



GUIDE SUR L'UTILISATION RESPONSABLE DE L'INTELLIGENCE ARTIFICIELLE

PROTECTION DES RENSEIGNEMENTS PERSONNELS

Direction de l'accès à l'information et de la protection des renseignements personnels (Bureau de la PCD, Affaires juridiques et Gouvernance)

Date : 8 août 2026

Production

Santé Québec

Direction de l'accès à l'information et de la protection des renseignements personnels

prp@sante.quebec

Ce guide a été rédigé avec l'aide de l'intelligence artificielle (IA) et s'inspire fortement du [Guide sur l'utilisation responsable de l'IA : Protection des renseignements personnels](#) créé par Santé Québec Centre hospitalier universitaire Sainte-Justine.

*Le présent document appartient à **Santé Québec**. Toute personne ayant accès à celui-ci s'engage à protéger et à garder confidentielles les informations qui y sont contenues, incluant tout renseignement personnel le cas échéant. Ces informations ne pourront être utilisées qu'aux fins prévues, le présent document ne pouvant être divulgué à des personnes non autorisées qu'avec le consentement préalable de **Santé Québec**. Toutes les mesures raisonnables doivent être mises en place pour assurer la confidentialité du présent document, notamment en respect des lois applicables au Québec.*

Table des matières

1.	INTRODUCTION	1
1.1.	Objectifs du guide	1
1.2.	Public cible	1
1.3.	Utilisation du guide	2
1.4.	Quelques définitions de base concernant l'IA	2
1.5.	Qu'est-ce qu'un renseignement personnel?	3
1.6.	Assistance et ressources	4
2.	PRINCIPES GÉNÉRAUX DE PRP APPLICABLES AU SEIN DE SANTÉ QUÉBEC	5
2.1.	Confidentialité	5
2.2.	Nécessité	6
2.3.	Dépersonnalisation	6
2.4.	Sécurité	7
2.5.	Destruction	8
3.	PRINCIPAUX RISQUES EN MATIÈRE DE DE PRP LIÉS À L'UTILISATION DE L'IA	9
3.1.	Communication non autorisée de renseignements personnels au fournisseur d'un outil d'IA	10
3.2.	Fuite de renseignements personnels	11
3.3.	Utilisation non autorisée de renseignements personnels pour le développement d'un outil d'IA	11
3.4.	Collecte ou utilisation excessive de renseignements personnels	12
3.5.	Communication de renseignements personnels à l'extérieur du Québec	13
3.6.	Anonymisation non conforme de renseignements personnels	14
4.	UTILISATION DE L'IA : BONNES PRATIQUES DE PRP	14
5.	UTILISATION DE MICROSOFT COPILOT	17
	CAS PRATIQUE : Rédaction de courriels avec l'IA	20
6.	UTILISATION DES SCRIBES MÉDICAUX BASÉS SUR L'IA	21
	CAS PRATIQUE : Utilisation d'un outil IA pour la rédaction de notes cliniques	23
7.	DÉVELOPPEMENT ET ENTRAÎNEMENT D'OUTILS D'IA	24
	CAS PRATIQUE : Déploiement d'un outil d'IA prédictive en génétique	25
8.	DÉCISIONS FONDÉES EXCLUSIVEMENT SUR UN TRAITEMENT AUTOMATISÉ DE RENSEIGNEMENTS PERSONNELS	27
9.	QUE FAIRE EN CAS D'INCIDENT DE CONFIDENTIALITÉ ?	28
	ANNEXE 1 – RÉFLEXIONS POUR UNE UTILISATION DE L'IA RESPECTUEUSE DE LA PRP	30

1. Introduction

1.1. Objectifs du guide

L'IA offre de nouvelles possibilités pour soutenir l'innovation, optimiser les processus et améliorer les pratiques cliniques, administratives et de recherche. Puisque le développement et l'utilisation de l'IA exigent des volumes importants de données, l'intégration de l'IA en santé et services sociaux présente des risques en matière de protection des renseignements personnels (PRP). Ce guide constitue donc un outil d'accompagnement et de sensibilisation destiné à soutenir les personnes œuvrant à Santé Québec afin de favoriser une intégration de l'IA au sein de l'organisation qui soit responsable et respectueuse des règles de PRP.

De façon plus précise, ce guide poursuit notamment les objectifs suivants :

- Expliquer les principes de PRP applicables au sein de Santé Québec ;
- Décrire les principaux risques de PRP associés à l'utilisation de l'IA ;
- Présenter les bonnes pratiques de PRP à adopter pour une utilisation responsable et sécuritaire de l'IA.

Ce guide se fonde sur le cadre normatif applicable ainsi que sur les principes généraux de PRP.

1.2. Public cible

Ce guide s'adresse à toutes les personnes œuvrant au sein de Santé Québec qui utilisent ou souhaitent utiliser l'IA dans le cadre de leurs fonctions. Il vise plus particulièrement :

- Les membres du personnel ;
- Les professionnelles et professionnels de la santé et des services sociaux ;
- Les étudiantes, étudiants et stagiaires ;
- Les chercheuses et chercheurs ;
- Toute autre personne appelée à exercer des fonctions ou à collaborer aux activités de Santé Québec.

Ce guide s'applique à toute utilisation des outils d'IA effectuée dans le cadre d'activités professionnelles, académiques, cliniques, administratives ou de recherche.

1.3. Utilisation du guide

L'utilisation de l'IA doit en tout temps respecter :

- Les lois et règlements applicables ;
- Les politiques, procédures, normes et directives de Santé Québec ;
- Les cadres normatifs spécifiques à chaque établissement de Santé Québec, le cas échéant ;
- Tout autre document normatif applicable, le cas échéant.

Le présent guide ne remplace pas ces documents normatifs. Il doit être lu et appliqué en cohérence avec l'ensemble des règles en vigueur. L'application des bonnes pratiques énoncées au présent guide ne dispense pas l'équipe responsable d'un projet d'effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) ou toute autre analyse PRP requise selon les circonstances. De même, le respect des bonnes pratiques énoncées au présent guide n'a pas pour effet de rendre automatiquement acceptable l'intégration des renseignements personnels dans un outil d'IA.

