



IA – Guide d'usage en ESMS

Septembre 2025 | Corpus documentaires



Sommaire

1	PREAMBULE	3
	<i>Ce que couvre ce guide.....</i>	<i>3</i>
	<i>Ce que ce guide ne couvre pas.....</i>	<i>3</i>
2	CADRE JURIDIQUE	3
	<i>Objectif.....</i>	<i>3</i>
	<i>Règles juridiques principales.....</i>	<i>3</i>
	<i>Éthique et obligations sociales</i>	<i>4</i>
	<i>IA Act (Loi européenne sur l'intelligence artificielle – 2024).....</i>	<i>4</i>
	<i>Cour des comptes – Rapport 2024.....</i>	<i>4</i>
3	FICHE « C'EST QUOI L'IA ? »	5
	<i>Définition claire</i>	<i>5</i>
	<i>Les principaux types d'IA.....</i>	<i>5</i>
	<i>Cas concrets d'utilisation en ESMS.....</i>	<i>5</i>
	FOCUS SUR L'IA GENERATIVE.....	5
	<i>Notions clés à connaître</i>	<i>5</i>
4	LES COMMANDEMENTS DE L'UTILISATION RESPONSABLE DE L'IA..	6
5	GUIDE DE MISE EN PLACE D'UN USAGE IA EN ESMS.....	6
6	GUIDE DE LA MISE EN PLACE D'UNE IA EN ESMS	6
	ANNEXE :	7
	ANNEXE A – CHARTE D'USAGE IA (SIGNABLE)	7
	ANNEXE B – WORKFLOW DE MISE EN PLACE IA EN ESMS.....	9
	ANNEXE C – FICHE PRATIQUE : « COMMENT REDIGER UN BON PROMPT ».....	10
	<i>Définition</i>	<i>10</i>
	<i>Checklist pour un prompt efficace</i>	<i>10</i>
	<i>Exemples</i>	<i>10</i>

1 Préambule

L'émergence rapide des outils d'intelligence artificielle (IA), notamment générative (ChatGPT, Gemini, Mistral, Claude, Midjourney...), bouleverse les pratiques professionnelles. Dans les établissements sociaux et médico-sociaux (ESMS), l'usage de l'IA peut représenter un levier pour améliorer la qualité de service, l'efficacité administrative et l'accompagnement des usagers.

Cependant, l'adoption non encadrée de ces technologies expose à des **risques majeurs** :

- fuites ou mésusage de données sensibles,
- erreurs ou hallucinations dans les résultats,
- biais discriminatoires,
- non-conformité réglementaire.

Ce guide vise à donner un **cadre clair, pragmatique et sécurisé** pour l'usage de l'IA en ESMS, afin de concilier innovation, éthique et protection des usagers.

Ce que couvre ce guide

- Les usages **administratifs, organisationnels et pédagogiques** de l'IA dans un ESMS.
- Les principes juridiques, éthiques et sécuritaires applicables.
- Les **bonnes pratiques** de mise en œuvre (procédures, validation, traçabilité).
- Une **charte d'usage à signer** par les professionnels.
- Des **outils pratiques** (checklist, registre, fiches pédagogiques).

Ce que ce guide ne couvre pas

- Le développement technique de solutions IA internes (conception d'algorithmes, entraînement de modèles).
- Les usages de l'IA dans le **diagnostic médical ou les actes de soin**, qui relèvent de la réglementation spécifique des dispositifs médicaux.
- Les expérimentations de recherche scientifique hors cadre ESMS.
- Les usages privés ou personnels de l'IA en dehors du contexte professionnel.

2 Cadre juridique

Objectif

Donner une vision claire des principales règles juridiques et éthiques qui encadrent l'usage de l'intelligence artificielle (IA) dans les ESMS, afin de sécuriser les pratiques et garantir la protection des droits des usagers.

