Charte d’usage de l’Intelligence Artificielle dans les SPSTI

Septembre 2025

I – Objet de la charte IA

La présente charte a pour objectif de **définir un cadre commun de l'intelligence artificielle (IA)** au sein des Services de Prévention et de Santé au Travail Interentreprises (SPSTI).

Elle vise à :

- Garantir que l'IA soit utilisée **au service de l'humain**, en soutien aux missions de prévention, de suivi et de santé au travail,
- **Protéger les données sensibles** et le secret médical,
- **Prévenir les dérives d'usage** (erreurs, biais, perte de sens, dépendance technologique),
- **Harmoniser les pratiques** entre les SPSTI, tout en laissant à chacun la liberté d'adapter la charte à ses spécificités.

Ce document complète la **charte informatique** existante et s'inscrit dans le respect du **RGPD**, du **code du travail**, et du futur **Règlement européen sur l'intelligence artificielle (AI Act)**.

II - L'IA en santé au travail

L'intelligence artificielle (IA) s'impose désormais comme un outil **incontournable** dans de nombreux secteurs, y compris celui de la **santé au travail**. Elle offre des perspectives d'innovation majeures qu'il s'agisse :

- **D'applications à visée médicale** comme la détection précoce des risques, l'aide à l'interprétation ou l'analyse de données médicales,
- **D'applications à visée organisationnelle et administrative**, comme l'optimisation des plannings, l'automatisation de tâches répétitives, l'assistance à la rédaction de documents ou la génération de supports de prévention.

Ces technologies permettent ainsi de mieux adapter **les actions de prévention** et d'améliorer l'efficacité des services de santé au travail.
Mais son usage soulève aussi des questions :

- Comment protéger le secret médical ou les secrets de fabrication ?
- Comment éviter que l'IA prenne une place qui doit rester celle du professionnel ?
- Comment utiliser ces outils tout en respectant le RGPD et les obligations réglementaires propre à l'IA ?

Afin d'harmoniser les pratiques et de garantir une utilisation responsable, Présanse a souhaité établir **une proposition de charte d'usage de l'IA**. Celle-ci a pour vocation de servir de cadre de référence pour l'ensemble des SPSTI, en s'alignant sur les réglementations en vigueur et sur les valeurs fondamentales de la santé au travail.

Elle n'a pas vocation à **s'imposer telle quelle**, mais à servir d'appui, de **modèle** et d'outil de sécurisation des pratiques.

Vous pouvez également **l'intégrer à votre propre gouvernance interne** en vous appuyant sur votre comité de direction, votre DPO, votre RSSI ou toute instance locale compétente,

afin de sélectionner les articles pertinents, **les adapter à vos processus existants** et les inscrire formellement dans votre charte informatique ou vos procédures internes.

Cette charte s'articule autour de **10 articles** qui définissent les engagements des SPSTI pour une IA éthique, responsable et au service de l'humain.

III – Les bonnes pratiques d'usage des outils d'IA

A - De manière générale :

- **Protéger les données confidentielles :** ne jamais saisir, copier ni transférer de données personnelles, médicales ou identifiantes dans un outil d'IA non validé par le SPSTI. Ne jamais saisir, copier ni transférer de données pouvant révéler un secret de fabrication dans un outil d'IA non validé par le SPSTI.
- **Vérifier systématiquement les résultats avant toute diffusion :** les productions d'IA peuvent comporter des erreurs, biais ou incohérences
- **Garder l'humain au centre :** l'IA ne doit jamais se substituer à la décision ou à l'évaluation d'un professionnel de santé
- **Conserver la traçabilité :** documenter les usages IA (outil utilisé, finalité, validation humaine)
- Participer à une **sensibilisation** sur les usages responsables de l'IA (éthique, RGPD, biais)

B - Pour les IA génératives publiques (ChatGPT, Copilot, Mistral AI, …) :

- **Les utiliser uniquement pour des besoins ponctuels et non sensibles :** aide à la rédaction de textes génériques, reformulation, traduction, veille documentaire, brainstorming, etc.
- **Ne jamais y insérer d'informations confidentielles :** relatives à un travailleur ou à un dossier médical ou à un process pouvant relever d'un secret de fabrication.
- **Toujours relire, corriger et contextualiser les contenus avant diffusion** interne ou externe
- **Mentionner l'utilisation d'une IA lorsqu'un contenu généré est diffusé en dehors du SPSTI** (rapport, support de prévention, communication)
- **Éviter d'utiliser l'IA pour produire des documents médicaux**, certificats, diagnostics ou comptes rendus officiels
- En cas de doute sur la légitimité d'un usage, demander l'avis du DPO, du RSSI ou du comité de gouvernance IA.