1.4. Quelques définitions de base concernant l'IA

Afin de faciliter la compréhension du présent guide, vous trouverez ci-dessous quelques définitions de base concernant l'IA :

Terme	Définition
Intelligence artificielle (IA)	Ensemble de technologies permettant de réaliser certaines tâches habituellement associées à l'intelligence humaine, comme analyser de l'information, effectuer des prédictions ou aider à la prise de décision à partir de données.

Intelligente artificielle générative (IAG)	Type d'intelligence artificielle capable de créer du nouveau contenu à partir des informations fournies, par exemple du texte, des images et des sons, grâce à l'entraînement de l'outil à l'aide de données existantes.
Outils d'IA publics	Outils accessibles au grand public gratuitement ou par abonnement et qui sont hébergés et/ou gérés par des entreprises privées ou organisations externes à Santé Québec. Il s'agit d'outils qui ne sont pas sécurisés ni adaptés pour un usage professionnel ou organisationnel.
Outils d'IA autorisés	Outils autorisés par Santé Québec ou l'un de ses établissements avec un cadre d'utilisation clairement défini. Les outils d'IA autorisés le sont à la suite d'analyses visant à évaluer leur sécurité et leur conformité au cadre légal applicable.

1.5. Qu'est-ce qu'un renseignement personnel?

Afin de pouvoir bien protéger les renseignements personnels, il est important d'être d'abord en mesure de les reconnaître.

Un renseignement personnel est un renseignement qui concerne une personne physique ET qui permet de l'identifier directement¹ ou indirectement².

¹ Identification directe : Par le recours à un seul renseignement (ex.: nom, numéro de dossier, numéro de chambre exact lors de l'épisode de soins, etc).

² Identification indirecte : Par recoupement ou avec la combinaison de plusieurs renseignements (ex. : date de naissance, âge, sexe, taille, code postal, unité/étage, etc).

Le fait qu'une personne soit une usagère ou un usager d'un établissement de Santé Québec constitue un renseignement personnel. Voici d'autres exemples de renseignements personnels :

- Le nom d'une usagère ou d'un usager ;
- Les soins dispensés à une usagère ou un usager ;
- Les coordonnées personnelles d'une personne ;
- L'état de santé d'une personne (usagère ou usager, membre du personnel) ;
- Les mesures disciplinaires prises à l'égard d'une personne membre du personnel ;
- Les habitudes de vie d'une personne participant à un projet de recherche.

Pour en apprendre davantage sur **les renseignements personnels**, nous vous invitons à consulter la fiche informative dédiée à ce sujet sur la [Page PRP de Santé Québec](#).

À retenir

Une personne peut être identifiée à partir d'un identifiant direct, mais aussi grâce à la combinaison de plusieurs informations la concernant.

Ainsi, **malgré l'absence d'identifiants directs tels que le nom et le numéro de dossier**, un ensemble d'informations portant sur une ou plusieurs personnes peut constituer des renseignements personnels.

1.6. Assistance et ressources

La mise en œuvre des bonnes pratiques de PRP peut soulever des questions. N'hésitez pas à demander du soutien aux instances appropriées :

- Si vous œuvrez dans un établissement, communiquez avec la ou les personnes responsables de la PRP de votre établissement.
- Si vous œuvrez au siège social de Santé Québec, vous pouvez joindre la Direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP) à l'adresse suivante : prp@sante.quebec.

Pour approfondir vos connaissances ou consulter d'autres ressources liées à la PRP, nous vous invitons à consulter la [Page PRP de Santé Québec](#).

2. Principes généraux de PRP applicables au sein de Santé Québec

Les principes généraux de PRP énoncés à la présente section sont ceux prévus à la [Politique-cadre sur l'accès à l'information et la gouvernance des renseignements personnels](#).

2.1. Confidentialité

Tout renseignement personnel doit être traité de manière confidentielle, dans le respect des règles prévues aux lois applicables et, lorsque requis, du consentement de la personne concernée par ces renseignements. La confidentialité implique de s'assurer de communiquer et/ou de donner accès aux renseignements personnels uniquement aux personnes autorisées. Ainsi, de façon concrète, afin de protéger la confidentialité des renseignements personnels :

- Nous devons nous abstenir de communiquer, de diffuser ou de divulguer les renseignements personnels dont nous prenons connaissance dans le cadre de nos fonctions, à moins d'y être dûment autorisés.
- Nous devons nous assurer de donner accès aux renseignements personnels uniquement aux personnes pour lesquelles cet accès est nécessaire à l'exercice de leurs fonctions. Puisque les renseignements personnels sont confidentiels, l'accès à ceux-ci doit être limité au plus petit nombre de personnes possible.

Pour en apprendre davantage sur le **principe de la confidentialité**, nous vous invitons à consulter la fiche informative dédiée à ce sujet en cliquant [ici](#).

2.2. Nécessité

Seuls les renseignements personnels nécessaires à l'atteinte des objectifs visés par un projet, une tâche ou une activité doivent être collectés, utilisés, conservés et communiqués. Ainsi, lors de chaque action impliquant des renseignements personnels (collecte, utilisation, conservation ou communication), nous devons réduire le plus possible le nombre de renseignements personnels impliqués. Si des renseignements personnels ne sont pas nécessaires à une activité, une tâche ou un projet, ceux-ci ne doivent pas être collectés, utilisés, conservés ou communiqués.

Réduire le nombre de renseignements personnels impliqués dans un projet, une tâche ou une activité permet de limiter les atteintes au droit à la vie privée. Les risques de préjudice en cas d'incident de confidentialité sont également réduits.

Comment savoir si vous respectez le principe de nécessité ?

Pour déterminer si vous respectez le principe de nécessité, vous devez vous questionner si chacun des renseignements personnels impliqués est nécessaire pour accomplir vos fonctions ou atteindre les objectifs de votre projet. La notion de nécessité dépasse la simple utilité : un renseignement sera jugé nécessaire s'il répond directement à un besoin réel et légitime et que son utilisation dépasse le simple avantage pratique.

Attention! Vous devez vous assurer de limiter les renseignements personnels utilisés à ce qui est vraiment nécessaire. Par exemple, ce n'est pas parce que vous avez besoin du code postal d'une personne que vous avez besoin de l'ensemble de son adresse.

Pour en apprendre davantage sur le **principe de la nécessité**, nous vous invitons à consulter la fiche informative dédiée à ce sujet en cliquant [ici](#).

