

Programme de protection des Participants à la recherche (PPPR) : Un programme à l'échelle de l'organisation composé d'un réseau d'entités interdépendantes qui partagent la responsabilité de la protection des Participants à la recherche et interagissent dans un système qui favorise une culture d'intégrité, de qualité, d'efficacité, de responsabilité et de pratiques fondées sur des données probantes. Un PPPR peut exister dans toute organisation à but lucratif ou sans but lucratif, publique ou privée où de la recherche humaine est menée et/ou supervisée.

Recherche humaine: Une enquête systématique et rigoureuse impliquant des êtres humains qui comprend, mais sans s'y limiter, aux disciplines suivantes: recherche en santé, recherche en sciences sociales et humaines, recherche créative et fondée sur les arts et recherche en ingénierie, et comprend, mais n'est pas limité aux méthodologies suivantes:

- recherche interventionnelle, recherche observationnelle
- recherche qualitative, recherche quantitative
- recherche sociale et comportementale, recherche sur les services de santé, recherche en santé publique, recherche en éducation
- recherche impliquant des données humaines existantes, du matériel biologique humain et leurs dérivés
- recherche impliquant des personnes vivantes ou décédées.

Souveraineté des données : Se réfère généralement au contrôle, à la gestion et à la gouvernance des données conformément aux lois, aux pratiques et aux coutumes de la juridiction dans laquelle elles sont situées, générées ou traitées.

- **Souveraineté des données autochtones :** Les Populations autochtones, dont les systèmes de croyances datent d'avant les dispositions coloniales actuelles, ont leurs propres structures de gouvernance de l'information. Dans ce contexte, la souveraineté des données correspond au droit des Populations autochtones de recueillir, d'analyser, d'interpréter, de gérer, de distribuer et de réutiliser toutes les données provenant de leurs Communautés ou en lien avec celles-ci.

La souveraineté s’applique également au savoir traditionnel et aux données numérisées.

Utilisation secondaire : L'utilisation dans la recherche d'informations ou de matériel biologique humain collecté à l'origine dans un but autre que le but actuel de la recherche.

Validation des systèmes : Le processus structuré visant à vérifier qu'un système dans son ensemble répond à des exigences et paramètres prédéfinis afin de garantir son bon fonctionnement dans des circonstances spécifiques. La validation des systèmes inclut les éléments matériels, logiciels et réseau.

Vie privée : Le droit des individus de déterminer eux-mêmes quelles informations les concernant sont collectées, consultées, utilisées, partagées, stockées et détruites, et par qui et à qui ces informations peuvent être divulguées.

4. Exigences techniques

La présente NNC décrit les politiques, les procédures, les personnes et les infrastructures qu’il faut pour soutenir les capacités de gouvernance de données d’une ER. Les méthodes de gouvernance varient dans les ER en fonction du degré de centralisation de la prise de décision et des responsabilités. Par exemple, la responsabilité entourant l’utilisation des données de recherche peut être beaucoup moins centralisée dans un cadre universitaire qu’en entreprise. Ces facteurs contextuels favoriseront la mise sur pied de structures de responsabilisation innovantes et l’harmonisation, dans les ER collaboratrices, des politiques et procédures qui régissent les données de recherche, dont les éléments sont décrits ci-dessous.

4.1 Autorité, obligation de rendre compte et responsabilité

4.1.1 L’ER doit avoir des documents de procédure qui sont cohérents avec les lois, les textes normatifs et les NNC pertinents régissant sa façon de recueillir, de stocker, d’utiliser et de divulguer des données sur des Participants à la recherche humaine. Ces lois, textes normatifs et NNC sont habituellement ciblés par l’autorité la plus élevée de l’établissement ou de l’organisation dans lequel l’ER travaille et sont inclus dans le mandat de l’ER (voir NNC CAN/HRSO-300.01-2022 La conduite de la recherche avec des êtres humains, article 4.1.1 « Mandat »).

4.1.2 Les activités de recherche de l’ER doivent respecter la NNC CAN/HRSO-300.01-2022 La conduite de la recherche avec des êtres humains.

4.1.3 L’ER doit avoir des documents de procédure pour garantir la continuité des ressources nécessaires à la gestion de la vie privée et de la sécurité des données de recherche tout au long de leur cycle de vie, conformément à la présente norme. L’assistance offerte doit être proportionnelle à l’importance et à la complexité de la recherche réalisée et doit inclure du financement, du personnel qualifié, un espace de travail, de l’équipement, du matériel et des technologies.

4.1.4 L’ER doit avoir des documents de procédure pour établir formellement la responsabilité et l’autorité (y compris une description des postes) en matière de gestion des banques de données en sa possession tout au long de leur cycle de vie. Voici certaines des activités associées à la gestion des banques de données dont l’autorité et la responsabilité doivent être déterminées :

a) tenir un registre des banques de données en la possession de l’ER (voir l’article 4.2);

b) sélectionner des systèmes de classification des données de sorte que toutes les données de recherche sous la responsabilité de l’ER soient classées de façon appropriée. Il se peut que plus d’un certain système soit nécessaire pour répondre aux besoins des divers types de recherches réalisées dans une ER (voir l’article 4.2.2);

c) soutenir l’élaboration et le maintien de plans de gestion des données au sein de l’ER (voir l’article 4.3);

d) définir, tenir à jour et contrôler les normes de qualité des données de recherche en matière d’exactitude, d’exhaustivité, de cohérence, d’immuabilité, d’intégrité, de fiabilité et d’actualité, lorsque nécessaire (voir l’article 4.6);

e) surveiller et faciliter le respect des lois, des textes normatifs et des NNC pertinents (voir l’article 4.7);

f) mettre en place des modalités de collecte de données, des environnements informatiques et d’autres solutions sécuritaires pour soutenir les activités de recherche tout au long du cycle de gestion des données (voir l’article 4.8) ;

g) définir, maintenir et surveiller les accès autorisés et justifiés qui sont appropriés aux données de recherche à des moments précis du cycle de vie des données (voir l’article 4.4), soit durant