Règles juridiques principales

RGPD (Règlement Général sur la Protection des Données – UE 2016/679)

Les **données de santé** et **données sociales** traitées dans les ESMS sont considérées comme des **données sensibles** (article 9).

- Principes clés :
- **Finalité déterminée** : les données ne doivent être utilisées que pour l'objectif défini.
- **Minimisation** : limiter la collecte et l'usage aux seules informations nécessaires.
- **Sécurité** : obligation de mettre en place des mesures techniques et organisationnelles adaptées (authentification forte, chiffrement, journalisation).
- **Information et consentement** : les usagers doivent être informés de l'usage de leurs données et, le cas échéant, donner leur consentement explicite.

Pour les ESMS : **aucune donnée nominative de santé ou sociale ne doit être communiquée à une IA**. [CNIL](#)

Éthique et obligations sociales

Le **Code de l'action sociale et des familles (CASF)** impose aux établissements de garantir :

- La **confidentialité** des informations relatives aux usagers.
- Le **respect de la dignité, de l'intimité et de la vie privée**.

La protection contre toute forme de discrimination.

- L'usage de l'IA doit s'inscrire dans ces valeurs fondamentales :
- **Éviter les biais** discriminatoires (âge, sexe, origine, handicap).
- **Préserver l'autonomie** et la prise de décision humaine.
- **Assurer la transparence** : informer usagers et familles quand une IA intervient.

IA Act (Loi européenne sur l'intelligence artificielle – 2024)

L'IA Act classe les systèmes d'IA en quatre catégories :

- **Risque inacceptable** : interdits (ex. manipulation subliminale, notation sociale).
- **Risque élevé** : soumis à des obligations strictes (documentation, supervision humaine, audits). Les ESMS peuvent être concernés si l'IA est utilisée dans le cadre de décisions impactant les droits fondamentaux des usagers.
- **Risque limité** : obligations de transparence (ex. mentionner qu'un contenu est généré par IA).
- **Risque minimal** : usage libre (ex. filtres anti-spam).

Pour les ESMS, la vigilance doit être maximale dès lors que l'IA intervient dans :

- La **gestion des parcours de soins et/ou d'accompagnement**.
- L'**accompagnement décisionnel** des professionnels.
- Toute situation pouvant avoir un impact sur la dignité ou les droits des usagers.

Cour des comptes – Rapport 2024

La Cour des comptes a souligné que l'IA dans la santé, le médico-social et social ne peut se développer qu'avec :

- Un **encadrement strict des usages**.
- Une **transparence renforcée** sur les finalités.
- Une **supervision humaine permanente**.

Elle alerte sur les risques de dépendance aux outils privés non maîtrisés et recommande une gouvernance publique forte.

Ressources complémentaires : CNIL (plan IA), ANSSI (sécurisation IA générative, 2024), ANAP (guide "Déployer une IA en toute confiance").

3 Fiche « C'est quoi l'IA ? »

Donner une définition simple et pratique de l'intelligence artificielle (IA), présenter ses différents types et usages, et sensibiliser aux bonnes pratiques.

Définition claire

« Système basé sur une machine, conçu pour fonctionner avec différents niveaux d'autonomie, qui peut s'adapter après son déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer des environnements physiques ou virtuels »

EU IA Act

L'IA n'a **pas de conscience ni d'intention** : elle fonctionne uniquement à partir d'algorithmes et de probabilités.

- **IA à usage interdit** : Pratiques de manipulation, d'exploitation et de contrôle social
Exemples : système de reconnaissance faciale pour la surveillance de masse, de scoring social, etc.

IA à haut risque : Préjudice potentiel pour la sécurité, la santé ou le respect des droits fondamentaux

Exemples : système de notation de crédit automatisé, d'assistance au recrutement, de diagnostic médical automatisé, de recommandation de produits, etc.)

