IA dans la Santé et HDS 2026 : Guide de Conformité

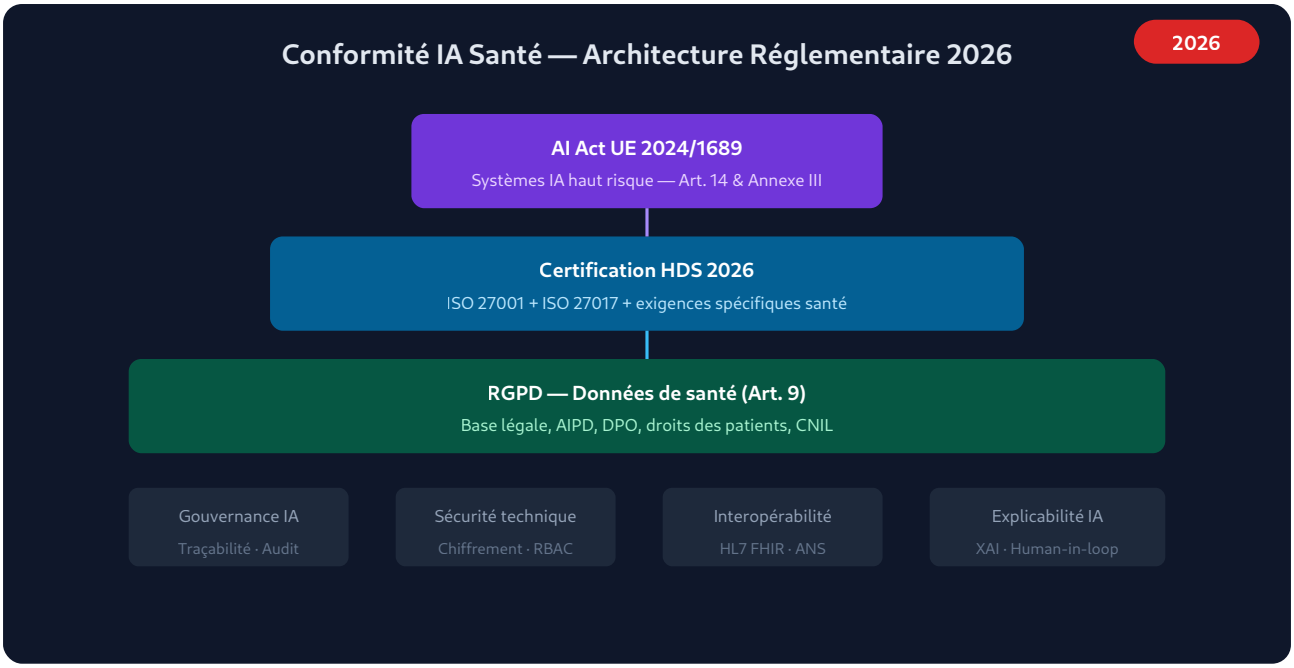
Maîtrisez la conformité IA santé HDS 2026 : certification HDS, AI Act, RGPD et exigences CNIL pour les établissements de santé utilisant l'IA en France.

Résumé exécutif

En 2026, les établissements de santé français font face à une triple contrainte réglementaire inédite : la certification HDS révisée, l'entrée en vigueur complète de l'AI Act européen pour les systèmes IA à haut risque, et le renforcement des obligations RGPD pour les données de santé traitées par l'intelligence artificielle. Ce guide technique décrypte les exigences, les risques de non-conformité et les étapes concrètes pour bâtir une architecture IA médicale conforme et pérenne.