- la phase active, lorsqu’elles sont recueillies, traitées et analysées,
- la phase de conservation, pour en simplifier l’accès par d’autres Investigateurs/Chercheurs, s’il y a lieu,
- la phase d’archivage ou de destruction (archivage à long terme ou destruction sécuritaire des données, s’il y a lieu).

4.1.5 L’ER doit avoir des documents de procédure qui précisent :

a) qui conserve les données de recherche recueillies si l’Investigateur/Chercheur principal cesse de participer à l’ER;

b) les méthodes de disposition et de gouvernance des données de recherche advenant la dissolution de l’ER ou un changement de propriétaire;

c) comment l’ER respecte et fait respecter la souveraineté autochtone des données (accès, propriété et contrôle) si une Communauté autochtone participe à la recherche.

4.1.6 L’ER doit avoir des documents de procédure de maintien et de contrôle de l’utilisation des systèmes informatiques servant à consigner l’ensemble des

politiques et processus. (Voir les exigences en matière de capacités aux paragraphes 4.8.7 b), k) et n).)

4.2 Tenue d’un registre des banques de données

L’ER doit avoir des documents de procédure sur la tenue d’un registre de banques de données. Les éléments qu’il contient devraient être accessibles au public afin d’encourager la transparence et l’innovation par la science ouverte.

4.2.1 L’ER doit avoir des documents de procédure sur la tenue d’un registre incluant minimalement ce qui suit pour chaque banque de données :

a) une description claire du sujet traité;

b) les variables incluses;

c) le système de classification des données utilisé (voir l’article 4.2.2);

d) les dates de début et de fin de la collecte des données de recherche;

e) les sources de données, tant pour leur collecte initiale que pour l’utilisation secondaire des banques de données existantes;

f) le lieu où se trouve le plan de gestion des données propre au projet concerné;

g) les coordonnées des individus ou des comités nommés responsables des banques de données (p. ex, Gestionnaire/Coordonnateur/Propriétaire d’actifs informationnels, conseiller juridique, Investigateur/Chercheur);

h) la phase du cycle de vie des données (active, enregistrement dans un répertoire, archivage/destruction);

i) la date de verrouillage des données (c.-à-d. moment où elles ne sont plus modifiables ou manipulables), le cas échéant;

j) la date d’expiration des données;

k) le plan de destruction des données et une preuve de leur destruction après coup;

l) un registre du personnel interne à qui un accès a été accordé ainsi que les motifs de cette autorisation, par exemple : créer, consulter, mettre à jour et supprimer des données de recherche, ou partager ou fournir un accès au téléchargement; et

m) un registre des personnes externes au projet initial à qui un accès a été accordé ou à qui les données ont été divulguées pour des raisons précises (comme des études multicentriques, des analyses secondaires, de l’assistance pour des éléments spécialisés de la recherche, ou dans le cadre d’une publication en libre accès).

4.2.2 L’ER doit avoir des documents de procédure sur la classification des données selon certains critères, par exemple :

a) la discipline de recherche (p. ex., santé, sciences de la vie, sciences sociales, arts, sciences naturelles, ingénierie, et sous-classifications appropriées);

b) les caractéristiques de la Population étudiée (p. ex., caractéristiques sociodémographiques et géographiques, santé, vulnérabilité et appartenance à une Communauté);

c) le modèle de la recherche (p. ex., méthodes quantitative, qualitative ou mixte; recherche expérimentale ou observationnelle, et exploratoire ou explicative); et

d) la sensibilité des données (p. ex., individuelles ou agrégées).

4.2.3 L’ER devrait avoir des documents de procédure pour la publication du registre des banques de données ainsi que du nom et des coordonnées des personnes à contacter pour les questions au sujet des banques.

4.2.4 L’ER devrait avoir des documents de procédure concernant la tenue d’un dossier de demandes au sujet des banques de données, y compris les demandes générales et d’accès. Lorsqu’une demande se conclut par une demande d’accès aux données ou de divulgation, l’ER devrait consigner les coordonnées du demandeur et la nature de l’accès ou de la divulgation.

4.2.5 L’ER doit avoir des documents de procédure de maintien et de contrôle de l’utilisation des systèmes informatiques afin d’agir comme système de consignation des informations sur le registre de données et les processus connexes. (Voir les exigences en matière de capacités aux paragraphes 4.8.7 b), k) et n).)

4.2.6 L’ER doit avoir des documents de procédure pour fournir et tenir à jour un catalogue complet des services, y compris de leurs objectifs, caractéristiques et exigences. Le catalogue devrait faciliter l’accès et les recherches, et comprendre des mécanismes de demandes de services et d’accès.

