Guide sur l'utilisation responsable de l'IA : **Protection des renseignements personnels**

Janvier 2026

transformation numérique

CHU Sainte-Justine
Le centre hospitalier universitaire mère-enfant

Université de Montréal

Ce guide, basé sur la politique de gouvernance des renseignements personnels du CHUSJ, énonce les bonnes pratiques généralement reconnues en matière de protection des renseignements personnels dans l'objectif d'utiliser l'intelligence artificielle de manière responsable. En plus de respecter les bonnes pratiques énoncées dans le présent guide, l'utilisation de renseignements personnels dans le cadre d'un projet d'intelligence artificielle doit être effectuée conformément au cadre légal applicable ainsi qu'aux politiques, procédures et directives du CHU Sainte-Justine.

Chaque projet ayant recours à l'intelligence artificielle est unique. Une analyse rigoureuse de chaque projet est nécessaire afin d'en assurer sa conformité, tel qu'énoncé à la Procédure sur les projets d'intelligence artificielle impliquant des renseignements personnels.

Au-delà du présent guide, d'autres ressources en matière de protection des renseignements personnels sont disponibles au CHU Sainte-Justine. Consultez notre section Intranet : intranet.chusj.org/confidentialite

En cas de question relative au présent guide ou aux bonnes pratiques en matière de protection des renseignements personnels, nous vous invitions à contacter l'équipe PRP de la Direction qualité, évaluation, performance et éthique par courriel : protection.renseignements.personnels.hsj@ssss.gouv.qc.ca

Ce guide a été rédigé avec l'aide de l'intelligence artificielle.

1. Introduction

L'intelligence artificielle (IA) transforme les pratiques cliniques, administratives et de recherche. Cette innovation constitue un levier pour propulser la transformation numérique du CHU Sainte-Justine en nous offrant l'opportunité de revoir et de moderniser nos méthodes de travail. Afin de tirer pleinement les bénéfices de l'IA, il est nécessaire de connaitre et de réduire les risques qui y sont associés.

L'utilisation et le déploiement de l'IA comportent certains risques en matière de protection des renseignements personnels (PRP). Afin d'atténuer ces risques et de protéger la vie privée des personnes concernées, certaines règles doivent être respectées. Ces règles sont présentées dans ce guide sous forme de bonnes pratiques. Le présent guide est structuré comme suit :

- Principes généraux de PRP
- Principaux risques de PRP liés à l'utilisation de l'IA
- Bonnes pratiques relatives à l'utilisation de l'IA
- Gestion d'un incident de confidentialité

Ce guide se fonde sur le cadre normatif applicable ainsi que sur les principes généraux de protection des renseignements personnels.

2. Principes généraux de protection des renseignements personnels

Le CHU Sainte-Justine s'est doté de principes généraux de PRP afin d'encadrer et de guider les pratiques des personnes qui y œuvrent. Ces principes s'appliquent lorsqu'une personne travaille avec des renseignements personnels, incluant notamment les situations où elle utilise l'IA.

Nécessité

Seuls les renseignements personnels nécessaires à l'atteinte des objectifs visés par un projet doivent être collectés, utilisés, conservés ou communiqués par le CHU Sainte-Justine. Le respect du principe de nécessité permet de limiter les atteintes au droit à la vie privée. Ce principe doit être appliqué à la lumière de la sensibilité des renseignements personnels concernés.

Dépersonnalisation et anonymisation

Lorsqu'il est possible d'utiliser ou de communiquer un renseignement personnel sous une forme ne permettant pas d'identifier, directement ou indirectement, la personne concernée, l'utilisation ou la communication doit se faire sous cette forme. L'utilisation de renseignements dépersonnalisés[1] ou anonymisés[2] doit alors être privilégiée.

Confidentialité

Tout renseignement personnel doit être traité de manière confidentielle dans le respect des règles prévues par les lois applicables et, lorsque requis, du consentement de la personne concernée. L'accès à un tel renseignement est permis seulement aux personnes pour lesquelles cet accès est autorisé par les règles applicables et nécessaire à l'exercice de leurs fonctions.

Obligation déontologique

Chaque professionnelle et professionnel a l'obligation déontologique de respecter le secret de tout renseignement de nature confidentielle qui vient à sa connaissance dans l'exercice de sa profession.