La **conformité IA santé HDS 2026** représente l'un des chantiers réglementaires les plus complexes que les établissements de santé français aient eu à affronter. L'essor de l'intelligence artificielle dans les hôpitaux, cliniques et laboratoires — qu'il s'agisse d'aide au diagnostic radiologique, de prédiction des durées de séjour, de tri des urgences ou de prescription médicamenteuse assistée — soulève des questions juridiques, techniques et éthiques sans précédent. Depuis le 1er août 2024, l'AI Act est entré en vigueur dans l'Union européenne, et ses dispositions les plus contraignantes s'appliquent pleinement aux systèmes IA déployés en contexte médical dès 2026. Parallèlement, la certification HDS (Hébergeur de Données de Santé) a été profondément révisée pour intégrer les nouvelles menaces cyber et les spécificités des environnements IA. Les données de santé — parmi les plus sensibles qui soient — nécessitent des garanties techniques et organisationnelles renforcées lorsqu'elles alimentent des modèles de machine learning ou des agents autonomes. Ce guide synthétise l'ensemble des obligations

applicables en 2026, propose une méthodologie d'audit structurée en cinq phases et détaille l'architecture technique attendue pour atteindre un niveau de conformité optimal face aux autorités de contrôle françaises et européennes.



Architecture réglementaire de la conformité IA dans la santé en 2026 : trois couches normatives superposées (AI Act, HDS, RGPD)

Le cadre réglementaire HDS 2026 et l'intelligence artificielle en santé

En 2026, le secteur de la santé numérique français opère dans un environnement normatif profondément reconfiguré. Trois textes majeurs s'articulent de manière complémentaire : le **Règlement européen sur l'intelligence artificielle (AI Act, 2024/1689)**, la **certification HDS révisée** pilotée par l'ANS (Agence du Numérique en Santé), et le **RGPD** dont les exigences sont amplifiées dès lors que des données de santé alimentent des systèmes IA. Ces trois dispositifs ne s'appliquent pas indépendamment l'un de l'autre : ils forment un triptyque normatif dont chaque établissement de santé doit maîtriser les intersections.

⚡ **Retour terrain**

J'ai réalisé un audit de conformité PCI-DSS pour un e-commerçant de taille moyenne. La surprise : leur prestataire de paiement gérait effectivement la conformité PCI côté serveur, mais les formulaires de carte côté client passaient par leurs propres serveurs via un JavaScript personnalisé — introduisant un scope PCI non déclaré. La remédiation a nécessité une migration vers un formulaire de paiement hébergé (redirect ou iFrame).

L'Agence du Numérique en Santé, via son portail esante.gouv.fr/securite, publie régulièrement les référentiels de sécurité applicables aux systèmes d'information de santé, incluant désormais des volets dédiés à l'IA. Ces référentiels s'imposent aux établissements de santé relevant du service public hospitalier et aux éditeurs de logiciels médicaux. La mise à jour 2025-2026 intègre explicitement les exigences de l'AI Act pour les systèmes embarqués dans des dispositifs médicaux ou utilisés dans des processus cliniques à fort enjeu.

Pour les équipes cybersécurité et conformité, la difficulté réside dans la superposition de temporalités différentes : le RGPD est applicable depuis 2018, l'AI Act entre en application progressive jusqu'en 2027, et la certification HDS oblige les hébergeurs à adapter leurs pratiques au fil des révisions annuelles. Naviguer dans cet environnement nécessite une veille réglementaire continue et une gouvernance transversale associant DSI, DPO, responsables qualité et directions médicales.

L'AI Act européen : classification des systèmes IA à haut risque dans la santé

Le Règlement UE 2024/1689 (AI Act) classe les systèmes IA utilisés en santé parmi les **systèmes à haut risque**, soumis aux obligations les plus contraignantes du texte. L'Annexe III identifie explicitement les systèmes IA déployés dans les dispositifs médicaux au sens du Règlement MDR 2017/745, les systèmes d'aide au diagnostic, de triage des urgences et de prédiction

pronostique. Cette classification entraîne des obligations de conformité avant mise sur le marché et tout au long du cycle de vie du système.