4.3 Plans de gestion des données

4.3.1 L’ER doit avoir des documents de procédure pour soutenir les Investigateurs/Chercheurs dans l’élaboration et le maintien de plans de gestion des données pour chaque projet, notamment pour ce qui suit :

a) fournir des gabarits et d’autres lignes directrices pour orienter l’élaboration, la conservation et la mise à jour de plans de gestions des données propres au projet, d’après les meilleures pratiques et les références normatives, y compris les éléments suivants :

- une explication claire de l’objectif ou de la question de recherche;
- des précisions sur les données et les métadonnées requises;
- les mesures entreprises pour s’assurer que des métadonnées cohérentes et justes sont enregistrées et mises à jour au fil du cycle de vie du projet;

- une liste des sources des données (comme les Gestionnaires d'actifs informationnels) et des méthodes et autorisations qui serviront à recueillir, à utiliser et à divulguer les données;
- une description des Participants à la recherche et de la population à l'étude (p. ex., personnes ayant un problème de santé particulier, résidents d'une zone géographique donnée);
- les paramètres d'utilisation des données, y compris leur réutilisation, et la disponibilité d'une preuve de consentement (y compris d'une exemption de consentement);
- les méthodes qui seront utilisées pour analyser la recherche (c.-à-d. les méthodes analytiques);
- les mesures mises en place pour gérer les données de façon sécuritaire tout au long du cycle de vie de la recherche humaine (p. ex., formation de l'Équipe de recherche et protocoles de protection des données);
- les mesures prises pour répondre aux obligations légales et éthiques en ce qui a trait à la collecte, à l'utilisation, au stockage, à la diffusion et à la publication des données;
- les mesures de gestion continue des données (p. ex., contrôle du stockage et de la qualité);
- les rôles et responsabilités des membres de l'Équipe de recherche en ce qui a trait aux données recueillies et traitées;
- la confirmation de l'inclusion, dans le budget du projet, des fonds nécessaires au respect et à la mise à jour continus du plan de gestion des données;
- les problèmes notables rencontrés quant aux données ainsi que les mesures et décisions prises en conséquence au fil du temps;
- la décision en ce qui a trait à la diffusion et à la réutilisation des données après le projet, et, le cas échéant, les moyens qui seront pris; et
- les mesures prises pour mettre en œuvre les accords de contribution et d'accès aux données au sein ou en dehors de l'ER (tels que les accords d'utilisation des données, les accords de partage des données, les accords de contribution aux données, les protocoles d'accord).

b) fournir un emplacement centralisé pour le stockage des plans de gestion des données;

c) stocker les plans de gestion des données et en conserver toutes les versions pour pouvoir tenir des registres d'audit;

d) établir et maintenir en place un processus d'examen et de mise à jour périodiques des plans de gestion des données, par exemple annuels ou au besoin (comme lorsque les lois ou les technologies d'accès et de stockage des données changent);

e) garantir la mise à jour et le respect des plans de gestion des données, y compris en définissant un processus de remontée hiérarchique des problèmes; et

f) tenir un registre des plans terminés.

4.3.2 L’ER devrait avoir des documents de procédure d’examen et d’approbation des plans de gestion des données élaborés par les Investigateurs/Chercheurs sous son égide.

4.3.3 L’ER doit avoir des documents de procédure de maintien et de contrôle de l’utilisation des systèmes informatiques devant servir de système de consignation de l’ensemble des plans de gestion des données. (Voir les exigences en matière de capacités aux paragraphes 4.8.7 b), k) et n).)

4.4 Accès aux données

4.4.1 L’ER doit avoir en place des documents de procédure à l’intention des Investigateurs/Chercheurs et de leur équipe pour :

a) déterminer à qui fournir un accès aux données (sur la base des rôles et responsabilités) et dans quels buts, par exemple : créer, consulter, mettre à jour et supprimer des données de recherche, ou partager ou fournir un accès au téléchargement;

b) surveiller et enregistrer qui accède aux données, par quel moyen et pour quelles raisons précises (p. ex., études multicentriques, analyses secondaires ou reproduction);

c) déterminer la durée des accès accordés aux données du projet de recherche ainsi que les critères pour établir la fréquence de révision des privilèges d’accès;

d) veiller à ce que le personnel autorisé ait un accès opportun et sans limitations aux données pendant le projet de recherche (p. ex., essais cliniques); et

e) retirer en partie ou entièrement les accès d’une personne.

4.4.2 L’ER doit avoir en place des documents de procédure à l’intention des Investigateurs/Chercheurs externes pour :

a) déterminer à qui fournir un accès aux données (sur la base des rôles et responsabilités) et dans quels buts, par exemple : créer, consulter, mettre à jour et supprimer des données de recherche, ou partager ou fournir un accès au téléchargement;

b) surveiller et enregistrer qui accède aux données, par quel moyen et pour quelles raisons précises (p. ex., études multicentriques, analyses secondaires ou reproduction);

c) déterminer la durée des accès accordés aux données du projet de recherche ainsi que les critères pour établir la fréquence de révision des privilèges d’accès;

d) veiller à ce que les Investigateurs/Chercheurs externes aient un accès facile aux informations (y compris les métadonnées) sur les banques de données de recherche disponibles pour une analyse secondaire, y compris au processus d’accès (voir l’article 4.1.2.3); et

e) retirer en partie ou entièrement les accès d’une personne.