2.3. Dépersonnalisation

Lorsqu'il est possible d'utiliser ou de communiquer un renseignement personnel sous une forme ne permettant pas d'identifier directement une personne, l'utilisation ou la communication de ce renseignement doit se faire sous cette

forme. Ainsi, l'utilisation ou la communication de renseignements dépersonnalisés³ doit être privilégiée. Par conséquent, s'il n'est pas nécessaire d'utiliser les noms ou autres identifiants directs dans le cadre d'un projet, d'une tâche ou d'une activité, ceux-ci doivent être retirés.

La dépersonnalisation permet de protéger la vie privée de manière proactive. En cas d'erreur, de bris de sécurité ou d'accès non autorisé à des renseignements dépersonnalisés, la vie privée de la personne concernée par ces renseignements est davantage protégée puisque son identité n'est pas directement révélée.

Comment savoir si vous respectez le principe de dépersonnalisation ?

Avant d'utiliser ou de communiquer un renseignement personnel, prenez un moment pour vous demander s'il est vraiment nécessaire d'utiliser un renseignement qui identifie directement la personne.

Par exemple, est-ce que le nom, l'adresse ou le numéro d'assurance maladie doivent absolument être utilisés ou communiqués pour atteindre les objectifs visés ?

Pour en apprendre davantage sur le **principe de la dépersonnalisation**, nous vous invitons à consulter la fiche informative dédiée à ce sujet en cliquant [ici](#).

2.4. Sécurité

Tout renseignement personnel doit être collecté, utilisé, conservé, communiqué ou détruit de façon sécuritaire. Des mesures de sécurité rigoureuses selon les circonstances doivent être mises en place et respectées par tous et toutes afin de protéger la confidentialité des renseignements personnels et ce, tant au niveau physique qu'informatique. Des mesures de sécurité robustes permettent de protéger le droit à la vie privée des personnes en prévenant notamment l'accès non autorisé ainsi que la perte ou la fuite de renseignements personnels.

³ Un renseignement dépersonnalisé est un renseignement personnel permettant d'identifier une personne de façon indirecte, mais non de façon directe.

Comment savoir si vous respectez le principe de sécurité ?

Afin de respecter le principe de sécurité, vous devez déterminer si les mesures de sécurité nécessaires afin d'assurer la protection des renseignements personnels sont en place, notamment en fonction de la sensibilité de ces renseignements. L'implication des équipes spécialisées en sécurité de l'information peut s'avérer nécessaire.

Voici quelques questions pertinentes à se poser afin de respecter le principe de sécurité :

- Est-ce que les renseignements personnels sont conservés dans un endroit sécuritaire, dont l'accès physique ou technologique est restreint ?
- Est-ce que le document devrait être protégé par un mot de passe ?
- Est-ce que les renseignements personnels sont conservés ou déposés dans un logiciel ou un appareil autorisé ?
- Est-ce que vous travaillez sur un réseau Internet sécuritaire ?

Pour vous assurer de traiter les renseignements personnels de façon sécuritaire, veuillez consulter l'équipe de sécurité de l'information de votre établissement ou du siège social de Santé Québec (securite@sante.quebec), selon le cas.

Pour en apprendre davantage sur le **principe de la sécurité**, nous vous invitons à consulter la fiche informative dédiée à ce sujet en cliquant [ici](#).

2.5. Destruction

Dès que les fins pour lesquelles un renseignement personnel a été collecté ou est conservé sont accomplies, le renseignement personnel doit être détruit, sous réserve des délais prévus au [Calendrier de conservation de Santé Québec](#). Ce principe est applicable également aux copies de renseignements personnels.

La méthode de destruction choisie doit être adaptée au support (papier, électronique, disque dur, serveur infonuagique, etc.) et au niveau de sensibilité des renseignements personnels. Elle doit permettre une destruction définitive et

irréversible des renseignements personnels ainsi qu'une destruction de toutes les copies de ces renseignements, le cas échéant.

La destruction des renseignements personnels est importante puisque la conservation de ceux-ci au-delà de la durée nécessaire accroît inutilement les risques d'incident de confidentialité.

Comment savoir si vous respectez le principe de destruction ?

Voici quelques questions pertinentes à se poser afin de respecter le principe de destruction :

- Quel est le délai de conservation prévu au Calendrier de conservation de Santé Québec pour ces renseignements ? Est-ce que ce délai est échu ?
- Est-ce qu'il est encore nécessaire que je conserve ces renseignements personnels ?
- Est-ce qu'il s'agit d'une copie de renseignements personnels ? Est-ce que celle-ci doit encore être conservée ? Est-ce qu'il existe d'autres copies de ces renseignements ?
- Est-ce que la méthode de destruction est sécuritaire et appropriée ? Est-ce qu'elle permet une destruction définitive ?

Pour en apprendre davantage sur le **principe de la destruction**, nous vous invitons à consulter la fiche informative dédiée à ce sujet en cliquant [ici](#).

3. Principaux risques en matière de de PRP liés à l'utilisation de l'IA

L'utilisation de l'IA peut contribuer à améliorer les façons de travailler et à soutenir la productivité. Toutefois, ces outils ne sont pas sans risque. L'IA doit être utilisée avec prudence, notamment en raison des enjeux liés à la PRP. Il est essentiel de bien comprendre les principaux risques associés à l'utilisation de l'IA afin de pouvoir les anticiper, les atténuer et les gérer adéquatement.

N'oubliez pas! Le fait qu'un outil d'IA soit accessible publiquement et gratuitement, utilisé ailleurs, facilement disponible ou populaire ne signifie pas qu'il est conforme et autorisé.

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

Afin de produire des réponses utiles, l'IA doit analyser les informations qui lui sont fournies. Autrement dit, ces outils utilisent les données saisies par l'utilisateur pour générer du contenu. Si un utilisateur saisit des renseignements personnels dans un outil public (par exemple, un outil accessible en ligne), les renseignements peuvent être rendus disponibles au fournisseur de l'outil, ce qui constitue une communication non autorisée.

Ainsi, saisir des renseignements personnels dans un outil qui n'est pas autorisé compromet la vie privée des personnes concernées et enfreint les règles en vigueur. C'est la raison pour laquelle il est essentiel de faire preuve de prudence et de ne jamais transmettre des renseignements personnels à un outil d'IA qui n'est pas autorisé.

À retenir

La saisie de renseignements personnels dans un outil d'IA public est strictement **interdite**. L'interdiction vise notamment les outils suivants :

- ChatGPT ;
- Claude ;
- Gemini ;
- DeepL ;
- DeepSeek.

