Modèle de charte d'utilisation de l'intelligence artificielle (IA)

pour les établissements sociaux et médico-sociaux (ESMS) de Nouvelle-Aquitaine

Table des matières

Version 1	Juillet 2026	

1. Préambule

L'Agence Régionale de Santé de Nouvelle-Aquitaine, le GRADeS ESEA Nouvelle-Aquitaine et le collectif SI ESMS Nouvelle-Aquitaine ont collaboré pour construire un modèle de charte d'utilisation de l'Intelligence Artificielle (IA) pour les établissements sociaux et médico-sociaux (ESMS) de la région.

Il a pour objectifs :

- De partager des éléments clés constitutifs d'une charte d'utilisation de l'IA,
- De guider les établissements dans la rédaction d'une future charte.

Il peut contribuer à mieux :

- Encadrer le déploiement, l'utilisation et l'évaluation des solutions d'IA au sein des ESMS,
- Définir un usage éthique, sûr, transparent et conforme à la réglementation française et européenne.

Cette charte n'a pas vocation à être reprise en l'état. Elle constitue une base de travail qui doit être adaptée par chaque établissement en fonction de son organisation, de sa gouvernance, de ses activités, de ses projets IA, de son niveau de maturité numérique et de son environnement réglementaire et contractuel.
La responsabilité de l'élaboration, de l'adaptation et de l'application de la charte incombe pleinement à chaque établissement. À ce titre, le document final doit faire l'objet d'une validation formelle par la direction de l'établissement après avis du Délégué à la Protection des Données (DPO), en lien avec les instances compétentes (DSI, RSSI, qualité, comités éthiques ou cliniques le cas échéant).

Dans son contexte d'usage, cette charte est :

- Soit un document complémentaire à une charte informatique existante,
- Soit pleinement inscrite dans la charte informatique de l'établissement avec un chapitre dédié.

Ce document est vivant et pourra être mis à jour dès évolution du cadre réglementaire (AI Act européen, nouvelles exigences HAS, nouvelles ressources ANAP etc).

Dans la continuité de notre démarche de co-construction, nous invitons les ESMS intéressés à nous envoyer leurs recommandations pour faire évoluer ce modèle et ainsi bénéficier à tous.
Pour contacter les équipes du GRADeS ESEA et de l'ARS Nouvelle-Aquitaine :

- **Le pôle numérique en santé de l'ARS : ars-na-numerique-en-sante@ars.sante.fr** ;
- **La direction innovation du GRADeS ESEA : innovation@esea-na.fr.**

2. Modèle : Charte de l'établissement sur l'utilisation d'une solution d'intelligence artificielle

Ce modèle présente les engagements que l'établissement a pris par rapport au déploiement de l'IA dans sa structure afin de garantir un usage cadré, de confiance, souverain, raisonnable et raisonné. Elle a pour objectifs d'informer les professionnels sur les actions portées par la direction.

Elle est constituée de 4 parties principales :

- Responsabilité et gouvernance,
- Transparence et explicabilité,
- Formation et cadre des usages,
- Sécurité, confidentialité et conformité réglementaire.

L'intégration de l'IA doit s'appuyer sur une organisation formalisée garantissant un usage responsable et conforme. Toute expérimentation isolée de l'IA (sans accord préalable de la direction) comporte un risque juridique, éthique et/ou de sécurité, et pourrait être proscrite au sein de l'établissement.

La structure reconnaît que la maîtrise des systèmes d'intelligence artificielle repose sur la compétence, la vigilance et la responsabilité des professionnels qui les utilisent. À ce titre, elle s'engage à mettre en place une politique de formation et de sensibilisation structurée, progressive et adaptée aux niveaux de responsabilité et aux usages, afin de garantir un recours à l'IA conforme aux exigences réglementaires, éthiques et professionnelles.

2.1. Responsabilité et gouvernance

- Intégrer les travaux sur les usages de l'IA à la gouvernance interne dédiée au numérique (référent IA, DPO, direction, directeur des systèmes d'informations), dans l'éventualité où il n'y a pas de gouvernance dédiée au numérique, en créer une dotée d'une instance spécifique à l'IA.
- Tracer les décisions et clarifier les responsabilités dans l'usage des systèmes d'IA via une matrice de responsabilités inspirée des modèles RACI (fig 1)
- Prendre en compte le cadre éthique national (responsabilité, transparence, explicabilité, équité, proportionnalité), conformément au guide éthique national sur l'IA en santé[1].
- Tenir à jour un registre des solutions d'intelligence artificielle autorisées au sein de l'établissement précisant notamment :
    - La finalité du système.
    - Son éditeur.
    - Les services utilisateurs.
    - Son niveau de risque au regard de l'IA Act.

[1] Guide | Ethique de l'intelligence artificielle en santé

  - Le responsable de son suivi.
- Fournir aux salariés une liste de logiciels intégrant une IA validée par la Direction, pour un usage professionnel au sein de l'établissement (cartographie des SIA autorisés).
- Assurer en interne une procédure de déclaration et de signalement pour
  - Les retours d'expérience et les besoins d'usages IA.
  - Les incidents relatifs à l'utilisation de l'IA
  - La formalisation d'une demande d'utilisation d'une IA non référencée par l'établissement.
- Mettre en place une veille réglementaire, technologique et sécuritaire afin d'anticiper les évolutions des systèmes d'intelligence artificielle, les nouvelles menaces et les recommandations des autorités compétentes.
- Rester en veille sur les recommandations de l'ANAP pour le choix des solutions d'IA et sur celles de la HAS dans les nouveaux critères de certification (information des patients).
- Toute évolution majeure d'une solution d'IA (nouveau modèle, réentraînement, évolution fonctionnelle ou modification des traitements de données) devra faire l'objet d'une nouvelle analyse avant sa mise en service dans l'établissement.
- L'établissement s'engage à une politique de sobriété numérique :
  - Évaluation systématique du rapport bénéfice / impact environnemental ;
  - Privilégier l'IA frugale, éviter les traitements superflus ;
  - Recours prioritaire à des solutions hébergées en Europe et conformes aux exigences applicables à l'hébergement de données de santé.