- **IA à risque "limité"** : Tous les autres systèmes d'IA

Les principaux types d'IA

- **IA analytique** : analyse des données pour détecter des tendances ou des anomalies.
Exemple : suivi des indicateurs de qualité en ESMS.
- **IA prédictive** : anticipe des événements ou des besoins à partir de données historiques.
Exemple : gestion de planning ou prédiction d'absences.
- **IA générative** : crée du contenu (texte, images, vidéos) à partir de requêtes en langage naturel.
Exemple : rédaction d'un compte rendu, création d'une affiche.

Cas concrets d'utilisation en ESMS

- **Administratif** : rédaction d'e-mails, synthèse de réunions, aide à la mise en page.
- **Communication** : création d'affiches internes, supports de sensibilisation.
- **Formation et sensibilisation** : générer des supports pédagogiques pour les équipes.
- **Analyse de données** : extraction de tendances à partir de questionnaires anonymisés.

Focus sur l'IA générative

Les IA génératives sont les plus visibles aujourd'hui. Elles permettent de produire du **texte, du code, des images ou des vidéos** à partir de simples instructions (appelées *prompts*).

- Outils courants : Copilot, ChatGPT, Gemini, Mistral, Claude, Midjourney.
- Risques spécifiques : hallucinations, biais, droits d'auteur.

Notions clés à connaître

Bien parler à l'IA : le prompt

- **Prompt** = consigne donnée à l'IA → précision = qualité.
- **Hallucinations** → une IA peut inventer. Vérification humaine obligatoire.
- **Images/vidéos** → attention aux droits d'auteur, pas de données personnelles dans des IA publiques.

Détails en annexe

Création d'images et vidéos par IA

- Les images/vidéos générées peuvent réutiliser des styles ou contenus existants → **risques liés aux droits d'auteur**.
- Obligation de vérifier la conformité avant diffusion publique.
- Interdiction d'utiliser des données personnelles (photos, vidéos d'utilisateurs ou de professionnels) dans des IA publiques.

En résumé : L'IA est un **outil d'assistance**. Elle peut faciliter le quotidien en ESMS (administration, communication, analyse), mais elle doit être utilisée **avec discernement, transparence et supervision humaine**.

4 Les commandements de l'utilisation responsable de l'IA

1. Je partage mes usages en toute transparence
2. Je veille à la sécurité informatique dans mon usage
3. Je veille à la confidentialité et à la protection des données
4. Je veille aux droits d'auteur
5. Je donne du sens à mon usage dans le cadre de mon travail
6. J'utilise l'IA de manière éco-responsable
7. Je respecte les enjeux humains et éthiques
8. Je ne diffuse pas d'informations générées par IA sans validation

Détails en annexe

5 Guide de mise en place d'un usage IA en ESMS

1. Identifier l'usage en interne : Quelle est la finalité ?
2. Analyser les risques : Analyse d'impact (AIPD) et sécurité
3. Évaluer le niveau de risque en fonction des usages
4. Définir une procédure interne claire pour l'utilisation des logiciels IA :
 - a. Validation avec le référent (DPO/RSSI)
 - b. Utilisation des outils validés par la direction
 - c. Intégration à la communauté interne d'utilisateurs
 - d. Respect strict du RGPD
 - e. Vérification systématique de la fiabilité des résultats

Détails en annexe

6 Guide de la mise en place d'une IA en ESMS

Les 7 étapes de validation interne

1. **Identifier l'usage** : Définir la finalité (ex. rédiger un compte rendu).
2. **Analyser les risques** : Vérifier la sensibilité des données et réaliser une AIPD si nécessaire.
3. **Évaluer le niveau de risque** : Classer l'usage selon l'IA Act (inacceptable, élevé, limité, minimal).
4. **Valider l'outil** : Soumettre au DPO/RSSI et à la direction.
5. **Définir la procédure** : Lister les outils autorisés, encadrer les usages.
6. **Vérifier les résultats** : Contrôle humain obligatoire avant diffusion.
7. **Tracer et documenter** : Inscrire l'usage dans le registre interne.