Les principales obligations imposées aux fournisseurs de systèmes IA à haut risque en santé comprennent : la mise en place d'un **système de gestion des risques** documenté et maintenu, la garantie de la qualité et de la représentativité des données d'entraînement, la disponibilité de *logs d'audit* permettant la traçabilité des décisions automatisées, et la fourniture d'une documentation technique exhaustive. L'article 14 du règlement impose en outre un **contrôle humain effectif** (human oversight) permettant à des professionnels de santé qualifiés d'intervenir, corriger ou désactiver le système à tout moment.

Pour les établissements de santé qui ne sont pas fournisseurs mais **déployeurs** (*deployers*) de systèmes IA tiers, le règlement impose néanmoins des obligations propres : s'assurer que le système est utilisé conformément aux instructions du fournisseur, mettre en place une surveillance de l'exploitation, désigner les personnes responsables du contrôle humain, et conserver des logs d'utilisation pendant une durée minimale définie. En 2026, les pénalités pour non-conformité à l'AI Act peuvent atteindre **30 millions d'euros ou 6 % du chiffre d'affaires mondial** pour les infractions les plus graves.

Il convient de distinguer les systèmes IA intégrés à des *dispositifs médicaux* — qui relèvent simultanément du MDR et de l'AI Act — des systèmes IA purement organisationnels (gestion des lits, planification du personnel, facturation). Ces derniers peuvent ne pas être classés à haut risque, mais ils traitent souvent des données de santé et restent soumis au RGPD et aux politiques de sécurité HDS. Consultez notre article sur l'AI Act, RGPD et agents IA en 2026 pour une analyse approfondie des régimes applicables selon les cas d'usage.

HDS 2026 : les nouvelles exigences de certification pour l'hébergement de données de santé

La **certification HDS** (Hébergeur de Données de Santé) est obligatoire en France pour tout acteur hébergeant des données de santé à caractère personnel pour le compte de tiers. En 2026, cette certification s'appuie sur un référentiel actualisé qui intègre les leçons des incidents cyber majeurs ayant touché le secteur hospitalier depuis 2021, ainsi que les nouvelles pratiques liées au

cloud et à l'IA. Notre article dédié sur la certification HDS 2026 détaille l'ensemble des changements du référentiel applicables aux environnements IA.

Le référentiel HDS 2026 s'articule autour de six activités d'hébergement certifiables : la mise à disposition et le maintien en condition opérationnelle des sites physiques, des infrastructures matérielles, des plateformes d'hébergement, des applications métier de santé, la sauvegarde externalisée, et la fourniture de l'accès aux données hébergées. Les systèmes IA en santé impactent particulièrement les activités 4 et 5 — plateformes et applications — qui doivent désormais intégrer des contrôles spécifiques : gestion des versions de modèles, traçabilité des inférences, isolation des environnements d'entraînement et de production.

Un point critique en 2026 concerne la **localisation des données d'entraînement** des modèles IA. Si le modèle est entraîné sur des données de santé pseudonymisées ou anonymisées, l'hébergeur doit démontrer que le processus d'anonymisation est robuste et irréversible — ce qui est techniquement difficile pour des données médicales complexes. La CNIL et l'ANS ont publié conjointement des lignes directrices précisant que l'anonymisation au sens de l'AI Act doit résister aux attaques de ré-identification, y compris par des techniques adversariales modernes.

RGPD et données de santé : obligations renforcées pour les systèmes IA

Le RGPD classe les données de santé comme des **données sensibles de catégorie spéciale** (article 9), dont le traitement est en principe interdit sauf exceptions limitativement énumérées. En contexte médical, les bases légales les plus fréquemment invoquées sont le consentement explicite du patient, la nécessité pour des fins de médecine préventive ou curative, et les intérêts publics dans le domaine de la santé publique. L'utilisation de ces données pour entraîner des modèles IA soulève des questions spécifiques : la base légale initiale de collecte couvre-t-elle l'entraînement IA ? L'information délivrée aux patients est-elle suffisamment transparente ?