Sécurité

Tout renseignement personnel doit être collecté, utilisé, conservé, communiqué, détruit ou anonymisé de façon sécuritaire. Des mesures de sécurité rigoureuses selon les circonstances doivent être mises en place et respectées par toutes les utilisatrices et tous les utilisateurs afin de protéger la confidentialité des renseignements personnels, et ce, tant au niveau physique qu'informatique.

Destruction

Dès que les fins pour lesquelles un renseignement personnel a été collecté ou conservé sont accomplies, le renseignement personnel doit être détruit, sous réserve des autres normes applicables, dont le calendrier de conservation de Santé Québec. Il peut également être anonymisé en respect des règles applicables. Par exemple, pour les projets de recherche, il n'est pas autorisé de détruire les renseignements personnels collectées ou utilisées sans respecter le délai de conservation prescrit par le calendrier de conservation de Santé Québec.

[1] Un renseignement dépersonnalisé est un renseignement personnel permettant d'identifier une personne de façon indirecte.

[2] Un renseignement anonymisé ne permet pas d'identifier une personne, même indirectement. Il n'est donc pas un renseignement personnel.

3. Principaux risques

L'utilisation et le déploiement de l'IA au sein d'une organisation de santé et de services sociaux entrainent certains risques liés à la PRP. Voici les risques principaux :

Communication non autorisée de renseignements personnels au fournisseur d'un outil d'IA

Les outils d'IA se fondent généralement sur l'entrainement de modèles effectué à partir de données massives. Plusieurs outils d'IA en ligne sont offerts gratuitement (ex. : ChatGPT, DeepL, DeepSeek, etc.) au détriment de la protection des informations qui y sont intégrées. Ces informations, même si elles sont confidentielles, sont généralement communiquées au fournisseur de l'outil en ligne afin de bonifier sa base de données massives visant l'entraînement et l'amélioration de son outil d'IA. La confidentialité des informations intégrées dans un outil d'IA en ligne gratuit n'est donc généralement pas respectée. Ces informations pourraient être rendues publiques ou transmises par l'outil d'IA en réponse à une ou un autre utilisateur de cet outil.

Fuite de renseignements personnels

Une fuite de renseignements personnels pourrait survenir en raison de l'intégration de renseignements personnels dans un outil d'IA non autorisé (par exemple, un fournisseur d'outil d'IA en ligne gratuit) ou en raison d'une brèche de sécurité dans un outil d'IA non sécurisé.

Utilisation non autorisée de renseignements personnels pour le développement d'un outil d'IA

L'utilisation de renseignements personnels pour développer et entrainer un outil d'IA nécessite l'autorisation du CHU Sainte-Justine par le biais du Comité d'approbation des projets d'intelligence artificielle ou une autre instance ayant reçue la délégation du Comité d'approbation. L'utilisation des renseignements personnels à cette fin doit être autorisée par la loi ou par le biais d'un consentement libre et éclairé de la personne concernée. De plus, d'autres processus d'autorisation peuvent être nécessaires, par exemple une évaluation des facteurs relatifs à la vie privée (EFVP).

Collecte ou utilisation excessive de renseignements personnels

En PRP, le principe de nécessité exige que seuls les renseignements personnels nécessaires à un projet ou une fin prédéterminée puissent être collectés ou utilisés. Ce principe, qui vise à limiter l'atteinte au droit à la vie privée, peut entrer en contradiction avec le développement et l'entrainement d'outils d'IA, lesquels exigent des données massives.

Une évaluation rigoureuse de chaque projet doit être effectuée afin de respecter le principe de nécessité et les autres principes de PRP applicables.

4. Utilisation de l'IA : bonnes pratiques

Toute personne qui utilise l'IA doit agir avec **prudence** et **vigilance**. Elle doit respecter les bonnes pratiques énoncées ci-dessous.