4.4.3 L’ER doit avoir en place des documents de procédure à l’intention des partenaires communautaires pour :

a) déterminer à qui fournir un accès aux données (sur la base des rôles et responsabilités) et dans quels buts, par exemple : créer, consulter, mettre à jour et supprimer des données de recherche, ou partager ou fournir un accès au téléchargement;

b) surveiller et enregistrer qui accède aux données, par quel moyen et pour quelles raisons précises (p. ex., études multicentriques, analyses secondaires ou reproduction);

c) déterminer la durée des accès accordés aux données du projet de recherche ainsi que les critères pour établir la fréquence de révision des privilèges d’accès; et

d) retirer en partie ou entièrement les accès d’une personne.

4.4.4 L’ER doit avoir en place des documents de procédure décrivant le processus que les Participants à la recherche doivent suivre pour consulter leurs données d’après le consentement fourni, les lois applicables, les textes normatifs et les NNC.

4.4.5 L’ER doit également avoir en place des procédures formelles pour veiller au respect de la souveraineté des données des Populations et des Communautés autochtones, y compris un processus pour garantir ce qui suit :

a) leurs droits, intérêts et pouvoirs de propriété, d’accès et de contrôle de leurs données de recherche demeurent protégés conformément aux lois, pratiques et habitudes de la région, y compris les traités, la Déclaration des Nations Unies sur les droits des Populations autochtones et les cadres de référence sur la souveraineté des données autochtones (p. ex., principes CARE, principes de PCAP^{MD}); et

b) les exigences et politiques réglementaires qui s’appliquent à l’ER ne deviennent pas un fardeau indu ni ne limitent les droits des Populations et des Communautés autochtones à la propriété des données de recherche, à leur accès et au contrôle de leur accès.

4.4.6 L’ER doit avoir en place des documents de procédure de maintien et de contrôle de l’utilisation des systèmes informatiques afin d’agir comme intermédiaire ou médiateur pour la transmission des données et leur accès. (Voir les exigences en matière de capacités aux paragraphes 4.8.7 c), f), g), i) et j).)

4.5 Validation des systèmes de données

Les exigences suivantes définissent les exigences techniques pour la validation des systèmes de données. NNC CAN/HRSO-300.01-2022 La conduite de la recherche sur les êtres humains, article 4.1.8 *«* Sélection des Fournisseurs et des Sous-traitants » doit s’applique à toute procédure en lien avec la sélection de Fournisseurs et de Sous-traitants.

4.5.1 L’ER doit avoir des documents de procédure pour évaluer et valider le matériel et les logiciels utilisés pour collecter et traiter les données de recherche (p. ex., systèmes de consentement éclairé, saisie électronique de données, résultats électroniques déclarés par les participants, dispositifs portables).

4.5.2 L’ER doit avoir des documents de procédure pour tenir à jour et mettre à la disposition des Investigateurs/Chercheurs une liste du matériel et des logiciels qu’elle a validés après avoir évalué et accepté tous les risques liés à l’usage prévu (y compris la disponibilité et l’intégrité des fonctions proposées), à la vie privée, à la sécurité et aux obligations légales/contractuelles.

4.5.3 L’ER doit avoir des documents de procédure pour maintenir dans le même état le matériel et les logiciels auparavant validés conformément à l’article précédent (4.5.2).

4.5.4 L’ER doit avoir des documents de procédure pour maintenir et contrôler l’utilisation des systèmes informatiques afin de consigner les données dans le cadre des activités de recherche. (Voir les exigences en matière de capacités aux paragraphes 4.8.7 h), k) et m).)

4.6 Qualité des données

4.6.1 L’ER doit s’assurer que les Investigateurs/Chercheurs ont des documents de procédure pour gérer les données tout au long de leur cycle de vie tel que :

- leur exactitude
- leur validité
- leur traçabilité
- leur exhaustivité
- leur unicité (non-redondance)
- leur cohérence

4.6.2 L’ER doit avoir des documents de procédure de maintien et de contrôle de l’utilisation des systèmes informatiques qui stockent les données consignées. (Voir les exigences en matière de capacités aux paragraphes 4.8.7 e) et n).)

4.7 Conformité et amélioration de la qualité

4.7.1 L’ER doit avoir des documents de procédure pour évaluer et surveiller le respect, par les Investigateurs/Chercheurs, les partenaires et les tiers, de ses politiques et procédures, et s’assurer que ses procédures sont conformes aux lois, textes normatifs et NNC pertinents (voir NNC CAN/HRSO-300.01-2022 La conduite de la recherche avec des êtres humains, article 4.1.7 « Conformité et amélioration de la qualité »).

4.7.2 L’ER doit avoir des documents de procédure pour évaluer l’efficacité des résultats en matière de gouvernance des données tout au long de leur cycle de vie.

4.7.3 L’ER doit avoir des documents de procédure pour :

a) répondre aux incidents ou aux possibles incidents de non-conformité (p. ex., violation de la vie privée) en investiguant la situation, en limitant les conséquences, en remédiant au problème et en informant les parties touchées, tout en soulevant la problématique aux parties externes envers lesquels l'ER a des responsabilités, s'il y a lieu;

b) enquêter sur les secteurs de risques qui menacent la capacité à demeurer conforme et en atténuer la portée; et

c) surveiller tous les incidents réels et présumés.

4.8 Vie privée et mesures de sécurité

Puisque la gestion sécuritaire des données est devenue très complexe, il revient à l'ER de s'assurer que les Investigateurs/Chercheurs gèrent leurs données de recherche dans des environnements privés et sécuritaires. À l'échelle de l'ER, la sécurité des données revient aux mesures et aux capacités de protection des données en place.