Détails en annexe

Annexe :

Annexe A – Charte d'usage IA (signable)

8 commandements présentés comme articles, avec **nom, fonction, date, signature**

1. Je partage mes usages en toute transparence

- Parce que l'IA est devenue un outil de notre quotidien : partager vos usages permet de mieux comprendre et maîtriser l'IA
- Parce que cela réduit le risque d'erreur ou de diffusion involontaire de données sensibles
- Parce que cela favorise l'entraide et l'appropriation collective des outils
- Parce que la transparence crée un cercle vertueux de bonnes pratiques

En partageant vos usages, vous aidez vos collègues à gagner du temps et à se concentrer sur des tâches à forte valeur ajoutée, tout en bénéficiant de leur regard bienveillant pour sécuriser vos pratiques.

2. Je veille à la sécurité informatique dans mon usage

- Parce que chaque outil IA peut être une porte d'entrée pour des menaces informatiques
- Parce que respecter les règles internes (mots de passe, MFA, réseau sécurisé) limite les risques
- Parce qu'une vigilance constante protège les systèmes et les données de votre établissement
- Parce qu'un usage responsable participe à la résilience collective

En intégrant la sécurité dans vos usages, vous contribuez à la protection de l'ensemble de votre ESMS et prévenez des incidents qui pourraient avoir des conséquences importantes.

3. Je veille à la confidentialité et à la protection des données

- Parce que les informations sensibles des usagers et des collaborateurs doivent rester protégées
- Parce que l'IA peut traiter des données sensibles et il faut respecter les obligations légales (RGPD, CASF)
- Parce que le partage non maîtrisé de données peut générer des risques juridiques et réputationnels
- Parce que la confidentialité est un pilier de confiance avec vos collègues et usagers

En appliquant ces principes, vous garantisiez la protection des données et la conformité légale, tout en renforçant la confiance autour de votre usage de l'IA.

4. Je veille aux droits d'auteur

- Parce que les contenus générés par l'IA peuvent être basés sur des œuvres protégées
- Parce que respecter les licences et droits d'auteur protège votre établissement et vous-même
- Parce que citer ses sources favorise l'exemplarité et la transparence
- Parce que le respect des droits d'auteur est un levier d'innovation responsable

En respectant les droits d'auteur, vous utilisez l'IA de manière éthique et légale, tout en valorisant le travail des créateurs.

5. Je donne du sens à mon usage dans le cadre de mon travail

- Parce que l'IA doit soutenir vos missions et non les détourner
- Parce que tout usage doit être justifié par un objectif professionnel clair
- Parce qu'un usage réfléchi maximise votre efficacité et la pertinence des résultats
- Parce que donner du sens favorise l'adoption responsable de l'outil par vos collègues

En alignant l'IA avec vos missions, vous créez de la valeur réelle pour votre établissement et vos usagers.

6. J'utilise l'IA de manière éco-responsable

- Parce que les outils IA consomment des ressources énergétiques importantes
- Parce que limiter les usages inutiles réduit l'impact environnemental
- Parce que le choix d'outils responsables et l'optimisation des requêtes contribuent à la durabilité
- Parce qu'un usage conscient est un exemple pour l'ensemble de votre équipe

En intégrant l'éco-responsabilité dans vos pratiques, vous contribuez à un usage durable de l'IA.

7. Je respecte les enjeux humains et éthiques

- Parce que l'IA ne doit pas remplacer le jugement humain ni la responsabilité professionnelle
- Parce qu'il faut éviter toute discrimination, biais ou préjugé dans ses usages
- Parce que l'éthique garantit que vos pratiques respectent les droits et la dignité des usagers
- Parce qu'un usage responsable renforce la confiance et la légitimité de l'IA

En respectant ces principes, vous placez l'humain au centre de vos décisions et de vos usages.