Pratiques à adopter	Pratiques à éviter
Verser ou intégrer des renseignements personnels ou autres informations confidentielles uniquement dans les **outils d'IA autorisés** (ex. Copilot à partir d'un compte Microsoft O365) par le CHU Sainte-Justine.	Verser ou intégrer des renseignements personnels ou autres informations confidentielles dans un outil d'IA non autorisé (ex. ChatGPT, DeepL, DeepSeek, etc.) par le CHU Sainte-Justine.
Privilégiez l'utilisation des outils IA dans le cadre de votre travail **sur un appareil corporatif.**	Utiliser l'outil d'IA sur un appareil personnel sans autorisation.
Utiliser l'outil d'IA sur un **réseau sécurisé**, tel que le réseau du CHU Sainte-Justine.	Utiliser un outil d'IA sur un réseau non sécurisé, tel qu'un réseau Wifi public.
Lorsque l'outil d'IA le requiert, utiliser un **mot de passe robuste et sécuritaire**.	Choisir un mot de passe simple ou fréquemment utilisé.
En cas d'intégration de renseignements personnels dans un outil d'IA autorisé (ex. Copilot à partir d'un compte Microsoft O365), **n'intégrer que les renseignements personnels nécessaires** à l'objectif poursuivi et préalablement déterminé.	Intégrer des renseignements personnels non nécessaires dans un outil d'IA, ce qui augmente inutilement le risque de bris de confidentialité.
Favoriser l'intégration, dans un outil d'IA autorisé, de **renseignements anonymisés ou dépersonnalisés**.	Intégrer, dans un outil d'IA autorisé, des renseignements personnels avec des identifiants directs, tel que le nom d'une personne, sans que cela soit nécessaire.
Lorsque vous obtenez ou créez une copie de renseignements personnels, ou encore lorsque vous collectez des renseignements personnels, **détruire dès que possible ces renseignements personnels**.	Conserver une copie de renseignements personnels alors que ceux-ci ne sont plus nécessaires au projet, ce qui augmente inutilement le risque de bris de confidentialité.

Lorsque pertinent et possible selon les circonstances, **informer toute personne concernée** de l'intégration de ses renseignements personnels dans un outil d'IA.	Omettre d'informer les personnes concernées de l'intégration de leurs renseignements personnels dans un outil d'IA, ce qui peut compromettre la confiance à l'égard du CHU Sainte-Justine.
Déclarer tout incident de confidentialité ou toute intégration de renseignements personnels dans un outil d'IA non autorisé, afin que les équipes concernées puissent prendre les mesures requises pour éviter ou diminuer le risque de préjudice.	Ne pas déclarer un incident de confidentialité ou une intégration de renseignements personnels dans un outil d'IA non autorisé.
S'informer et maintenir à jour ses connaissances relativement aux **exigences en matière de PRP et d'IA**, notamment celles énoncées par le CHUSJ et son ordre professionnel.	Utiliser l'IA en ne s'informant pas des exigences en matière de PRP qui y sont liées.
S'informer et maintenir à jour ses connaissances relativement aux **limites et risques d'un outil d'IA**, notamment en ce qui concerne la PRP.	Utiliser un outil d'IA en ne connaissant pas les limites et les risques de cet outil.
En cas de question, **se référer à sa gestionnaire ou son gestionnaire**.	Utiliser l'IA de façon non responsable et ne pas adresser ses questions par peur de la critique.

Veuillez consulter l'Annexe 1 pour une liste des questions à se poser afin d'utiliser l'IA de manière à respecter les exigences relatives à la PRP.

Utilisation de Microsoft Copilot

Copilot est un outil de Microsoft basé sur l'IA. Il vise à fournir une assistance au personnel en temps réel.

Copilot est un outil sécurisé et autorisé par le CHU Sainte-Justine, **lorsqu'il est utilisé à partir d'un compte Microsoft O365 professionnel**. Sur un compte professionnel Microsoft O365, la politique de protection des données de Microsoft O365 s'applique et les renseignements personnels intégrés dans Copilot sont protégés de la même façon que ceux échangés via les autres outils de Microsoft O365, tels que Teams et Outlook.
Chaque fois où des renseignements personnels ou d'autres informations confidentielles sont intégrés dans Copilot, il est nécessaire de préalablement vérifier que c'est bien le

compte professionnel Microsoft O365 qui est utilisé. En cas de doute sur la connexion, s'abstenir d'intégrer des renseignements personnels ou d'autres informations confidentielles dans Copilot.