Fig 1 : modèle de RACI

Lettre	Signification	Rôle
R	Réalisateur	Personne(s) en charge de l'exécution opérationnelle de la tâche.
A	Approbateur	Personne responsable du travail réalisé par le ou les réalisateurs. Décisionnaire final.
C	Consulté	Personne sollicitée pour apporter un avis, une expertise ou des conseils dans son domaine de compétence.
I	Informé	Personne ou partie prenante tenue informée de l'avancement ou des résultats, sans implication directe dans la réalisation.

2.2. Transparence et explicabilité

- Interroger son fournisseur/éditeur sur la documentation complète qui concerne le système d'IA et s'informer sur ce qu'elle contient, notamment sur tout ce qui concerne le traitement et l'hébergement des données décrivant notamment :
  - La finalité du système.
  - Les usages autorisés.
  - Les usages exclus.

  - Les catégories de données traitées.
  - Les modalités d'hébergement.
  - Les composants logiciels tiers utilisés.
  - Les limites connues du système.
- S'assurer que les professionnels disposent d'une information compréhensible sur :
  - Le fonctionnement général de l'IA.
  - Son degré d'autonomie.
  - Les interventions humaines nécessaires.
  - Les limites de fiabilité des résultats produits.
- S'assurer de la traçabilité (ou journalisation) des réponses apportées de l'IA (soit via le fournisseur soit en interne en fonction de la sensibilité des données et en vue d'améliorer l'outil IA aux usages propres à l'établissement)
- Notifier les personnes accompagnées, tuteurs légaux dès que des solutions d'IA sont utilisées pour aider à leur prise en charge, notamment s'il s'agit d'une IA aide à la décision ou diagnostic. Les personnes sont en droit de refuser, ce qui peut conduire à devoir trouver des alternatives.
- Intégrer l'usage de l'IA dans la charte établissement remise au patient.

2.3. Formation et cadre des usages

- Former le personnel de l'établissement sur les fondamentaux autour de l'intelligence artificielle et ses bonnes pratiques en santé
- Fournir au personnel de l'établissement :
  - Des règles de bonnes pratiques sur l'usage de l'IA dans leurs quotidien et tâches. Ce document sera mis à jour régulièrement par la gouvernance de l'établissement.
  - Un guide propre à l'utilisation du SIA proposé (à voir avec le fournisseur ou en interne, et spécifiant bien le cadre de son utilisation et ses limites)
- Assurer un retour d'expérience des usages, des bonnes pratiques mais aussi des incidents et difficultés pour la bonne appropriation du cadre d'usage.
- Sensibiliser les utilisateurs aux limites connues des systèmes d'IA, aux risques de biais algorithmiques et aux situations dans lesquelles l'outil ne doit pas être utilisé.
- Organiser des actions régulières de mise à jour des connaissances lors des évolutions importantes des outils ou de la réglementation.

2.4. Sécurité, confidentialité et conformité réglementaire

L'établissement s'engage à :

- Utiliser des outils IA hébergés en France ou Union Européenne, et donc soumis directement au RGPD.

- Encadrer explicitement le traitement des données sensibles dans le cadre des projets d'IA, notamment en interrogeant l'éditeur/le fournisseur. Le cadre légal devra être respecté.
- Evaluer régulièrement avec le fournisseur, les mesures de sécurité des solutions intégrant une IA.
- Formaliser un protocole de sécurité en cas d'incident lié à l'IA empêchant le fonctionnement du service
- S'assurer du respect de l'IA Act par le fournisseur de la solution avec notamment :
    - Mise en place d'un système de gestion du risque (risk management) ;
    - Documentation technique complète ;
    - Qualité et gouvernance des données d'entraînement : vérifier que les données ou documents transmis à une IA ne sont pas réutilisés à des fins d'entraînement sans autorisation explicite de l'établissement….
- S'assurer que les performances annoncées par l'éditeur sont documentées et adaptées aux usages envisagés (robustesse, fiabilité, précision lorsque ces informations sont disponibles).
- Vérifier que les conversations (prompts) et les réponses générées peuvent être supprimées et qu'elles ne sont pas conservées au-delà des durées nécessaires.
- Limiter la collecte des métadonnées (adresse IP, localisation, informations techniques…) au strict nécessaire.
- Vérifier que les fichiers téléversés dans une solution d'IA peuvent être supprimés automatiquement ou à la demande.
- Lorsque des solutions Cloud sont utilisées, identifier les risques liés à la localisation des données et aux législations extraterritoriales pouvant permettre l'accès à ces données par des autorités étrangères.
- Lorsque cela est possible, privilégier le traitement des données pseudonymisées et conserver les opérations de réidentification sous le contrôle de l'établissement.
- S'assurer que les interconnexions entre les systèmes d'IA et le système d'information sont limitées aux seuls besoins fonctionnels afin de réduire les risques de cybersécurité.