IV – Les 10 articles de référence pour un usage responsable de l'IA

Article 1 : Supervision Humaine

Ne jamais laisser une IA décider à la place d'un professionnel. Toute utilisation de l'IA doit être contrôlée, validée et assumée par un humain.

L'intelligence artificielle ne doit **en aucun cas se substituer au jugement d'un professionnel de santé ou d'un membre du personnel administratif compétent**. Aucune décision, analyse ou recommandation produite par une IA ne doit être utilisée sans **validation humaine préalable**, adaptée à la nature de l'usage.

Ignorer cette supervision reviendrait à transférer la responsabilité de décisions à un outil non conscient, ce qui est contraire aux obligations légales et déontologiques des SPSTI. Le maintien d'une supervision humaine garantit la **responsabilité médicale et administrative**, et préserve la **confiance des entreprises et des travailleurs** dans les dispositifs proposés.

Bon réflexe à adopter
Avant d'utiliser ou de diffuser une information issue d'un outil d'IA, vérifier **systématiquement son exactitude** et **la valider avec un professionnel compétent** (médecin, préventeur, ou agent administratif selon le cas).

Article 2 : Protection des données médicales

Ne jamais communiquer de données personnelles ou médicales à une IA non sécurisée. Toute information sensible doit rester confidentielle et protégée.

Les données de santé sont **strictement confidentielles, comme les données permettant d'identifier des process de fabrication**. Il est **interdit de transférer, saisir ou stocker** des données médicales ou personnelles identifiables dans un outil d'IA non validé par le SPSTI.

Aucune donnée ne doit être partagée avec des **IA génératives publiques** (ex. ChatGPT, Copilot, Gemini…) ni avec des applications externes dont les hébergements ne sont pas **certifiés et agréés** (ex. HDS). Le non-respect de ces règles met en péril le **secret médical**, le secret de fabrication, la **conformité RGPD** et la **confiance** entre travailleurs, employeurs et services de santé au travail.

Bon réflexe à adopter
Avant d'utiliser une IA, **vérifier le niveau de sécurité et d'hébergement des données** (HDS, RGPD) et **anonymiser** systématiquement les informations sensibles.

Article 3 : Transparence et explicabilité

Ne pas utiliser d'IA dont le fonctionnement est opaque. Tout outil d'IA doit être compréhensible, traçable et explicable par ses utilisateurs.

Une IA ne doit jamais être une **« boîte noire »** dont les résultats sont impossibles à interpréter. Il est **interdit d'utiliser ou de diffuser des résultats produits par une IA sans en comprendre les fondements, les limites et les sources de données**.

Les médecins, préventeurs et personnels des SPSTI doivent pouvoir **expliquer comment et pourquoi** un résultat a été généré, afin de pouvoir le **corriger ou le compléter** si nécessaire. Un usage non explicable de l'IA engendre **méfiance, perte de contrôle et risque d'erreur**, contraires aux valeurs de prévention et de santé publique.

Bon réflexe à adopter
Avant de valider un résultat produit par une IA, **demander systématiquement à l'éditeur ou à l'administrateur de l'outil** d'expliquer le fonctionnement et les critères d'analyse.

Article 4 : Équité et non-discrimination

Ne jamais utiliser une IA sans vérifier qu'elle ne produit pas de biais ou d'inégalités. Une IA ne doit pas défavoriser une personne en raison de son âge, de son sexe ou de son métier.

Les algorithmes apprennent à partir de données existantes, qui peuvent contenir des **biais sociaux, géographiques ou professionnels**. Il est donc **interdit d'utiliser un outil d'IA dont les résultats n'ont pas été analysés ou corrigés pour éviter ces biais**, sous peine de reproduire ou d'amplifier des formes de discrimination.