Afin de s'assurer que la personne qui l'utilise est bel et bien dans le compte Microsoft O365 professionnel, la présence de l'un ou l'autre des éléments suivants dans le coin supérieur droit de la fenêtre Copilot doit être validé :

- Les initiales de l'utilisatrice ou utilisateur
- La photographie personnelle de l'utilisatrice ou utilisateur
- Le crochet vert 

Cas pratique #1

Un membre de l'équipe médicale souhaite utiliser un outil d'IA dans le cadre de la rédaction de ses notes cliniques. L'outil d'IA identifié par ce dernier enregistre chaque consultation médicale avec ses patientes et patients et rédige une note clinique résumant la consultation afin que celle-ci puisse être déposée au dossier médical.

Soucieux de la confidentialité, ce membre de l'équipe médicale s'est assuré de choisir un outil d'IA pour lequel le fournisseur affirme respecter les exigences en protection des renseignements personnels et achète donc une licence de cet outil sans autre formalité.

Commentaires :

✗ Toute personne œuvrant au CHU Sainte-Justine a l'obligation d'utiliser uniquement les produits et services technologiques autorisés par l'établissement. Dans le cadre du processus d'autorisation d'un produit ou service technologique, le CHU Sainte-Justine s'assure que les exigences en matière de PRP et de sécurité de l'information sont respectées.

✓ L'intégration de renseignements personnels dans un **outil d'IA autorisé** permettant la rédaction de notes cliniques est possible puisque ces renseignements sont nécessaires à l'objectif poursuivi.

Cas pratique #2

Un membre du personnel administratif souhaite augmenter sa capacité de réponse aux courriels qu'il reçoit. De plus, il s'agit d'une tâche qui l'ennuie. Cet employé administratif décide donc d'avoir recours à l'utilisation de l'IA pour l'aider dans son travail, plus particulièrement en lien avec la rédaction de réponses à ses courriels. Pour ce faire, il choisit l'outil ChatGPT, accessible gratuitement en ligne et y copie de façon intégrale les courriels qu'il reçoit, lesquels contiennent souvent des informations confidentielles, et demande à ChatGPT de produire une réponse selon les grandes lignes demandées.

Commentaires :

✗ Toute personne œuvrant au CHU Sainte-Justine a l'obligation d'utiliser uniquement les produits et services technologiques autorisés par l'établissement. ChatGPT n'est pas un outil autorisé pour y intégrer des renseignements personnels ou d'autres informations confidentielles. L'outil à utiliser est plutôt Microsoft Copilot, à partir d'un compte Microsoft O365.

✓ L'intégration de renseignements personnels ou d'autres informations confidentielles dans un **outil d'IA autorisé** (ex. : Copilot à partir d'un compte Microsoft O365) permettant la rédaction de réponses à des courriels est possible puisque ces renseignements sont nécessaires à l'objectif poursuivi.

Considérations supplémentaires concernant la création et/ou l'entraînement d'outils d'IA

La création et/ou l'entraînement d'outils d'IA nécessitent la mise en place de mesures de sécurité et de protection des renseignements personnels supplémentaires, telles que :

- Favoriser l'utilisation de renseignements anonymisés lors des tests ou entraînements. S'il est impossible d'utiliser des renseignements anonymisés, des renseignements dépersonnalisés peuvent être utilisés. Aucun identifiant direct ne peut être utilisé pour effectuer des tests ou des entraînements, à moins d'avoir reçu une autorisation expresse à cet effet.
- Obtenir l'autorisation du CHU Sainte-Justine pour la collecte ou l'utilisation de renseignements personnels à des fins de développement ou d'entrainement d'un outil d'IA. Le consentement de la personne concernée peut également être exigé en fonction des dispositions légales applicables.
- Conserver les renseignements personnels de façon sécuritaire et confidentielle, ce qui implique notamment d'assurer une saine gestion des accès à ces renseignements et de les conserver sur des serveurs sécurisés.
- Utiliser des environnements sécurisés pour l'entraînement de l'outil d'IA.