4.8.1 L'ER doit avoir des documents de procédure pour obtenir et offrir les services de personnes qualifiées et spécialisées ayant l'expertise, l'expérience et les autorisations pour appliquer, mettre en place et gérer des mesures de protection de la vie privée et de sécurité dans toutes les banques de données et tout au long du cycle de vie des données de recherche, à la hauteur du mandat confié par l'ER (voir l'article 4.1.3, les paragraphes 4.1.4 e), f) et g), et l'article 4.4).

4.8.2 L'ER doit avoir des documents de procédure pour évaluer les exigences de formation sur la vie privée et la sécurité conformément au type de recherche réalisée, dont les exigences suivantes :

a) CAN/DGSI 104:2021/Rev1:2024 Contrôles de cybersécurité de base des petites et moyennes organisations, article 4.3;

b) CAN/DGSI 118 Cybersécurité : cyberrésilience en santé, article 5.

4.8.3 L'ER doit avoir des documents de procédure pour s'assurer que les personnes détenant un accès direct ou indirect aux données durant leur cycle de vie :

a) ont un motif valable pour y accéder, et que ce dernier respecte le protocole approuvé par le CER ainsi que le plan de gestion des données applicables, et qu'elles ont obtenu le consentement pour utiliser les données;

b) ont été soumises à un examen diligent, y compris à la vérification appropriée des antécédents;

c) ont signé les documents fournis par l'ER concernant la non-divulgation des renseignements confidentiels ainsi qu'une déclaration de conflits d'intérêts et de rôles;

d) sont supervisées et ont reçu la formation nécessaire; et

e) ont un accès contrôlé et surveillé aux données de recherche.

(Voir l’article 4.4 *Accès aux données* et NNC CAN/HRSO-300.01-2022 La conduite de la recherche avec des êtres humains, article 4.1.2 « Qualifications et formation des Personnes qui jouent un rôle dans l'ER ».)

4.8.4 L’ER doit avoir des documents de procédure pour fournir et utiliser des environnements privés et sécuritaires, qu’ils soient gérés directement par elle, par un Fournisseur ou par une autre entité sous contrat. Si l’ER compte sur des Fournisseurs ou des Sous-traitants pour fournir de tels environnements, consultez l’article 4.5 Validation des systèmes de données.

4.8.5 L’ER doit avoir des documents de procédure indiquant les exigences en matière d’expertise et de formation sur la vie privée et la sécurité qui correspondent au type de recherche réalisée au sein de l’organisation ainsi qu’au rôle des stagiaires.

4.8.6 L’ER doit avoir des documents de procédure pour évaluer les risques, dans son contexte opérationnel, à chaque étape du cycle de vie des données. Parmi les risques pour la vie privée et la sécurité associés aux données de recherche, notons :

a) la perte, le vol ou la corruption des données (par des moyens comme les rançongiciels ou l’espionnage industriel);

b) le piratage psychologique ou les attaques similaires, comme l’hameçonnage;

c) les communications ou le transfert non sécuritaires de données (p. ex., lorsque les personnes n’utilisent pas de réseau privé virtuel ni d’authentification à deux facteurs); et

d) l’utilisation inappropriée de données, qu’elle soit accidentelle ou intentionnelle, par des personnes autorisées.

4.8.7 L’ER doit avoir des documents de procédure pour mettre en place des mesures de contrôle (physiques, techniques, procédurales) des risques ciblés à l’article 4.8.6. Voici des exemples de mesures pour contrer les risques liés à la vie privée et à la sécurité des données de recherche :

a) demander la modification des mots de passe par défaut;

b) installer des programmes automatisés de détection des mots de passe faibles ou compromis;

c) mettre place des procédures approuvées d’anonymisation des données de recherche identifiables;

d) gérer les espaces de travail;

e) gérer les postes de travail;

f) gérer les identités et l’accès; et

g) veiller à ce que les Fournisseurs de services tiers respectent les exigences.

4.8.8 L’ER doit avoir des documents de procédure pour mettre à profit et gérer les moyens qu’elle possède pour protéger la vie privée et assurer la sécurité. Voici des exemples de ces moyens :

a) un système dédié au stockage et à la gestion sécuritaires de l'information sensible, comme des mots de passe, des jetons d'API et des identificateurs de bases de données;

b) un système de signatures numériques pour obtenir la signature vérifiée des participants;

c) un système pour gérer le consentement donné par les participants;

d) des méthodes de gestion des processus pour faciliter l'ajout et le retrait d'accès utilisateurs en temps opportun;

e) un système dédié pour générer, stocker et gérer les clés de chiffrement utilisées pour le chiffrement, le déchiffrement et d'autres opérations cryptographiques;

f) un système centralisé de gestion des identités et de contrôle des accès aux ressources;

g) un système centralisé de gestion des identités dans divers domaines ou organisations pour permettre aux utilisateurs d'accéder aux ressources et aux services sans avoir besoin de comptes distincts dans chaque domaine (fédération d'identités);

h) un service de gestion de la position en matière de cybersécurité pour surveiller et évaluer en continu les pratiques et les mesures de contrôle de la sécurité mises en place pour protéger les données et les systèmes de recherche;

i) un système centralisé pour gérer et administrer les contrats conclus entre les parties;

j) un système centralisé pour colliger, analyser et surveiller systématiquement les journaux d'audit et les activités dans différents systèmes, applications et répertoires de données;

k) un système de gestion des versions de documents pour garantir le contrôle, la traçabilité et la collaboration par rapport à l'historique des documents, y compris les pistes de vérification complètes et la documentation connexe;

l) un système centralisé pour faciliter l'échange sécuritaire et efficace des données entre diverses parties autorisées, qu'elles soient internes ou externes à l'ER;

m) un ou des postes de travail ou environnements informatiques conçus et configurés spécialement pour fournir un accès sécuritaire aux données sensibles;

n) un système de gestion des processus pour pouvoir répéter et coordonner des processus et des flux de travail complexes; et

o) au besoin, un système pour gérer, sécuriser et surveiller efficacement les interfaces de programmation d'applications (API) qui permettent de transférer des données et des services entre systèmes et applications.