La **CNIL** a publié en 2025 et mis à jour en 2026 des recommandations opérationnelles sur l'utilisation de l'IA générative en santé. Ces recommandations, que nous analysons dans notre guide sur le référentiel CNIL IA générative 2026, imposent notamment une *Analyse d'Impact relative à la Protection des Données (AIPD)* systématique pour tout traitement IA utilisant des

données de santé à grande échelle. L'AIPD doit spécifiquement évaluer les risques de ré-identification, les biais algorithmiques susceptibles de créer des discriminations dans les soins, et les impacts sur l'autonomie décisionnelle des patients.

Les droits des patients face aux systèmes IA médicaux sont également renforcés en 2026. L'article 22 du RGPD interdit les décisions entièrement automatisées produisant des effets juridiques ou significatifs sur les personnes, sauf exceptions. En santé, cela signifie qu'une décision de traitement ne peut être fondée exclusivement sur un algorithme IA sans intervention humaine qualifiée. Les établissements doivent mettre en œuvre des **mécanismes d'explication algorithmique** (*XAI — Explainable AI*) permettant aux soignants et aux patients de comprendre les bases des recommandations IA, et des procédures permettant de contester ces recommandations.

Gouvernance des algorithmes IA dans les établissements de santé

La gouvernance des algorithmes IA en santé constitue un défi organisationnel majeur en 2026. Les établissements les plus avancés ont mis en place des **comités d'éthique algorithmique** réunissant médecins, soignants, représentants des patients, juristes, DSI et experts en IA. Ces comités évaluent chaque nouveau système IA avant déploiement, suivent ses performances en production, et décident des mesures correctives ou de l'arrêt du système en cas de dérive. Cette gouvernance multidisciplinaire n'est pas seulement une bonne pratique : elle est exigée par l'AI Act pour les systèmes à haut risque.

La Haute Autorité de Santé (HAS) a publié un cadre méthodologique d'évaluation des outils IA en santé, articulé autour de quatre dimensions : la performance technique (précision, sensibilité, spécificité), la validité clinique (pertinence pour la pratique médicale réelle), l'utilité clinique (amélioration des outcomes patients), et l'acceptabilité (adoption par les professionnels et les patients). Ce cadre HAS s'impose progressivement comme la référence française pour la validation des systèmes IA médicaux, en complément de la certification CE pour les dispositifs médicaux.

Un **registre interne des systèmes IA** doit être maintenu par tout établissement déployant de l'IA en 2026. Ce registre documente pour chaque système : le fournisseur, la version déployée, les données utilisées, les performances observées en production, les incidents signalés, les mises à jour effectuées et les décisions du comité d'éthique algorithmique. Ce registre constitue la pièce maîtresse lors d'un audit de conformité par la CNIL, l'ANS ou un auditeur HDS accrédité.

Audit de conformité IA santé : méthodologie pratique en cinq phases

L'audit de conformité d'un système IA en contexte de santé suit en 2026 une méthodologie structurée en cinq phases. Notre article sur les agents IA dans l'audit de conformité 2026 décrit comment l'automatisation peut accélérer certaines de ces phases, mais le jugement humain reste indispensable pour l'interprétation des résultats et les décisions de remédiation.

Phase 1 — Cartographie : identifier l'ensemble des systèmes IA déployés ou en cours de déploiement dans l'établissement, les données traitées, les flux entre systèmes, et les responsabilités (fournisseur versus déployeur). Cette cartographie doit couvrir les systèmes IA évidents — aide au diagnostic, prédiction — mais aussi les systèmes moins visibles intégrant du machine learning : gestion des ordonnances, analyse des images médicales, chatbots patients.

Phase 2 — Classification réglementaire : pour chaque système identifié, déterminer son statut au regard de l'AI Act (haut risque, limité, minimal), du MDR (dispositif médical logiciel ou non), et du RGPD (traitement de données de santé ou non). Cette classification conditionne le niveau d'exigences applicable et les contrôles à mettre en place. Utiliser la grille de classification officielle publiée par la Commission européenne en 2025 et les guidelines de l'AI Office.