- Détruire de façon sécuritaire et définitive les renseignements personnels lorsqu'ils ne sont plus nécessaires au développement ou à l'entraînement de l'outil d'IA. Pour les projets de recherche, il n'est pas autorisé de détruire les renseignements personnels collectées ou utilisées sans respecter le délai de conservation prescrit par le calendrier de conservation applicable (Calendrier de conservation de Santé Québec).
- S'assurer que tout contrat conclu avec un fournisseur contienne les clauses contractuelles appropriées en regard de la PRP.
- Élaborer un plan pour déceler et réagir aux incidents de confidentialité découlant de l'utilisation de l'outil d'IA.
- Veiller à l'exactitude et la représentativité des données utilisées pour l'entraînement afin de minimiser les risques de biais des résultats générés par l'outil d'IA.

Tous les outils d'IA impliquant des renseignements personnels, même ceux créés au CHU Sainte-Justine, doivent être autorisés par l'organisation avant d'être utilisés et déployés, conformément à la Procédure sur les projets d'intelligence artificielle impliquant des renseignements personnels.

Cas pratique #3

Une équipe multidisciplinaire en génétique, alliant des membres des équipes de recherche et clinique, travaille depuis quelque temps sur la création d'un outil d'IA prédictive. Cette équipe a obtenu l'ensemble des autorisations et consentements nécessaires afin d'utiliser les renseignements dépersonnalisés et anonymisés pour développer et entrainer cet outil.

L'équipe souhaite rendre disponible l'outil d'IA prédictive à l'ensemble de leurs collègues du CHU Sainte-Justine afin que cette innovation puisse être utilisée au bénéfice des mères et des enfants du Québec. Comme l'ensemble des autorisations et consentements nécessaires à l'utilisation de données pour la création de cet outil ont été obtenus, l'équipe ne juge pas opportun d'obtenir des autorisations supplémentaires pour le déploiement de cet outil. L'utilisation de cet outil d'IA prédictive dans le cadre de la prestation de soins exige l'intégration de renseignements personnels dans l'outil afin d'obtenir un résultat personnalisé pour chaque patiente et patient.

L'équipe multidisciplinaire souhaite également collaborer avec des expertes et experts en éthique afin de former leurs collègues sur les risques de biais et de résultats discriminatoires découlant de l'utilisation de l'outil d'IA prédictive.

Commentaires :

- ✗ Toute personne œuvrant au CHU Sainte-Justine a l'obligation d'utiliser uniquement les produits et services technologiques autorisés par l'établissement. Le déploiement de cet outil nécessite donc une autorisation institutionnelle conformément à la Procédure sur les projets d'intelligence artificielle impliquant des renseignements personnels, laquelle concernera l'utilisation de cet outil dans le cadre de la prestation de soins. Ce processus d'autorisation permet au CHU Sainte-Justine de s'assurer que les exigences en matière de PRP et de sécurité de l'information sont respectées.

- ✓ L'intégration de renseignements personnels dans un **outil d'IA autorisé** pour appuyer les cliniciennes et les cliniciens dans leur évaluation du diagnostic ou pronostic est possible puisque ces renseignements sont nécessaires à l'objectif poursuivi.

- ✓ Il est nécessaire d'obtenir l'autorisation du CHU Sainte-Justine pour utiliser des renseignements personnels à des fins de développement ou d'entrainement d'un outil d'IA. Le consentement de la personne concernée peut également être exigé.

- ✓ L'utilisation de l'IA comporte des risques relatifs à des biais ou des résultats discriminatoires. Être conscient de ces risques et sensibiliser les équipes à cet effet permet de repérer plus facilement les biais potentiels et les résultats discriminatoires.

Considérations supplémentaires concernant les décisions fondées exclusivement sur un traitement automatisé de renseignements personnels

Lorsque des renseignements personnels sont utilisés afin de rendre une décision fondée exclusivement sur un traitement automatisé[3] de ceux-ci, donc sans intervention humaine, il est nécessaire d'en informer la personne concernée au plus tard au moment où elle est informée de cette décision.

La personne concernée a également le droit d'être informée :

- des renseignements utilisés pour rendre la décision;
- des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision;

[3] Pour en savoir davantage : GOUVERNEMENT DU QUÉBEC, Décision fondée exclusivement sur un traitement automatisé.

- de son droit de faire rectifier les renseignements utilisés pour rendre la décision.

Cette personne doit également avoir l'occasion de présenter ses observations à une personne en mesure de réviser la décision fondée exclusivement sur un traitement automatisé de ses renseignements personnels.