Voir les exemples de mesures de contrôle de base de la sécurité à l'annexe C.

4.8.9 L'ER doit avoir des documents de procédure lui permettant de s'assurer que les parties concernées connaissent les capacités décrites à l'article 4.8.8 ci-dessus.

4.8.10 L'ER doit avoir des documents de procédure pour réviser et mettre à jour les mesures de contrôle et les capacités décrites ci-dessus au moins tous les ans ou plus fréquemment en cas de changements majeurs (p. ex., nouvelles mesures de contrôle ou changement de Fournisseur).

4.8.11 L'ER doit avoir des documents de procédure pour collaborer avec les Communautés autochtones ou non autochtones afin de s'assurer :

a) que la gestion sécuritaire des données ne constitue pas un fardeau pour elles; et

b) qu'elles ont accès aux ressources requises pour leurs besoins en infrastructures.

4.8.12 L'ER doit avoir des documents de procédure décrivant les méthodes de disposition à long terme des données de recherche (p. ex., destruction sécurisée, anonymisation irréversible, archivage).

Annexes informatives

Les références qui suivent ont été prises en considération lors de l’élaboration de la présente NNC et peuvent aider les lecteurs à comprendre les concepts qui y sont traités.

Annexe A : Références informatives

Thompson, Kristi; Elizabeth Hill; Emily Carlisle-Johnston; Danielle Dennie et Émilie Fortin. « Research Data Management in the Canadian Context: A Guide for Practitioners and Learners ». Publié par Pressbooks. La version originale est disponible gratuitement sous les conditions de la licence CC BY-NC 4.0 au https://ecampusontario.pressbooks.pub/canadardm.

Annex B : Exemples de cycles de vie des données de recherche (Informatif)

Tayler, Felicity; Marjorie Mitchell; Chantal Ripp et Pascale Dangoisse. « Data Primer : Making Digital Humanities Research Data Public », 2022, Annexe 1, https://ecampusontario.pressbooks.pub/dataprimer/front-matter/annex-1-data-flow-and-discovery-model/. Fait référence aux éléments suivants : consentement, collecte de données, traitement des données, analyse critique, transmission et préservation.

National Institutes of Health des États-Unis, National Library of Medicine. « Research Lifecycle », https://www.nnlm.gov/guides/data-glossary/research-lifecycle. Fait référence aux éléments suivants du cycle de vie de la recherche : plan, acquisition, traitement, analyse, préservation, transmission des résultats et réutilisation.

Department of Commerce des États-Unis, National Institute of Standards and Technology (NIST). « Research Data Framework », NIST SP 1500-18r2, version 2.0, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/1500-18/NIST.SP.1500-18r2.html. Fait référence aux éléments suivants : vision, plan, génération/acquisition, traitement/analyse, transmission/utilisation/réutilisation et préservation/élimination.

Winter, Caroline. « The Current State of Research Data Management in Canada: A Report by the Digital Research Alliance of Canada » (Alliance de recherche numérique du Canada). Open Scholarship Policy Observatory, 3 décembre 2021, https://ospolicyobservatory.uvic.ca/current-state-of-rdm/. Fait référence aux éléments suivants : planification, création, traitement, analyse, dissémination, préservation et réutilisation.

Annexe C : Contrôles de sécurité de base (Informatif)

Ces mesures de contrôle sont basées sur la version 8 des contrôles de sécurité critiques du Center for Internet Security (CIS Critical Security Controls). La liste des contrôles figurant dans la présente norme constitue une ligne directrice pour savoir comment et quand les contrôles devraient être utilisés à divers degrés d'après la perspective d'une ER. Consultez la version 8 du document sur les contrôles du CIS pour en savoir plus sur chaque mesure et sa mise en place.

Les contrôles de cybersécurité de niveau 1 ont un rôle essentiel : ils constituent une protection de base solide pour les ERs, sans égard à la sensibilité de leurs données. Ces mesures de contrôle fondamentales visent l'établissement de pratiques de sécurité indispensables pour se munir d'une protection robuste contre une large gamme de cybermenaces. En mettant l'accent sur les aspects fondamentaux, ces mesures jettent les bases d'une position solide en matière de sécurité sur laquelle des mesures plus poussées peuvent être ajoutées. À l'ère où les cybermenaces et la fuite de données évoluent constamment, les entreprises qui adoptent des mesures de contrôle de la cybersécurité de niveau 1 font preuve de proactivité et de prudence; elles réduisent leurs risques et assurent la confidentialité, l'intégrité, et la disponibilité de leurs précieuses données de recherche.