Qu'en est-il de Microsoft Copilot?

Microsoft Copilot est un outil d'IA intégré à la suite Microsoft Office 365 (M365). Son utilisation est **permise**, strictement à partir d'un compte professionnel MO365 de Santé Québec, et à condition qu'elle soit effectuée de manière

responsable, sécuritaire et conforme aux règles en vigueur. Pour plus d'information, consultez la section 5 du présent guide.

3.2. Fuite de renseignements personnels

L'utilisation d'un outil d'IA peut comporter un risque de fuite de renseignements personnels si les renseignements sont saisis dans un outil d'IA public (communication non autorisée de renseignements personnels au fournisseur d'un outil d'IA). Ces renseignements peuvent être conservés, réutilisés ou exposés par l'outil d'IA, généralement à l'insu de l'utilisateur, ce qui peut compromettre la confidentialité et la vie privée des personnes concernées par ces renseignements.

Ces fuites peuvent survenir de différentes façons, par exemple :

- Par l'enregistrement des informations dans des journaux techniques (logs) de l'outil d'IA ;
- À la suite de failles de sécurité de l'outil d'IA ou de son infrastructure ;
- Lors de l'entraînement ou de l'amélioration de l'outil d'IA, si les données saisies sont réutilisées.

Le risque est encore plus élevé lorsque l'outil d'IA n'indique pas clairement de quelles façons les données sont protégées dans sa politique de confidentialité. L'absence de mesures comme le chiffrement des données ou l'engagement de ne pas réutiliser les données fournies augmente le risque de fuite.

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

L'utilisation de renseignements personnels est encadrée par la loi. Cela signifie que ces renseignements ne peuvent pas être utilisés librement, notamment pour développer, entraîner ou améliorer un outil d'IA. Dans certains cas précis, la loi permet l'utilisation de renseignements personnels à des fins de développement d'un outil d'IA. Toutefois, ces situations sont limitées, encadrées et doivent respecter des conditions strictes.

Ainsi, l'utilisation de renseignements personnels afin d'entraîner un outil d'IA nécessite une analyse juridique et une analyse de PRP au préalable. Par ailleurs, l'utilisation de renseignements personnels pour développer ou entraîner un outil d'IA doit être autorisée et, le cas échéant, encadrée contractuellement par l'établissement qui détient ces renseignements. D'autres mécanismes d'autorisation ou analyses peuvent également être requis selon le contexte.

De plus, il est à noter que plusieurs outils d'IA publics (ex. : ChatGPT, Gemini, etc.) utilisent les données saisies par leurs utilisateurs afin d'entraîner leurs modèles d'IA, d'où l'importance de ne jamais intégrer de renseignements personnels dans les outils d'IA publics.

3.4. Collecte ou utilisation excessive de renseignements personnels

En PRP, le principe de nécessité signifie qu'on ne doit collecter ou utiliser que les renseignements personnels réellement nécessaires pour atteindre un objectif précis. Ce principe vise à limiter les atteintes à la vie privée des personnes concernées par les renseignements.

Dans le contexte de l'IA, ce principe peut poser un défi : le développement et l'entraînement des outils d'IA nécessitent souvent de grandes quantités de données, ce qui peut entraîner une collecte ou une utilisation excessive de renseignements personnels si aucune limite claire n'est fixée.

C'est la raison pour laquelle chaque projet impliquant l'IA doit faire l'objet d'une analyse rigoureuse. Il est essentiel (1) de vérifier quels renseignements personnels sont réellement nécessaires, (2) d'éviter toute collecte superflue et (3) de s'assurer que tous les principes de PRP applicables sont respectés avant d'aller de l'avant. L'anonymisation⁴ peut être une alternative intéressante dans certaines circonstances.

⁴ L'anonymisation est le processus qui consiste à modifier ou supprimer, de façon irréversible, des variables dans un ensemble de données afin qu'il ne soit plus possible d'identifier, de façon directe ou indirecte, les personnes concernées par cet ensemble de données.

3.5. Communication de renseignements personnels à l'extérieur du Québec

Plusieurs outils d'IA communiquent et/ou conservent les renseignements personnels qui y sont saisis à l'extérieur du Québec. Dans ces cas, les renseignements personnels sont généralement assujettis au cadre juridique applicable dans la juridiction où ils se trouvent. Cette protection peut s'avérer équivalente à celle offerte par la législation québécoise ou, dans certains cas, être plus limitée.

Une telle situation peut comporter des risques importants comme la perte de contrôle sur les renseignements personnels, l'accès non autorisé par des tiers, l'utilisation secondaire des renseignements sans autorisation ou encore des atteintes à la confidentialité des renseignements.

Afin d'atténuer ces risques, il est recommandé de privilégier le maintien des renseignements personnels au Québec ou au Canada afin qu'ils bénéficient d'une protection juridique adéquate. Lorsque cela n'est pas possible, il est nécessaire de réaliser, avant toute communication de renseignements personnels à l'extérieur du Québec, une EFVP dont le résultat démontre que les renseignements bénéficieraient d'une protection adéquate.

À retenir

Avant d'utiliser un outil d'IA qui pourrait communiquer un renseignement personnel à l'extérieur du Québec, il faut :

- Réaliser une EFVP ;
- Limiter au strict nécessaire l'intégration des renseignements personnels ;
- Anonymiser ou dépersonnaliser les renseignements avant leur utilisation dans l'outil, lorsque possible ;
- Vérifier que les mesures de sécurité offertes par le fournisseur sont suffisantes.

3.6. Anonymisation non conforme de renseignements personnels

Certains fournisseurs d'outils d'IA affirment assurer la protection des renseignements personnels en anonymisant ces renseignements avant leur utilisation pour l'entraînement de leur outil. Au Québec, un renseignement est considéré comme anonymisé lorsqu'il ne permet plus, et de façon permanente, d'identifier directement ou indirectement la personne qu'il concerne. L'anonymisation doit s'effectuer en conformité avec le [Règlement sur l'anonymisation des renseignements personnels](#), lequel exige notamment l'application de techniques d'anonymisation conformes aux meilleures pratiques généralement reconnues ainsi la réalisation d'une analyse des risques de réidentification. L'anonymisation d'un renseignement est un seuil difficilement atteignable.