Qu'est-ce qu'une décision fondée exclusivement sur un traitement automatisé de renseignements personnels ?

Il s'agit d'une décision qui est prise sans aucune intervention humaine, c'est-à-dire qu'aucune personne n'a exercé un contrôle sur la décision finale. Les décisions fondées exclusivement sur un traitement automatisé de renseignements personnels font généralement appel à un algorithme décisionnel.

Par exemple, l'attribution des rendez-vous d'une clinique externe par un algorithme sur la base des renseignements de santé et de services sociaux préalablement saisis et ce, sans intervention ou vérification humaine, constitue une décision fondée exclusivement sur un traitement automatisé de renseignements personnels.

5. Que faire en cas d'incident de confidentialité ?

Un incident de confidentialité se produit en cas d'accès ou toute autre utilisation ou communication d'un renseignement personnel non autorisée par la loi, de perte d'un renseignement personnel ou de toute autre atteinte à sa protection. Le non-respect des bonnes pratiques énoncées dans le présent guide constitue généralement un incident de confidentialité.

Voici les étapes à suivre lorsque survient un incident de confidentialité :

1. Mettre fin à l'incident, le cas échéant.
2. Informer sa ou son gestionnaire ou la personne responsable du projet, selon le cas.
3. Prendre les mesures immédiates pour prévenir et/ou limiter le préjudice pouvant découler de l'incident, le cas échéant.
4. Prendre les mesures préventives nécessaires afin de s'assurer qu'un tel incident ne se reproduise plus.
5. Déclarer l'incident selon les modalités suivantes[4] :

[4] Lorsqu'un incident de confidentialité survient dans le cadre d'un projet de recherche où les participantes et participants sont également des patientes et patients du CHU Sainte-Justine, il est possible qu'une double déclaration soit nécessaire (via un AH-223 et un F8H).

- Pour un **incident impliquant des renseignements de santé** : déclaration via le formulaire AH-223 (Rapport de déclaration d'incident ou d'accident).
- Pour un **incident survenu lors d'une activité de recherche** : déclaration via le formulaire F8H à remplir dans le logiciel Nagano.
- Pour **tout autre incident de confidentialité** : déclaration via le Formulaire de déclaration d'un incident de confidentialité (autre que clinique et recherche).

Lorsque l'incident de confidentialité constitue également un **incident de sécurité de l'information**[5], la ou le gestionnaire concerné doit également déclarer cet incident au Centre opérationnel de sécurité informationnelle par le biais d'une requête via le portail Octopus.

[5] Un incident de sécurité de l'information se définit comme une atteinte à la disponibilité, à l'intégrité ou à la confidentialité des systèmes d'information ou aux informations qu'ils contiennent. Un incident de confidentialité constitue donc dans certaines situations un incident de sécurité de l'information.

Annexe 1 – Réflexions pour une utilisation de l'IA respectueuse de la PRP

Voici quelques questions à se poser afin d'utiliser l'IA de manière à respecter les exigences relatives à la PRP :

- Est-ce que l'outil d'IA dans lequel je m'apprête à intégrer des renseignements personnels est **sécuritaire et autorisé par mon établissement** ?
- Est-ce qu'il est nécessaire que j'intègre des **identifiants directs** dans l'outil d'IA ?
- Est-ce que des **renseignements dépersonnalisés ou anonymisés** pourraient plutôt être utilisés ?
- Est-ce que j'utilise l'outil d'IA sur un **appareil corporatif** du CHU Sainte-Justine ainsi que sur un **réseau sécurisé** ?
- Est-que ce que mon **mot de passe est robuste et sécuritaire** ?
- Est-ce que j'ai bien **détruit toute copie de renseignements personnels** qui ne m'est plus nécessaire ?
- Est-ce que j'ai réfléchi à la possibilité et à la pertinence d'**informer les personnes concernées** de l'intégration de leurs renseignements personnels dans un outil d'IA et de **recueillir leur consentement** dans ce contexte?
- Est-ce que je me suis informé(e) sur les **exigences de PRP particulières** à mon projet ou outil d'IA ?
- Est-ce que je connais bien les **limites et risques** de mon projet ou outil d'IA ?