Dans les SPSTI, une IA non maîtrisée pourrait conduire à des **évaluations inéquitables** selon le sexe, l'âge, le poste ou le secteur d'activité. Toute utilisation de l'IA doit garantir à chacun **le même niveau de qualité, d'attention et de considération** dans le suivi médical et les actions de prévention.

Bon réflexe à adopter
Avant de déployer un outil d'IA, **vérifier avec le fournisseur ou le DPO** si les données d'apprentissage et les résultats ont été **testés pour détecter d'éventuels biais**.

Article 5 : Responsabilité et traçabilité

Ne pas utiliser l'IA sans savoir qui en est responsable. Toute décision issue d'un outil d'IA doit pouvoir être justifiée, tracée et validée par un humain.

Chaque usage de l'IA doit être **rattaché à un responsable identifié**. Il est **interdit d'utiliser un outil d'IA sans en documenter les usages, la finalité et les résultats**, car cela empêche tout contrôle en cas d'erreur ou de contestation. Les décisions prises à l'aide de l'IA doivent être **enregistrées, justifiées et conservées** afin de garantir la relecture et la responsabilité humaine.

L'intelligence artificielle ne peut **en aucun cas être considérée comme responsable** de ses productions : la responsabilité finale reste **entièrement humaine**. Toute information ou recommandation issue d'un outil IA doit être **vérifiée et validée** avant utilisation.
Concrètement, il convient de :

- **Consigner** chaque usage d'IA dans un registre interne ou un document partagé (date, outil, finalité, validation humaine)
- **Conserver** les versions ou résultats utilisés dans des décisions importantes
- **Mentionner** dans les comptes rendus lorsque l'IA a contribué à une rédaction ou à une analyse

Bon réflexe à adopter
Tenir un registre des usages IA, **vérifier chaque résultat avant diffusion**, et **ne jamais publier une donnée générée par IA sans validation humaine**.

Article 6 : Gouvernance

Ne pas déployer l'IA sans gouvernance claire. Chaque SPSTI doit définir qui contrôle, valide et suit les usages de l'IA.

L'intégration de l'IA doit s'appuyer sur une **organisation formalisée** garantissant un usage responsable et conforme. Il est **interdit de laisser se développer des usages d'IA sans contrôle ou coordination** : toute expérimentation isolée comporte un risque juridique, éthique ou de sécurité.

Chaque SPSTI doit donc mettre en place une **gouvernance claire et adaptée à sa taille**, capable de suivre les projets IA, d'en évaluer les risques et de garantir leur conformité réglementaire. Il est recommandé de constituer un **comité de gouvernance IA**, se réunissant au moins **une fois par trimestre**, chargé de :

- **Examiner** les nouveaux outils ou cas d'usage envisagés
- **Vérifier** la conformité au RGPD et aux exigences de sécurité
- **Partager** les retours d'expérience et incidents éventuels

Ce comité peut inclure Le **Directeur du SPSTI** (ou son représentant), le **DPO** (délégué à la protection des données), le **RSSI** (responsable sécurité des systèmes d'information), un **médecin du travail** ou **infirmier en santé au travail**, selon les cas, un **référent IA** ou un **assistant administratif impliqué dans les outils numériques**

Bon réflexe à adopter
Désigner un **référent IA** chargé de centraliser les questions, les incidents et les retours d'expérience, pour éviter les usages non encadrés.

Article 7 : Usage proportionné et utile

Ne pas utiliser l'IA par effet de mode. Tout usage doit répondre à un besoin concret, validé et utile à la prévention et à la santé au travail.

L'IA ne doit **jamais être utilisée sans finalité claire** ou simplement parce qu'un outil est disponible.

Un usage non justifié entraîne une **perte de temps, de ressources et des risques pour la sécurité des données**.

L'IA doit être mobilisée uniquement lorsqu'elle **apporte une réelle valeur ajoutée** à la mission de santé au travail, améliore la qualité de service ou simplifie un processus.

Chaque SPSTI doit ainsi distinguer les usages selon deux typologies :

- **Les IA "publiques"** (ChatGPT, Copilot, Gemini…) : utilisables uniquement à des fins de **veille, d'aide rédactionnelle ou de formation**, mais **jamais pour traiter des données personnelles, médicales, potentiellement relative à un secret de fabrication ou confidentielles.**
- **Les IA "métier" ou "professionnelles"** : intégrées dans des **solutions validées** (SaaS métier, outils internes, plateformes agréées), pouvant être utilisées dans le cadre du travail sous réserve de **validation par la gouvernance locale** (RSSI, DPO, direction).