Phase 3 — Évaluation des contrôles : pour les systèmes à haut risque, vérifier l'existence et l'efficacité de chaque contrôle requis par l'AI Act — documentation technique, système de gestion des risques, tests de robustesse, mécanismes de contrôle humain, logs d'audit. Pour les systèmes utilisant des données de santé, vérifier les bases légales RGPD, les AIPD, les contrats avec les sous-traitants et les mécanismes d'exercice des droits des patients.

Phase 4 — Tests techniques : effectuer des tests de performance sur des données réelles représentatives, des tests de robustesse face aux données adversariales, des évaluations de biais algorithmiques sur des sous-groupes de population (sexe, âge, origine), et des tests de sécurité spécifiques : injection de données corrompues, tentatives d'extraction du modèle, *attaques d'inférence* sur les données d'entraînement. Ces tests requièrent des compétences en *adversarial machine learning* et en sécurité des systèmes IA.

Phase 5 — Plan de remédiation : prioriser les non-conformités identifiées selon leur criticité, définir les actions correctives avec des responsables et des délais, et établir un plan de surveillance continue. Les non-conformités critiques — absence de contrôle humain, pas d'AIPD pour un traitement à haut risque — doivent être traitées avant la mise en production ou immédiatement si le système est déjà déployé.

Environnement de test recommandé pour l'audit IA santé

Pour réaliser les tests techniques de la phase 4 sans exposer de données de patients réels, l'équipe d'audit doit disposer d'un environnement isolé comprenant : des datasets synthétiques représentatifs générés par des outils comme Synthea ou des GAN médicaux, une copie du modèle IA en version de test déployée en sandbox, des outils d'attaque adversariale (Foolbox, ART — Adversarial Robustness Toolbox d'IBM), et des outils d'évaluation des biais (Fairlearn, AIF360). Cet environnement doit lui-même être conforme HDS si des données réelles pseudonymisées y transitent à titre d'exemple.

Architecture technique sécurisée pour l'IA médicale en 2026

L'architecture technique d'un système IA médical conforme en 2026 repose sur plusieurs principes fondamentaux. Le principe de **privacy by design** exige que la protection des données soit intégrée dès la conception du système, et non ajoutée a posteriori. Concrètement, l'entraînement des modèles doit s'effectuer sur des données minimales (principe de minimisation), dans un environnement isolé du système de production, avec des accès strictement contrôlés par des mécanismes de *RBAC (Role-Based Access Control)*.

Le **chiffrement des données** est obligatoire à tous les niveaux en 2026 : données au repos (chiffrement AES-256 des bases de données et des stockages objets contenant les datasets et les logs d'inférence), données en transit (TLS 1.3 minimum pour toutes les communications entre composants), et données en cours d'utilisation. Ce dernier point est particulièrement exigeant : les techniques de *confidential computing* — enclaves sécurisées Intel TDX, AMD SEV-SNP — commencent à être déployées en production pour les traitements IA sur des données de santé ultra-sensibles.

La **traçabilité des inférences** constitue un impératif technique critique en 2026. Chaque recommandation produite par un système IA médical doit être tracée avec : l'identifiant pseudonymisé du patient (jamais le nom en clair dans les logs), l'horodatage précis, la version du modèle utilisée, les features d'entrée pseudonymisées, le score de confiance de la prédiction, et l'identifiant du professionnel de santé qui a consulté la recommandation. Ces logs doivent être stockés de manière intègre — protection contre la modification par WORM storage ou signature cryptographique — et conservés conformément aux durées réglementaires applicables (10 ans minimum pour les données de soin).