Il peut s'avérer difficile de vérifier si le fournisseur respecte réellement les exigences strictes prévues au *Règlement sur l'anonymisation des renseignements personnels*. **Le fait qu'un fournisseur affirme anonymiser les renseignements personnels avant de les réutiliser ne signifie pas que l'intégration de renseignements personnels dans l'outil d'IA de ce fournisseur est autorisée.**

4. Utilisation de l'IA : bonnes pratiques de PRP

Avant d'utiliser un outil d'IA, il est important de bien cerner le besoin et l'objectif recherché. Les utilisateurs d'un outil d'IA doivent (1) s'assurer que l'outil est approprié au contexte, (2) veiller à comprendre les limites et les risques de cet outil et (3) exercer, en tout temps et de façon indépendante à l'outil d'IA, leur jugement professionnel.

Toute personne qui utilise l'IA doit le faire avec prudence et vigilance. Les bonnes pratiques présentées ci-dessous visent à favoriser une utilisation responsable de

l'IA afin de réduire les risques, notamment en matière de PRP, et d'assurer un usage conforme et sécuritaire.

Pratiques à adopter 	Pratiques à éviter 
Utiliser uniquement les outils d'IA autorisés par Santé Québec ou un de ses établissements lorsque vous souhaitez y intégrer des renseignements personnels. Ex. : Microsoft Copilot connecté à votre compte Microsoft Office M365.	Intégrer des renseignements personnels dans un outil d'IA non autorisé . Ex. : ChatGPT, DeepL, DeepSeek, Microsoft Copilot en étant non connecté à votre compte Office M365, etc.
Intégrer, dans un outil d'IA, uniquement les renseignements personnels strictement nécessaires à l'objectif précis et préalablement déterminé. Privilégier les renseignements anonymisés ou dépersonnalisés lorsque cela est possible.	Intégrer des renseignements personnels non nécessaires dans un outil d'IA, ce qui augmente inutilement le risque d'incident de confidentialité. Inclure des identifiants directs (nom, prénom, numéro, etc.) dans un outil d'IA autorisé lorsque cela n'est pas essentiel à l'objectif visé.
Travailler sur un appareil corporatif lors de l'utilisation d'un outil d'IA dans le cadre de votre travail.	Utiliser un outil d'IA sur un appareil personnel , à moins d'y être expressément autorisé par son établissement.
Utiliser un réseau Internet sécurisé , comme celui d'un établissement de Santé Québec.	Utiliser un outil d'IA sur un réseau non sécurisé, comme un réseau Wi-Fi public .
Protéger vos accès en utilisant des mots de passe robustes et sécuritaires lorsqu'un outil d'IA l'exige.	Utiliser un mot de passe faible , simple ou déjà utilisé ailleurs.

(Ex. : Utiliser au minimum 12 caractères incluant des majuscules et caractères spéciaux).	
Détruire dès que possible toute copie de renseignements personnels que vous créez ou obtenez (détruire cette copie dès qu'elle n'est plus nécessaire).	Conserver des copies de renseignements personnels lorsqu'ils ne sont plus nécessaires au projet ou à la tâche.
Supprimer l'historique de conversation d'un outil d'IA autorisé lorsque celui-ci contient des renseignements personnels et qu'il n'est plus nécessaire de le conserver.	Conserver inutilement un historique de conversation dans un outil d'IA autorisé lorsque celui-ci contient des renseignements personnels.
Maintenir vos connaissances à jour concernant les exigences en matière de PRP, notamment celles de votre ordre professionnel.	Utiliser l'IA sans connaître les exigences en matière de PRP.
S'informer sur les limites et les risques des outils d'IA, particulièrement en ce qui concerne la PRP.	Utiliser un outil d'IA sans en comprendre les limites et les risques , notamment en matière de PRP.
En cas de doute ou de question , consulter votre gestionnaire ou les ressources appropriées.	Hésiter à poser des questions ou à demander de l'aide par crainte de la critique ou du jugement.

Déclarer immédiatement tout incident de confidentialité ou toute intégration de renseignements personnels dans un outil d'IA non autorisé, afin de permettre une intervention rapide.

En cas d'incident de confidentialité, **collaborer et prendre les mesures requises** pour éviter ou diminuer le risque de préjudice.

Ignorer un incident de confidentialité ou l'utilisation d'un outil d'IA non autorisé par crainte de blâme ou parce que vous hésitez à savoir si l'événement se qualifie d'incident de confidentialité.

Ne pas prendre de mesures à la suite d'un incident de confidentialité.

Veuillez consulter l'Annexe 1 pour une liste des questions qu'il est utile de se poser afin d'utiliser l'IA de manière respectueuse des exigences relatives à la PRP.

5. Utilisation de Microsoft Copilot

Microsoft Copilot est un outil d'IA visant à offrir un environnement sécuritaire afin de soutenir et d'améliorer la productivité des personnes œuvrant à Santé Québec. Microsoft Copilot offre de nombreuses fonctionnalités pour accomplir des tâches plus efficacement, par exemple :

- Rédiger des textes et des courriels ;
- Résumer des rencontres ou des documents ;
- Analyser des données dans Excel ;
- Créer des ébauches de présentations PowerPoint ;
- Rechercher des informations.

Comme tout outil technologique, l'utilisation de Microsoft Copilot exige de la vigilance et le respect de bonnes pratiques afin de protéger adéquatement les renseignements personnels.

L'intégration de renseignements personnels dans Microsoft Copilot est **autorisée** par Santé Québec **lorsque les quatre règles ci-dessous sont respectées**. Veuillez noter que l'intégration de renseignements personnels est possible uniquement avec l'agent conversationnel Copilot. L'intégration de renseignements personnels

dans la plateforme de conception et de gestion Microsoft Copilot Studio nécessite des analyses contextuelles supplémentaires au préalable.

Utiliser en tout temps son compte Microsoft O365 professionnel de Santé Québec

L'utilisation de Microsoft Copilot doit, en tout temps, se faire à partir d'un compte Microsoft Office 365 (MO365) professionnel de Santé Québec, pour les raisons suivantes :

- En utilisant un compte MO365 professionnel, les données bénéficient d'une politique de protection des données. Les renseignements personnels intégrés dans Microsoft Copilot sont donc protégés de la même manière que ceux transmis dans Teams ou Outlook.
- Les données demeurent hébergées à l'intérieur du tenant organisationnel (espace dédié à notre organisation) sécurisé de Microsoft, situé au Canada.
- Les données ne sont pas réutilisées pour entraîner ou améliorer l'outil, contrairement aux outils d'IA accessibles gratuitement en ligne.