Les contrôles de cybersécurité de niveau 2 rehaussent le degré de protection des ERs avec des mesures de sécurité renforcées, précaution indispensable pour les organisations manipulant des données sensibles. Ces contrôles réunissent un ensemble plus avancé de pratiques et de technologies de protection des données sensibles de divers types, comme les renseignements personnels identificatoires, les dossiers médicaux, la propriété intellectuelle et les résultats de recherche classifiés. Par exemple, si l'on applique les contrôles de niveau 2 dans une ER en soins de santé, on mettra à l'essai les mesures de sécurité et on vérifiera si les Fournisseurs de services respectent les exigences de sécurité. Ces mesures de contrôle contribuent non seulement à prévenir les fuites de données, mais également à renforcer la résilience générale des ERs en leur permettant de répondre à des exigences de conformité strictes et de garder la confiance des intervenants, des collaborateurs et des personnes à qui appartiennent les données sensibles. Essentiellement, les contrôles de cybersécurité de niveau 2 sont un investissement essentiel au maintien de l'intégrité et de la sécurité des données de recherche critiques.

N.B : Il n'est pas question, dans la présente norme, des contrôles de cybersécurité au regard de la création d'applications. Les ERs qui créent par ailleurs une application ou une composante d'application qui interagira avec des données de recherche devraient aussi s'informer des mesures de contrôle suivantes :

- Article 16 du CIS
- ASVS (Application Security Verification Standard) de l'OWASP

Les contrôles de sécurité critiques du CIS adaptés aux ERs

Numéro de CIS	Titre/Description	Niveau 1	Niveau 2
1.1	Créer et tenir à jour un inventaire détaillé des actifs de l'entreprise	X	X
1.2	Gérer les actifs non autorisés	X	X
1.3	Utiliser un outil d'investigation active		X
2.1	Créer et tenir à jour un inventaire de logiciels	X	X
2.2	Veiller à ce que les logiciels autorisés soient supportés au moment de leur utilisation	X	X
2.3	Gérer les logiciels non autorisés	X	X
2.4	Utiliser des outils d'inventaire de logiciels automatisés		X
2.5	Créer une liste des logiciels autorisés		X
2.6	Créer une liste des bibliothèques autorisées		X
3.1	Créer et tenir à jour un processus de gestion des données	X	X
3.2	Créer et tenir à jour un inventaire des données	X	X
3.3	Configurer des listes de contrôle de l'accès aux données	X	X
3.4	Exiger la conservation des données	X	X
3.5	Disposer des données de façon sécuritaire	X	X
3.6	Chiffrer les données sur les appareils des utilisateurs finaux	X	X
3.7	Créer et tenir à jour un plan de classification des données	X	X
3.8	Documenter le flux des données	X	X
3.9	Chiffrer les données sur les unités amovibles	X	X
3.10	Chiffrer les données sensibles en transit	X	X
3.11	Chiffre les données sensibles au repos	X	X
3.12	Segmenter le traitement et le stockage des données en fonction de leur sensibilité		X
3.13	Déployer une solution de prévention de la perte des données		X
3.14	Consigner les accès aux données sensibles	X	X
4.1	Mettre en place et maintenir un processus de configuration sécuritaire	X	X
4.2	Mettre en place et maintenir un processus de configuration sécuritaire de l'infrastructure réseau	X	X

Numéro de CIS	Titre/Description	Niveau 1	Niveau 2
4.3	Configurer le verrouillage automatique des sessions sur les actifs de l'entreprise	X	X
4.4	Installer et gérer un pare-feu sur les serveurs	X	X
4.5	Installer et gérer un pare-feu sur les appareils des utilisateurs finaux	X	X
4.6	Gérer de façon sécuritaire les actifs et les logiciels de l'entreprise	X	X
4.7	Gérer les comptes par défaut sur les actifs et dans les logiciels de l'entreprise	X	X
4.8	Désinstaller ou désactiver les services superflus sur les actifs de l'entreprise	X	X
4.9	Configurer des serveurs de DNS fiables sur les actifs de l'entreprise		X
4.10	Exiger le verrouillage automatique des appareils portables des utilisateurs finaux		X
4.11	Faire installer une fonctionnalité d'effacement des données à distance sur les appareils portables des utilisateurs finaux		X
5.1	Créer et tenir à jour un inventaire des comptes	X	X
5.2	Utiliser des mots de passe uniques	X	X
5.3	Désactiver les comptes inutilisés	X	X
5.6	Centraliser la gestion des comptes	X	X
5.7 (nouveau)	Configurer l'authentification étape par étape, adaptative ou « juste à temps » pour les administrateurs		X
6.1	Établir un processus d'attribution des accès	X	X
6.2	Établir un processus de révocation des accès	X	X
6.3	Exiger l'authentification à facteurs multiples (AFM) pour les applications exposées à l'externe	X	X
6.4	Exiger l'AFM pour l'accès aux réseaux à distance	X	X
6.5	Exiger l'AFM pour les accès administratifs	X	X
6.7	Centraliser le contrôle des accès	X	X
6.8	Définir et maintenir le contrôle des accès basé sur les rôles	X	X
7.1	Établir et maintenir un processus de gestion des vulnérabilités		X
7.2	Établir et maintenir un processus de remédiation		X
7.3	Mettre en place la gestion automatisée des correctifs des systèmes d'exploitation	X	X