Interopérabilité et standards HL7 FHIR avec les systèmes IA

L'interopérabilité est un prérequis technique incontournable pour les systèmes IA en santé. En 2026, le standard **HL7 FHIR R4/R5** (Fast Healthcare Interoperability Resources) s'est imposé comme la référence nationale et européenne pour l'échange de données de santé structurées. L'ANS impose son adoption dans le cadre de l'Espace Numérique de Santé (ENS) et du Dossier Médical Partagé (DMP). Les systèmes IA qui consomment ou produisent des données cliniques doivent être compatibles FHIR pour s'intégrer dans l'écosystème applicatif hospitalier.

Cette contrainte d'interopérabilité a des implications directes sur la conformité IA. Les **modèles de données FHIR** standardisent la représentation des informations cliniques — observations, prescriptions, résultats de biologie, comptes rendus — ce qui facilite la constitution de datasets d'entraînement homogènes et la comparaison des performances entre établissements. En revanche, la standardisation expose aussi à des risques spécifiques : une vulnérabilité dans un

serveur FHIR peut affecter simultanément l'ensemble des applications connectées, y compris les systèmes IA qui en dépendent pour leurs données d'entrée.

La sécurité des API FHIR utilisées par les systèmes IA nécessite une attention particulière. Les authentifications doivent reposer sur des mécanismes robustes (**OAuth 2.0 / SMART on FHIR**), les autorisations doivent être granulaires au niveau de la ressource FHIR, et les accès des modèles IA doivent être audités séparément des accès humains. Les tests de sécurité des API FHIR — fuzzing, injection, escalade de privilèges, attaques SSRF — doivent être intégrés dans le plan d'audit de conformité IA santé.

La cybersécurité des dispositifs médicaux connectés utilisant l'IA

Les **dispositifs médicaux connectés** (DMC) intégrant de l'IA représentent en 2026 la catégorie la plus complexe à sécuriser. Ces dispositifs — moniteurs de surveillance, pompes intelligentes, systèmes d'imagerie avec aide au diagnostic embarquée — combinent les contraintes du Règlement MDR 2017/745, du règlement IVDR pour les dispositifs in vitro, de l'AI Act, et des exigences de cybersécurité du Cyber Resilience Act (CRA) entré en application en 2025. Cette multiplication des référentiels applicables simultanément constitue un défi considérable pour les fabricants et les établissements utilisateurs.

Les attaques ciblant les dispositifs médicaux IA sont en forte augmentation depuis 2023. Les vecteurs d'attaque spécifiques aux systèmes IA médicaux incluent : les *attaques adversariales* visant à tromper les modèles de classification d'images (modifier imperceptiblement un scanner pour obtenir un diagnostic erroné), les *attaques d'empoisonnement* (data poisoning) ciblant les pipelines de ré-entraînement, et les attaques d'extraction de modèle permettant de reconstituer un modèle propriétaire à partir des réponses de l'API d'inférence. Ces vecteurs doivent être explicitement pris en compte dans l'analyse de risques MDR et dans l'AIPD RGPD.

La gestion des mises à jour des modèles IA embarqués dans des dispositifs médicaux est particulièrement contrainte en 2026. Toute modification substantielle du modèle — changement d'architecture, ré-entraînement sur un nouveau dataset — peut constituer une modification significative du dispositif médical au sens du MDR, nécessitant une nouvelle évaluation de

conformité voire une nouvelle certification CE. Les fabricants doivent définir dans leur documentation technique un critère de changement significatif (performance floor, drift threshold) et démontrer que les mises à jour mineures ne franchissent pas ce seuil.

