

SENSIBILISATION A L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE (IA) DANS LES ACTIVITES DE RECHERCHE

2026-04-07

1. Principes de base et considérations

L'IA peut soutenir efficacement plusieurs étapes du travail scientifique : revue de littérature, idéation, écriture, analyses exploratoires, génération de code, etc.

L'usage décrit ici concerne uniquement **la recherche**. Les outils d'IA mentionnés ne doivent pas être utilisés pour soutenir la prise de décision en pratique de soins (ex. : **diagnostic, triage** ou **décision clinique**).

Vous pouvez vous référer à ce document illustrant les différentes considérations à prendre en compte lors de l'utilisation de l'IA, dont celles liées à l'éthique et à la propriété intellectuelle.

2. Outils autorisés selon les usages

Selon le type d'activité, plusieurs options existent :

- Pour du contenu **non sensible, confidentiel ou identifiant**, des outils généraux (ex. : chatbots grand public ou spécialisés) peuvent être utilisés avec précaution.
- Pour des données plus sensibles, identifiantes, ou pour des projets nécessitant des garanties renforcées (résidence, journalisation, contrôles d'accès), privilégier des environnements institutionnels ou des plateformes plus sécurisées.

Revue de littérature (sans données sensibles)

Les outils spécialisés comme SciSpace Advanced ou OpenEvidence peuvent être utiles pour explorer la littérature scientifique, tant qu'aucune donnée sensible, confidentielle ou identifiante n'y est déposée.

Outils d'IA grand public (comptes individuels Pro)

Les agents conversationnels comme ChatGPT Pro, Gemini Pro ou Claude Pro peuvent soutenir l'idéation ou des tâches générales, mais uniquement lorsqu'aucune information sensible, confidentielle ou identifiante n'est utilisée. Ils ne sont pas adaptés pour du contenu interne ou des données liées à la recherche impliquant des personnes.

Outils d'IA "Entreprise" gérés par le CRHSJ

Pour les travaux impliquant des données sensibles, confidentielles ou identifiantes, il peut être préférable d'utiliser des outils d'IA sous licence Entreprise gérés par le CRHSJ (ex. : Microsoft Copilot). Ces environnements offrent généralement des protections additionnelles.

À l'inverse, les licences Pro individuelles ne permettent pas d'assurer ces garanties, particulièrement pour la résidence des données ou l'inférence hors Canada.

Outils d'IA pour le développement de code

Les outils d'IA pour le développement de code (ex. : Claude Code) peuvent faciliter l'automatisation, la documentation et le débogage. Leur utilisation introduit toutefois un changement important en matière de sécurité : ces outils peuvent agir comme de véritables acteurs, capables de provoquer des modifications concrètes, et non plus seulement comme des conseillers formulant des suggestions. Leur usage doit donc se faire sans exposer de données sensibles, confidentielles, identifiantes ou propriétaires.

Une attention particulière doit être portée aux droits d'accès accordés à ces outils, tant en lecture qu'en écriture. Il convient d'évaluer précisément ce que l'agent peut lire (p. ex. : code source, documentation, secrets, variables d'environnement ou services connectés) ainsi que ce qu'il peut écrire ou exécuter (p. ex. : modifications de fichiers, commandes terminal, changements de dépendances ou mises à jour de la configuration CI). Les dépôts de code accessibles ne doivent contenir aucune clé SSH, jeton d'authentification, mot de passe ou autre secret d'accès, même à des fins de test.

Tout code généré doit être revu, testé et validé par le chercheur, notamment sur les plans de la sécurité, des licences logicielles et de la reproductibilité.

Accès aux modèles LLM via API

Lorsqu'un traitement nécessite un accès API à des modèles LLM, il est recommandé de passer par les environnements infonuagiques institutionnels (Azure ou AWS) mis à disposition par le Centre d'excellence infonuagique (CEI) de Santé Québec. Ces environnements offrent des contrôles adaptés au traitement de données de recherche plus sensibles.

Veillez contacter votre Directrice des données et des infrastructures informatiques du Centre de recherche pour toute question relative à ce sujet.

3. Risques et bonnes pratiques

Quelques éléments qui méritent une attention particulière :

- La possibilité de fuites involontaires lorsqu'on partage des documents internes dans un outil non prévu pour cet usage,
- Les variations importantes entre plateformes quant à la protection, la rétention ou l'emplacement du traitement,
- Les obligations prévues par les lois sur la protection des renseignements de santé,
- Le risque de créer un usage parallèle d'outils non validés (« shadow AI »), difficile à superviser,
- Le risque de collecte ou d'utilisation excessive de renseignements personnels et le non-respect du principe de nécessité.

Selon le contexte, il est requis de :

- Utiliser les environnements institutionnels mis à votre disposition,
- Suivre les recommandations de sécurité spécifiques aux outils utilisés,
- Éviter d'insérer des données sensibles dans des outils qui ne sont pas conçus ou autorisés pour ce type d'information,
- 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 nécessaires à l'objectif poursuivi, préalablement déterminé,
- Favoriser l'intégration, dans un outil d'IA autorisé, de renseignements anonymisés ou dépersonnalisés,
- Conserver une trace de l'utilisation de l'IA dans les protocoles et les publications (méthodologie, limitations, outils utilisés),
- Préciser, dans les livrables, que les résultats issus de l'IA ont été revus par des chercheurs qualifiés,

- Demander conseil aux équipes responsables de la gouvernance des données, de la recherche ou de la sécurité lorsqu'un projet soulève des questions particulières.

4. Références

- **Guide sur l'utilisation de l'IA au centre de recherche Azrieli du CHU Sainte-Justine :**
https://enseignement.chusj.org/getmedia/6988dedd-d8c5-4297-9492-599782758d89/GUI_GDR_IA_v01.pdf.aspx
- **Guides sur l'utilisation responsable de l'IA au CHU Sainte-Justine :** <https://www.chusj.org/fr/a-propos/La-transformation-numerique/Une-approche-centree-sur-l-humain>
- **Politiques et procédures sur le respect de la confidentialité au CHU Sainte-Justine :**
<https://intranet.chusj.org/fr/Nos-equipes/directions/Qualite-performance/Confidentialite>
- **Mesures de sécurité pour l'utilisation de l'IA agentique (ex : Claude code) :**
<https://code.claude.com/docs/en/security>
<https://code.claude.com/docs/en/devcontainer>
<https://codewithandrea.com/articles/run-ai-agents-inside-devcontainer/>