Bon réflexe à adopter
Avant d'utiliser un outil IA, il faut se poser 3 questions : - Est-ce que cet usage répond à **un besoin professionnel réel** ? - Est-ce que l'outil est **autorisé et sécurisé** par le SPSTI ? - Est-ce que les données saisies sont **non confidentielles** ?

Article 8 : Sécurité et fiabilité

Ne jamais déployer une IA sans contrôle de sécurité préalable. Toute solution doit être vérifiée, testée et conforme avant utilisation.

Les systèmes d'IA doivent être **fiables, sûrs et protégés contre toute défaillance ou cyberattaque**.

Il est **interdit d'utiliser ou de connecter un outil d'IA non validé** par le DPO, le RSSI ou la gouvernance du SPSTI. Avant tout déploiement, chaque outil doit être **évalué selon les principes du "Security by Design"**, c'est-à-dire en intégrant dès la conception la protection des données, la cybersécurité et la conformité RGPD.

Concrètement, cela implique de : **vérifier** la conformité RGPD et les conditions d'hébergement des données, **mettre à jour régulièrement** les logiciels et les accès utilisateurs et **réaliser des tests ou audits internes** avant tout déploiement à grande échelle

En cas d'incident lié à l'IA (fuite de données, erreur de contenu, utilisation non autorisée, dysfonctionnement technique), il est **obligatoire d'agir immédiatement** :

1. **Informer sans délai** le DPO et/ou le RSSI en précisant la nature de l'incident et l'outil concerné
2. **Suspendre l'utilisation** de l'outil jusqu'à évaluation du risque
3. **Analyser l'incident** avec le comité de gouvernance IA
4. **Déclarer l'incident à la CNIL** sous 72h si des données personnelles sont concernées
5. **Corriger les causes** et **documenter** les mesures prises

Bon réflexe à adopter
Ne jamais ignorer un incident, même mineur. Tout dysfonctionnement ou comportement anormal d'un outil IA doit être **signalé immédiatement** au RSSI ou au DPO.

Article 9 : Formation et accompagnement

Ne pas laisser les équipes utiliser l'IA sans formation adaptée. Chaque professionnel doit comprendre les limites et les risques des outils avant leur usage.

L'intelligence artificielle ne peut être utilisée efficacement que par des utilisateurs **formés, sensibilisés et conscients de ses limites**.

Les SPSTI ne doivent pas déployer d'outils d'IA sans avoir assuré un **accompagnement préalable**, garantissant que chacun maîtrise les bonnes pratiques, la protection des données et les enjeux éthiques.

La formation doit inclure : les **risques éthiques et juridiques** (biais, confidentialité, responsabilités), l'**explication claire des règles d'usage** et des limites d'intervention de l'IA et le **partage de retours d'expérience** et de bonnes pratiques internes.

Il est recommandé d'organiser **au minimum une session annuelle de sensibilisation**, intégrée au plan de formation ou à la réunion d'équipe, pour tenir compte des évolutions rapides de la réglementation et des technologies.

Bon réflexe à adopter
Ne jamais présumer qu'un collaborateur "sait déjà" utiliser une IA. Avant tout déploiement, **vérifier que chaque utilisateur a reçu une formation** ou une sensibilisation adaptée à son poste et à l'outil utilisé.

Article 10 : Éco-responsabilité

Ne pas utiliser l'IA inutilement. Chaque usage doit être justifié et évaluer son impact environnemental et énergétique.

L'intelligence artificielle repose sur des infrastructures **fortement consommatrices d'énergie et de ressources**. Les SPSTI doivent éviter les usages superflus ou redondants, et **ne pas recourir à l'IA lorsqu'une solution humaine, simple ou locale suffit**.