Il est important de **toujours vérifier que vous êtes bien connecté(e) à votre compte MO365 professionnel avant d'intégrer des renseignements personnels dans Microsoft Copilot**. En cas de doute sur la connexion, veuillez vous abstenir d'intégrer une information sensible ou un renseignement personnel.

Comment vérifier que vous êtes bien connecté(e) à votre compte MO365 professionnel?

Avant d'utiliser Microsoft Copilot, assurez-vous de voir dans **le coin droit supérieur de la fenêtre**, l'un des éléments suivants :

- Vos initiales ou votre photo de profil ;
- Un bouclier avec un crochet vert.

Ne pas intégrer de renseignements personnels hautement sensibles

Bien que Microsoft Copilot soit un outil d'IA sécuritaire, des risques résiduels demeurent malgré la mise en place de mesures de sécurité. Ainsi, **il est fortement déconseillé de fournir à Microsoft Copilot des renseignements personnels hautement sensibles**⁵. À titre d'exemple, les renseignements ci-après, lorsqu'ils permettent d'identifier directement une personne, sont jugés comme hautement sensibles :

- renseignements concernant les dossiers en protection de la jeunesse ;
- renseignements relatifs à des actes de maltraitance, d'abus ou de violence ;
- données génétiques sensibles ;
- renseignements concernant des diagnostics hautement stigmatisants.

Respecter les principes de PRP

Même si l'intégration de renseignements personnels dans Microsoft Copilot est permise, **les principes de PRP demeurent pleinement applicables**, notamment :

- Le principe de nécessité : n'intégrer que les renseignements personnels réellement requis pour atteindre l'objectif poursuivi ;
- Le principe de dépersonnalisation : éviter les identifiants directs (ex. : nom, numéro de dossier, etc.) lorsque ceux-ci ne sont pas essentiels.

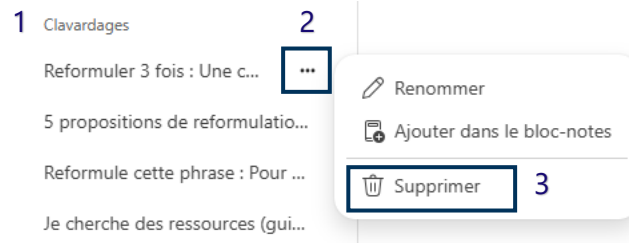
Ainsi, lorsque c'est possible, privilégiez l'utilisation de renseignements dépersonnalisés ou n'intégrez pas de renseignements personnels.

Supprimer régulièrement l'historique des clavardages

À titre de mesure de précaution supplémentaire, il est recommandé de supprimer manuellement, de façon régulière, l'historique des clavardages dans Microsoft Copilot lorsque celui-ci contient des renseignements personnels. Pour ce faire, vous devez :

⁵ Il s'agit des données « Protégé C » en application du *Modèle de classification de sécurité des données numériques gouvernementales* du ministère de la Cybersécurité et du Numérique (MCN).

1. Identifier le clavardage devant être supprimé dans le menu à gauche de l'écran ;
2. Cliquer sur « ... », à droite du clavardage à supprimer ;
3. Cliquer sur « Supprimer », dans le menu qui s'ouvre.



Cette suppression devrait être effectuée à la fin de chaque session lorsque la conservation de l'historique n'est pas nécessaire. Cette pratique contribue à réduire les risques d'incident de confidentialité.

CAS PRATIQUE : Rédaction de courriels avec l'IA

Un membre du personnel administratif reçoit un grand nombre de courriels et souhaite répondre plus rapidement à ceux-ci. Comme cette tâche lui semble répétitive et peu stimulante, il décide d'utiliser un outil d'IA pour l'aider à rédiger ses réponses.

Il choisit ChatGPT, un outil gratuit accessible en ligne, et y copie l'intégralité des courriels reçus, qui contiennent souvent des renseignements personnels ou des informations confidentielles. Il demande ensuite à l'outil de rédiger une réponse à partir de ces informations.

⊗ **Ce comportement n'est pas conforme**

Toute personne qui œuvre au sein de Santé Québec ne doit utiliser que les outils technologiques autorisés par l'organisation. ChatGPT n'est pas un outil d'IA autorisé pour y intégrer des renseignements personnels ou des informations confidentielles.

✓ **La bonne pratique**

Pour obtenir de l'aide dans la rédaction de courriels, l'outil approprié est Microsoft Copilot, à condition d'y accéder en étant connecté(e) à son

compte Microsoft Office 365 professionnel et de respecter les autres règles applicables mentionnées précédemment.

Dans ce contexte, l'intégration de renseignements personnels dans Copilot est **permise**, lorsqu'ils sont **nécessaires à l'objectif poursuivi**, soit la rédaction d'une réponse adéquate.

6. Utilisation des Scribes médicaux basés sur l'IA

Les Scribes médicaux basés sur l'IA, aussi nommés « outils de reconnaissance vocale et de transcription basés sur l'IA », permettent de soutenir les personnes œuvrant au sein de Santé Québec dans la rédaction des notes cliniques. De façon générale, ces outils enregistrent la consultation entre un usager et un professionnel, puis génèrent un résumé sous forme de note clinique.

La note générée par un Scribe médical basé sur l'IA ne constitue pas un document final. Elle doit obligatoirement être révisée, corrigée et validée par le professionnel avant d'être intégrée au dossier clinique.

En raison de la nature sensible des renseignements traités, l'utilisation des Scribes médicaux basés sur l'IA exige une **vigilance accrue** et le respect des exigences ci-dessous.