Numéro de CIS	Titre/Description	Niveau 1	Niveau 2
7.4	Mettre en place la gestion automatisée des correctifs d'applications	X	X
7.5	Mettre en place des analyses automatisées des vulnérabilités des actifs internes de l'entreprise		X
7.6	Mettre en place des analyses automatisées des vulnérabilités des actifs de l'entreprise exposés à l'externe		X
7.7	Résoudre les vulnérabilités détectées		X
8.1	Établir et maintenir un processus de gestion des journaux de vérification	X	X
8.2	Recueillir les journaux de vérification	X	X
8.3	Veiller au stockage adéquat des journaux de vérification	X	X
8.4	Recueillir les journaux de vérification détaillés	X	X
8.9	Centraliser les journaux de vérification		X
8.10	Conserver les journaux de vérification		X
8.11	Réaliser des examens des journaux de vérification		X
8.12	Recueillir les journaux des Fournisseurs de services		X
9.1	Veiller à ce que seuls des navigateurs et des logiciels de courriel entièrement supportés soient utilisés	X	X
9.2	Utiliser des services de filtrage DNS		X
9.3	Maintenir et appliquer des filtres d'URL sur les réseaux		X
9.4	Restreindre l'utilisation d'extensions de navigateurs ou de logiciels de courriel superflue ou non autorisée		X
9.5	Mettre en place un protocole DMARC		X
9.6	Bloquer les types de fichiers superflus	X	X
9.7	Déployer et maintenir des mesures de protection anti-malicielles des serveurs de courriels	X	X
10.1	Déployer et maintenir un logiciel anti-maliciel	X	X
10.2	Configurer des mises à jour automatiques anti-malicielles des signatures	X	X
10.3	Désactiver l'ouverture et la lecture automatique des unités amovibles	X	X
10.4	Configurer l'analyse anti-malicielle automatique des unités amovibles		X
10.5	Mettre en place une fonctionnalité anti-exploitation		X

Numéro de CIS	Titre/Description	Niveau 1	Niveau 2
10.6	Gérer de façon centralisée les logiciels anti-maliciels		X
10.7	Utiliser des logiciels anti-maliciels basés sur les comportements		X
11.1	Établir et maintenir un processus de récupération des données	X	X
11.2	Mettre en place des copies de sauvegarde automatisées	X	X
11.3	Protéger les données de récupération	X	X
11.4	Créer et conserver des copies isolées des données de récupération		X
11.5	Tester la récupération des données		X
12.1	Veiller à ce que l'infrastructure réseau soit à jour	X	X
12.2	Établir et maintenir une architecture réseau sécuritaire		X
12.3	Gérer l'infrastructure réseau de façon sécuritaire		X
12.4	Créer et converser des diagrammes de l'architecture		X
12.5	Centraliser la connexion aux réseaux, et les autorisations et les vérifications en lien avec les réseaux		X
12.6	Suivre des protocoles de gestion des réseaux et de communication avec les réseaux sécuritaires		X
13.1	Centraliser les alertes d'événements de sécurité		X
13.2	Déployer une solution de détection des intrusions par l'hôte		X
13.3	Déployer une solution de détection des intrusions dans les réseaux		X
13.4	Effectuer le filtrage du trafic entre les segments réseau		X
13.5	Gérer le contrôle des accès aux actifs à distance		X
13.6	Recueillir les journaux de trafic des réseaux		X
13.10	Filtrer les couches application		X
14.1	Mettre et maintenir en place un programme de sensibilisation à la sécurité	X	X
14.2	Enseigner au personnel à reconnaître les attaques de piratage psychologique	X	X
14.3	Enseigner les pratiques exemplaires d'authentification au personnel	X	X
14.4	Enseigner les pratiques exemplaires de manipulation des données au personnel	X	X

Numéro de CIS	Titre/Description	Niveau 1	Niveau 2
14.5	Enseigner au personnel les causes d'exposition involontaire des données	X	X
14.6	Enseigner au personnel à reconnaître et à signaler les incidents de sécurité	X	X
14.7	Montrer au personnel comment voir si des mises à jour de sécurité des actifs de l'entreprise ont été omises et comment le signaler	X	X
14.8	Enseigner au personnel les dangers d'une connexion à un réseau non sécurisé et de la transmission de données d'entreprise sur un tel réseau	X	X
14.9	Sensibiliser les employés à la sécurité liée à chaque rôle et leur enseigner les compétences connexes		X
15.1	Créer et tenir à jour un inventaire des Fournisseurs de services	X	X
15.2	Créer et tenir à jour une politique de gestion des Fournisseurs de services		X
15.3	Classifier les Fournisseurs de services		X
15.4	Veiller à ce que les contrats des Fournisseurs de services décrivent les exigences de sécurité		X
16.4	Créer et gérer un inventaire des composants logiciels tiers	X	X
16.5	Utiliser des composants logiciels tiers à jour et fiables	X	X
17.1	Désigner du personnel pour gérer le traitement des incidents	X	X
17.2	Définir et mettre à jour les coordonnées pour le signalement des incidents de sécurité	X	X
17.3	Établir et maintenir un processus pour signaler les incidents au sein de l'entreprise	X	X
17.4	Établir et maintenir un processus de réponse aux incidents	X	X
17.5	Assigner les rôles et responsabilités principaux		X
17.6	Définir les mécanismes de communication durant la réponse aux incidents		X
17.7	Réaliser des exercices réguliers de réponse aux incidents		X
17.8	Réaliser des bilans des incidents		X
18.1	Mettre sur pied et maintenir un programme de tests d'intrusion		X
18.2	Réaliser des tests périodiques d'intrusion externe		X
18.3	Régler les problèmes détectés lors des tests d'intrusion		X
18.4	Valider les mesures de sécurité		X

Numéro de CIS	Titre/Description	Niveau 1	Niveau 2
18.5	Réaliser des tests périodiques d’intrusion interne		X