Chaque outil ou fournisseur doit être sélectionné en privilégiant les **solutions sobres, hébergées localement** et respectueuses des principes de développement durable. L'éco-responsabilité dans le cadre de l'IA consiste à :

- **Limiter les requêtes et traitements inutiles** qui génèrent une charge de calcul excessive
- **Favoriser les outils mutualisés** plutôt que la multiplication des logiciels
- **Choisir des prestataires engagés** dans une démarche de sobriété numérique
- **Former les utilisateurs** à adopter un usage raisonné et conscient de l'impact écologique du numérique

Bon réflexe à adopter
Avant d'utiliser une IA : « Est-ce que cette tâche nécessite une IA, ou puis-je la réaliser autrement ? » **Le meilleur moyen de réduire l'empreinte écologique de l'IA est souvent d'utiliser d'abord son intelligence humaine.**

Vous retrouverez ci-dessous un tableau illustrant les typologies principales d'usages de l'IA dans les SPSTI. Il vise à aider les équipes à identifier les usages autorisés et donc à éviter les dérives.

V – Quand utiliser… et quand ne pas utiliser l'IA

Typologie d'usage	Utiliser l'IA pour	Ne pas utiliser l'IA pour
Fonctions supports / RH	Automatiser la planification des visites, ou de comptes rendus simples, sous supervision humaine	Partager des données **nominatives** dans des outils IA non sécurisés (ex. ChatGPT, Copilot public)
Analyse & plans d'actions	Identifier des **tendances anonymisées** sur les risques professionnels, accidents, pour orienter les actions de prévention	Établir des **conclusions ou diagnostics individuels** à partir de données médicales **non validées par un professionnel**
Communication interne & externe	Rédiger ou adapter des supports d'information sur les risques (bruit, sommeil, addictions, ergonomie), **sous relecture avant diffusion**	Diffuser **automatiquement** du contenu **sans validation humaine**, ou générer des messages personnalisés à partir de données sensibles
Aide à la décision	**Appuyer un professionnel de santé** dans la priorisation des actions, le repérage de signaux faibles ou la veille scientifique	**Remplacer le jugement clinique**, émettre un avis d'aptitude ou de contre-indication sans validation humaine
Formation et accompagnement	**Créer des supports** pédagogiques, fiches pratiques ou modules de sensibilisation interne à partir de données publiques	Former des professionnels en s'appuyant uniquement sur des contenus produits par IA sans vérification du contenu scientifique
Veille et documentation	**Rechercher des informations réglementaires ou médicales** à jour (AI Copilot, Mistral, etc.) pour faciliter la veille métier	Citer des contenus IA **sans vérification des sources** ou sans préciser que le texte a été généré automatiquement
	Utiliser l'IA pour **cartographier les risques** dans une entreprise ou un	Créer des profils individuels de risque ou des classements de

Gestion des risques collectifs	secteur à partir de données **anonymisées**	travailleurs à partir de données personnelles
Assistant IA « bureautique »	**Aider à rédiger** des documents internes (notes, rapports, procédures), sous validation d'un responsable	**Déléguer des décisions d'organisation ou d'évaluation** des travailleurs à un outil d'IA sans validation hiérarchique
Innovation et projets pilotes	Tester de nouveaux cas d'usage IA avec un comité de gouvernance local (RSSI, DPO, médecin, direction) et retour d'expérience partagé	Lancer des projets IA impliquant des données médicales sans avis préalable du comité ou sans documentation de l'expérimentation

VI – Annexes

Définitions utiles :

Intelligence Artificielle (IA) : ensemble de techniques permettant à un système de reproduire des comportements associés à l'intelligence humaine (raisonnement, apprentissage, perception, génération de texte ou d'image, etc.).

IA générative : forme d'IA capable de créer du contenu nouveau (texte, image, audio, code) à partir d'instructions ou d'exemples existants (ex : ChatGPT, Mistral AI, Copilot).

IA métier : application d'IA intégrée dans un logiciel professionnel validé et hébergé de manière sécurisée.

Donnée sensible : toute information relative à la santé, à l'identité ou à la situation professionnelle d'un travailleur.

Anonymisation : procédé par lequel toute donnée personnelle est transformée de manière irréversible pour qu'aucune identification ne soit possible.

DPO (Délégué à la Protection des Données) : personne chargée de veiller à la conformité des traitements de données au RGPD.

RSSI (Responsable de la Sécurité des Systèmes d'Information) : garant de la sécurité technique et organisationnelle des systèmes d'information.