À RETENIR

À retenir — Conformité IA Santé HDS 2026

Triptyque réglementaire : AI Act (haut risque), certification HDS (hébergement), RGPD (données de santé) s'appliquent simultanément et de manière complémentaire en 2026

Contrôle humain obligatoire : l'article 14 de l'AI Act interdit les décisions médicales entièrement automatisées — un professionnel de santé qualifié doit toujours pouvoir intervenir et corriger

AIPD systématique : toute IA traitant des données de santé à grande échelle nécessite une Analyse d'Impact RGPD documentée, actualisée à chaque modification substantielle du modèle

Registre des systèmes IA : chaque établissement doit tenir un registre de tous les systèmes IA déployés, avec traçabilité des versions, performances observées et incidents signalés

Sécurité par conception : privacy by design, chiffrement AES-256/TLS 1.3, RBAC strict, logs d'inférence intègres et pseudonymisés, confidential computing pour les données ultra-sensibles

Interopérabilité HL7 FHIR : prérequis technique pour l'intégration dans l'ENS/DMP — les API FHIR des systèmes IA doivent faire l'objet de tests de sécurité spécifiques

Pénalités 2026 : jusqu'à 30 M€ ou 6 % du CA pour non-conformité AI Act ; jusqu'à 20 M€ ou 4 % du CA mondial pour violation RGPD sur données de santé

Tableau comparatif des exigences réglementaires IA santé 2026

Réglementation	Acteurs concernés	Obligations principales	Sanctions maximales	Autorité de contrôle
AI Act (2024/1689)	Fournisseurs et déployeurs de systèmes IA à haut risque	Documentation technique, gestion des risques, contrôle humain, logs d'audit, enregistrement EU	30 M€ ou 6 % CA mondial	Commission européenne / AI Office
Certification HDS 2026	Hébergeurs de données de santé pour le compte de tiers	ISO 27001/27017, disponibilité, sauvegarde, gestion des incidents, continuité d'activité	Retrait de certification, sanctions ANS	ANS / organismes certificateurs accrédités
RGPD (Art. 9)	Tout responsable de traitement de données de santé	Base légale, AIPD, DPO désigné, droits des personnes, contrats sous-traitants	20 M€ ou 4 % CA mondial	CNIL
MDR (2017/745)	Fabricants de dispositifs médicaux intégrant de l'IA	Marquage CE, évaluation clinique, vigilance post-marché, cybersécurité intégrée	Retrait du marché, poursuites pénales	ANSM / organismes notifiés
Cyber Resilience Act	Fabricants de produits numériques connectés (dont DMC)	Sécurité by design, gestion des vulnérabilités, déclaration de conformité CE	15 M€ ou 2,5 % CA mondial	Autorités de surveillance du marché

Roadmap de mise en conformité IA santé HDS pour 2026

La mise en conformité d'un établissement de santé avec l'ensemble des exigences applicables à ses systèmes IA ne peut s'envisager comme un projet ponctuel : il s'agit d'un programme continu

structuré sur plusieurs trimestres. Pour un établissement hospitalier débutant sa démarche de conformité IA santé HDS 2026, voici la roadmap recommandée sur douze mois :

Trimestre 1 — Inventaire et classification : réaliser la cartographie exhaustive de tous les systèmes IA en usage (y compris les outils SaaS intégrant du ML), classifier chaque système selon l'AI Act et le MDR, identifier les lacunes documentaires les plus critiques et prioriser les risques immédiats

Trimestre 2 — Gouvernance et documentation : constituer le comité d'éthique algorithmique, créer le registre des systèmes IA, initier les AIPD pour les traitements à haut risque, mettre à jour les contrats avec les fournisseurs d'IA pour inclure les clauses AI Act et RGPD renforcées

Trimestre 3 — Contrôles techniques : déployer les mécanismes de logging des inférences, renforcer les contrôles d'accès RBAC, implémenter les tableaux de bord de surveillance des performances des modèles, effectuer les premiers tests de robustesse et d'évaluation des biais sous-groupes

Trimestre 4 — Audit et certification : conduire un audit interne de conformité AI Act, préparer ou renouveler la certification HDS en intégrant les volets IA, soumettre les AIPD complétées à la CNIL si nécessaire, former les équipes cliniques aux procédures de contrôle humain et de signalement des incidents IA

Cette roadmap doit être adaptée au niveau de maturité initial de l'établissement, au nombre et à la criticité des systèmes IA déployés, et aux ressources disponibles. Les établissements disposant d'un RSSI expérimenté et d'un DPO actif seront dans une meilleure position pour accélérer ce programme.