Exigences	Description
Outils autorisés	Seuls les Scribes IA approuvés par Santé Québec et/ou autorisés par l'établissement peuvent être utilisés. L'utilisation de tout autre outil est interdite, y compris par les médecins.
Consentement des personnes concernées	Le consentement explicite de l'usagère ou de l'utilisateur est obligatoire avant toute utilisation d'un Scribe IA qui effectue l'enregistrement de la

	consultation (donc un Scribe IA qui ne fait pas seulement une transcription en temps réel)⁶. Le consentement doit également être obtenu auprès de toute autre personne présente lors de la consultation. Afin que le consentement soit éclairé, l'usagère ou l'utilisateur doit recevoir une information claire et compréhensible concernant le fonctionnement de l'outil, notamment à l'égard de : • l'enregistrement de la voix; • la façon dont les données sont traitées; • les risques possibles liés à la sécurité et à la confidentialité. La preuve du consentement doit être documentée et conservée, qu'il soit obtenu verbalement ou par écrit. Cette documentation doit être conforme aux pratiques et exigences de l'établissement.
Utilisation sur des appareils autorisés	Les Scribes IA doivent être utilisés sur des appareils corporatifs. À défaut, l'utilisation sur un appareil personnel sécurisé est permise uniquement avec l'autorisation de l'établissement.
Destruction des renseignements collectés	Les renseignements collectés par les Scribes IA doivent être détruits dès qu'ils ne sont plus nécessaires. Dans tous les cas, la destruction doit avoir lieu au plus tard dans un délai maximal de 48 heures suivant l'enregistrement de la consultation.

⁶ Si le Scribe IA n'enregistre pas la consultation (et fait plutôt une transcription en temps réel) et que l'outil est acquis par l'établissement (et non directement par un professionnel), le consentement n'est pas requis.

CAS PRATIQUE : Utilisation d'un outil IA pour la rédaction de notes cliniques

Un médecin souhaite utiliser un outil d'IA pour l'aider à rédiger ses notes cliniques. L'outil qu'il identifie permet d'enregistrer les consultations médicales avec les usagères et usagers puis de générer automatiquement un résumé sous forme de note clinique destinée à être déposée au dossier.

Souhaitant respecter la confidentialité des renseignements, ce médecin a interrogé le fournisseur sur ses pratiques de PRP, et celui-ci confirme que l'outil respecte les exigences en matière de PRP et celles de la Loi 25. Il décide alors d'acheter une licence de l'outil de sa propre initiative, sans effectuer d'autres démarches auprès de son établissement.

⊗ **Ce comportement n'est pas conforme**

Toute personne œuvrant au sein de Santé Québec doit uniquement utiliser les outils autorisés par Santé Québec.

Le simple fait que le fournisseur atteste respecter les exigences en PRP ne suffit pas. La conformité de l'outil doit être analysée par un expert de Santé Québec considérant que (1) le cadre juridique applicable aux renseignements de santé et de services sociaux est distinct du cadre général de la Loi 25 et (2) Santé Québec possède ses propres exigences organisationnelles visant à protéger les renseignements qu'elle détient.

✓ **La bonne pratique**

L'intégration de renseignements personnels dans un outil d'IA pour la rédaction de notes cliniques est possible, lorsque :

- Lorsque l'outil a été préalablement autorisé par Santé Québec et/ou l'établissement ;
- Ces renseignements sont nécessaires à l'objectif poursuivi ;
- L'utilisation de l'outil respecte les exigences en matière de consentement, de sécurité et de conservation des renseignements personnels ;
- L'utilisation de l'outil s'inscrit dans les pratiques cliniques et organisationnelles en vigueur.

Le processus d'autorisation d'un outil d'IA permet de vérifier les éléments suivants :

- La conformité de l'outil aux lois applicables en matière de PRP ;
- Les mesures de sécurité de l'information ;

- Les conditions d'hébergement, de conservation et de destruction des données ;
- Les risques liés à l'utilisation clinique de l'outil.

7. Développement et entraînement d'outils d'IA

Le développement et l'entraînement d'outils d'IA impliquent des **enjeux en matière de PRP**. À ce titre, des **mesures supplémentaires** doivent obligatoirement être mises en place afin de limiter les risques et d'assurer la conformité aux exigences légales et organisationnelles. Les bonnes pratiques ci-dessous doivent être respectées.

Privilégier l'utilisation de renseignements anonymisés ou dépersonnalisés

- Utiliser des renseignements anonymisés lors des tests ou d'entraînement des outils d'IA⁷.
- Lorsque l'anonymisation n'est pas possible, des renseignements dépersonnalisés peuvent être utilisés.
- Aucun identifiant direct ne doit être utilisé (ex.: nom, numéro d'assurance maladie, etc.).

Obtenir l'autorisation de l'établissement

- Obtenir l'autorisation de l'établissement préalablement à la collecte ou l'utilisation de renseignements personnels à des fins de développement ou d'entraînement d'un outil d'IA, notamment en effectuant une EFVP.
- Selon les circonstances, le consentement des personnes concernées par les renseignements peut également être requis.

⁷ L'anonymisation doit être effectuée conformément au *Règlement sur l'anonymisation des renseignements personnels*.

Veiller à la sécurité et à la protection des renseignements personnels

- Assurer la conservation sécuritaire et confidentielle des renseignements personnels, notamment par :
 - Une gestion rigoureuse des droits d'accès à ces renseignements;
 - L'utilisation de serveurs et d'infrastructures sécurisés.
- Utiliser exclusivement des environnements sécurisés lors de l'entraînement et des tests des outils d'IA.
- Détruire de façon sécuritaire et définitive les renseignements personnels dès qu'ils ne sont plus nécessaires au développement ou à l'entraînement de l'outil.
- S'assurer que tout contrat conclu avec un fournisseur comporte les clauses contractuelles adéquates en matière de PRP, de sécurité de l'information et de gestion des incidents, notamment en sollicitant le service des affaires juridiques.
- Mettre en place un plan clair pour détecter, gérer et signaler les incidents de confidentialité liés à l'utilisation de l'outil d'IA.

Autorisation obligatoire des outils d'IA

- Tout outil d'IA développé à l'interne par Santé Québec doit faire l'objet d'une **autorisation institutionnelle avant son utilisation ou son déploiement**.
- Cette autorisation passe notamment par la réalisation d'une **EFVP**, lorsque requise, afin d'identifier les risques de PRP et de mettre en place les mesures d'atténuation appropriées.

CAS PRATIQUE : Déploiement d'un outil d'IA prédictive en génétique

Une équipe multidisciplinaire en génétique, composée de chercheurs et de personnel clinique, travaille depuis un certain temps à la création d'un outil d'IA prédictive. Pour développer et entraîner cet outil, l'équipe a obtenu toutes les autorisations nécessaires, ainsi que les consentements requis, et utilise uniquement des renseignements anonymisés et dépersonnalisés.