8. Je ne diffuse pas d'informations générées par IA sans validation

- Parce que les contenus générés peuvent contenir des erreurs, imprécisions ou biais
- Parce que la vérification des informations protège votre établissement et vos collègues
- Parce qu'une validation préalable garantit la fiabilité et la crédibilité des contenus
- Parce que diffuser sans contrôle peut entraîner des conséquences professionnelles et juridiques

En validant les informations avant diffusion, vous assurez la qualité, la sécurité et la confiance autour de l'usage de l'IA.

Annexe B – Workflow de mise en place IA en ESMS

1. Identifier l'usage en interne : quelle est la finalité ?

- Parce qu'il est essentiel de savoir pourquoi vous utilisez l'IA avant de l'implémenter
- Parce que définir clairement la finalité permet d'aligner l'outil avec vos missions et besoins
- Parce que cela évite les usages superflus ou inadaptés
- Parce que cette étape facilite l'adhésion des équipes et la communication interne

En clarifiant la finalité, vous assurez un usage ciblé, utile et sécurisé, et vous favorisez l'efficacité collective dans votre ESMS.

2. Analyser les risques : Analyse d'impact (AIPD) et sécurité

- Parce que tout usage d'IA peut générer des risques pour les données et la sécurité
- Parce qu'une AIPD identifie les impacts potentiels sur les droits et libertés des usagers
- Parce que la sécurité informatique doit être intégrée dès le départ
- Parce qu'une analyse rigoureuse permet de prévenir incidents et non-conformités

En réalisant cette analyse, vous protégez votre établissement, vos collègues et les usagers, et vous vous conformez aux obligations légales.

3. Évaluer le niveau de risque en fonction des usages

- Parce que tous les usages ne présentent pas le même niveau de risque
- Parce que hiérarchiser les risques permet de prioriser les mesures de protection
- Parce que cette évaluation facilite la décision sur l'opportunité et les conditions d'utilisation
- Parce que cela guide la définition des procédures et responsabilités

En évaluant le risque, vous prenez des décisions éclairées et sécurisez l'intégration de l'IA dans vos pratiques.

4. Définir une procédure interne claire pour l'utilisation des logiciels IA

a. Validation avec le référent (DPO/RSSI)

- Parce que le référent garantit la conformité aux règles internes et légales
- Parce que cette étape limite les erreurs et les usages non autorisés

b. Utilisation des outils validés par la direction

- Parce que seuls les outils évalués sont sûrs et conformes
- Parce que cela centralise la responsabilité et la traçabilité

c. Intégration à la communauté interne d'utilisateurs

- Parce que partager vos expériences favorise l'appropriation collective et les bonnes pratiques
- Parce que cela permet de bénéficier du retour d'expérience de vos collègues

d. Respect strict du RGPD

- Parce que les données personnelles des usagers et collaborateurs doivent être protégées
- Parce que le non-respect entraîne des risques juridiques et réputationnels

e. Vérification systématique de la fiabilité des résultats

- Parce que l'IA peut générer des erreurs ou biais
- Parce qu'une validation préalable garantit des décisions fiables et responsables

En suivant cette procédure, vous sécurisez l'usage de l'IA, vous assurez la conformité légale et éthique, et vous favorisez un déploiement maîtrisé et durable au sein de votre ESMS.

Annexe C – Fiche pratique : « Comment rédiger un bon prompt »

Définition

Un **prompt** est la consigne donnée à une IA. Plus il est précis, plus le résultat est pertinent.

Checklist pour un prompt efficace

- **Contexte** : préciser le public et l'objectif
- **Tâche** : indiquer ce que l'IA doit faire
- **Format attendu** : liste, tableau, texte court...
- **Style / ton** : professionnel, pédagogique, neutre...
- **Contraintes** : RGPD, pas de jargon, pas de données sensibles

Exemples

✗ Mauvais prompt : « Fais-moi un rapport. »

✓ Bon prompt :

« Rédige un rapport de réunion pour des professionnels d'ESMS en 5 points clés, style professionnel et clair, sans jargon. »

⚠ Rappel : toujours vérifier et valider les résultats avant diffusion.