Souhaitant que cette innovation profite au plus grand nombre de professionnels, l'équipe envisage de rendre l'outil accessible à l'ensemble des professionnels du département. Comme les autorisations et consentements liés à l'utilisation des renseignements pour la création de l'outil ont déjà été obtenus, l'équipe estime qu'aucune autorisation supplémentaire n'est requise pour son déploiement. L'utilisation de cet outil dans le cadre de la prestation de soins nécessite l'intégration de renseignements personnels afin d'obtenir des résultats personnalisés pour chaque usagère et usager.

Par ailleurs, l'équipe souhaite collaborer avec des expertes et experts en éthique afin de sensibiliser et former les collègues aux risques de biais et de résultats discriminatoires liés à l'utilisation de l'outil d'IA prédictive.

⊗ **Ce comportement n'est pas conforme**

Toute personne œuvrant au sein de Santé Québec doit utiliser uniquement des produits et services technologiques autorisés par son établissement et/ou par Santé Québec.

Même si l'utilisation de renseignements personnels pour créer l'outil a été autorisée, le déploiement de l'outil en contexte clinique constitue une nouvelle étape qui nécessite une autorisation institutionnelle distincte.

Ce processus d'autorisation permet notamment de s'assurer que :

- Les exigences en matière de PRP sont respectées ;
- Les mesures de sécurité de l'information sont adéquates ;
- Les conditions d'utilisation en contexte de soins sont clairement définies.

✓ **La bonne pratique**

L'intégration de renseignements personnels dans un outil d'IA autorisé pour soutenir les cliniciennes et les cliniciens dans l'évaluation d'un diagnostic ou d'un pronostic est possible lorsque ces renseignements sont nécessaires à l'objectif poursuivi. Cette utilisation doit toutefois être formellement autorisée par l'établissement et/ou par Santé Québec.

Bon coup à souligner!

La volonté de sensibiliser les équipes aux risques de biais et de résultats discriminatoires est une bonne pratique. Comprendre ces risques et en discuter ouvertement permet de mieux les repérer, de les limiter et d'assurer une utilisation plus équitable et responsable de l'IA.

8. Décisions fondées exclusivement sur un traitement automatisé de renseignements personnels

Dans certains cas, des renseignements personnels peuvent être utilisés pour prendre une décision de façon entièrement automatisée, c'est-à-dire **sans aucune intervention humaine**. Lorsqu'une telle décision est prise, l'usagère ou l'utilisateur doit en être informé au plus tard au moment où la décision lui est communiquée.

Lorsqu'une décision est prise uniquement par un système automatisé, la personne concernée a le droit d'être informée :

- des renseignements personnels utilisés pour prendre la décision ;
- des principales raisons qui ont mené à cette décision, incluant les facteurs importants pris en compte et les paramètres du système ;
- de son droit de faire corriger les renseignements personnels utilisés pour rendre la décision.

La personne doit également avoir la possibilité de présenter ses observations à une personne œuvrant au sein de Santé Québec en mesure de réviser la décision.

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

Il s'agit d'une décision prise entièrement par un système informatique, sans validation, vérification ou jugement humain. Ces décisions reposent généralement sur des algorithmes qui analysent des données et appliquent des règles prédéfinies afin d'arriver à un résultat.

Exemples concrets :

- L'attribution automatique d'un rendez-vous en consultation externe par un algorithme, basée uniquement sur des renseignements de santé déjà saisis.

- Lors du processus d'embauche, la sélection des personnes à convoquer en entrevue à la suite d'une analyse des CV par un outil d'IA.

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

Un incident de confidentialité survient lorsqu'un renseignement personnel est consulté, utilisé, communiqué, perdu ou lors de toute autre atteinte à sa protection. Le non-respect des bonnes pratiques présentées dans ce guide peut, dans plusieurs cas, constituer un incident de confidentialité.

Agir rapidement est essentiel! Plus un incident est pris en charge tôt, plus il est possible d'en limiter les conséquences pour les personnes concernées et pour l'organisation.

Les étapes ci-dessous indiquent clairement quoi faire, dans quel ordre, lorsqu'un incident se produit ou est soupçonné.

1 Mettre fin à l'incident et empêcher que les renseignements personnels soient davantage consultés, partagés ou exposés.

Par exemple :

- Arrêter immédiatement d'utiliser l'outil d'IA concerné;
- Fermer la session de l'outil d'IA;
- Cesser toute utilisation d'un outil d'IA non autorisé;
- Arrêter d'utiliser l'outil d'IA sur un appareil personnel non autorisé ou sur un réseau non sécurisé (ex. Wi-Fi public);
- Éviter toute action qui pourrait aggraver la situation.

2 Informer sa ou son gestionnaire ou la personne responsable du projet, selon le cas.

Aviser sans délai son gestionnaire ou, selon le contexte, la personne responsable du projet. Cette étape permet une prise en charge rapide et coordonnée de la situation.

3 Déclarer l'incident selon les modalités applicables au sein de l'établissement ou du siège social de Santé Québec, selon le cas

Tout incident de confidentialité doit être **déclaré officiellement**, conformément aux procédures en vigueur dans l'établissement ou au siège social de Santé Québec. Cette déclaration est essentielle pour :

- Évaluer les risques ;
- Déterminer les mesures à prendre ;
- Respecter les obligations légales.

4 Prendre les mesures nécessaires afin de prévenir la récurrence d'un incident

Une fois l'incident pris en charge, il est important de revoir les pratiques afin de prévenir des situations similaires. Cela peut inclure :

- D'ajuster les pratiques d'utilisation liées à l'IA ;
- De revoir les processus ou les protocoles applicables ;
- Une formation sur les exigences en matière de PRP et d'IA.

Un incident peut arriver, mais ne doit jamais être ignoré. Agir rapidement, signaler la situation et corriger les pratiques sont des gestes essentiels pour protéger les personnes concernées et maintenir la confiance envers Santé Québec.

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

Voici quelques questions qu'il est utile de se poser afin d'utiliser l'IA de manière respectueuse des 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 Santé Québec ?
- Est-ce qu'il est nécessaire que j'intègre des identifiants directs dans l'outil d'IA autorisé ? 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 ainsi que sur un réseau sécurisé ?
- Est-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 ?
- 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 les risques de mon projet ou outil d'IA ?
- Est-ce que mon gestionnaire autorise l'utilisation de cet outil d'IA ?
- Est-ce que je sais quoi faire en cas d'incident de confidentialité ?