Référentiels recommandés : NIST AI RMF pour la gestion des risques IA, ISO/IEC 42001:2023 pour le système de management de l'IA, PGSSI-S de l'ANS pour la sécurité des systèmes d'information de santé, ANSSI Guide de la sécurité des systèmes IA

Partenaires clés : organismes certificateurs HDS accrédités (Bureau Veritas, AFNOR Certification, BSI), CNIL (accompagnement des acteurs), ANS (référentiels techniques et identité numérique), ANSSI (homologation et guides techniques), GHT pour la mutualisation des ressources

Veille réglementaire continue : abonner les équipes juridiques et techniques aux alertes de l'AI Office de la Commission européenne, aux newsletters CNIL et ANS, et suivre les travaux de normalisation ISO/IEC JTC1/SC42 et CEN/CENELEC pour les standards IA médicale en cours d'élaboration en 2026

FAQ sur la conformité IA santé HDS 2026

Qu'est-ce qu'un système IA à haut risque en santé selon l'AI Act en 2026 ?

Selon l'AI Act européen (Règlement 2024/1689), un système IA est classé à haut risque dans le domaine de la santé lorsqu'il entre dans les catégories listées à l'Annexe III, notamment les systèmes IA intégrés dans des dispositifs médicaux au sens du Règlement MDR 2017/745 — imagerie médicale avec aide au diagnostic, monitoring de patients, systèmes de chirurgie assistée — les systèmes utilisés pour le triage des urgences, et les systèmes de prédiction des risques cliniques. Cette classification entraîne des obligations renforcées : documentation technique exhaustive, système de gestion des risques documenté, logs d'audit des décisions, mécanismes de contrôle humain effectif, et enregistrement dans la base de données européenne. Le Comité européen de l'IA publie régulièrement des orientations pour clarifier les cas limites. En pratique en 2026, tout système IA influençant directement une décision clinique doit être présumé à haut risque jusqu'à preuve du contraire, afin d'éviter tout risque de sanction.

Comment réaliser une AIPD pour un système IA traitant des données de santé ?

Une AIPD pour un système IA de santé doit suivre la méthodologie CNIL et intégrer des éléments spécifiques aux algorithmes de machine learning. Elle doit décrire précisément le système IA (architecture, données d'entrée, type de décision ou recommandation produite), évaluer la nécessité et la proportionnalité du traitement — peut-on atteindre le même objectif avec moins de données ou un modèle plus simple ? — et analyser les risques spécifiques : biais algorithmiques créant des inégalités de soins, ré-identification des patients à partir des données d'entraînement, défaillances du modèle entraînant des erreurs médicales graves, et accès non

autorisés aux données via l'API d'inférence. L'AIPD doit documenter les mesures techniques et organisationnelles mises en place pour maîtriser ces risques, et être mise à jour à chaque modification substantielle du modèle ou des données traitées. Si l'AIPD conclut à un risque résiduel élevé non maîtrisable, une consultation préalable de la CNIL est obligatoire avant tout déploiement en production.

Comment la certification HDS s'articule-t-elle avec les obligations AI Act pour un hébergeur cloud santé ?

Pour un hébergeur de données de santé proposant des services cloud sur lesquels des établissements déploient des systèmes IA, les obligations HDS et AI Act se cumulent sans se substituer l'une à l'autre. La certification HDS couvre l'infrastructure d'hébergement (disponibilité, sécurité physique, sauvegardes, gestion des incidents) mais ne couvre pas les systèmes IA déployés par les clients sur cette infrastructure. L'hébergeur HDS devient co-responsable de traitement ou sous-traitant au sens du RGPD pour les données de santé qu'il héberge, et doit offrir des garanties contractuelles suffisantes au regard de l'article 28 RGPD. Concernant l'AI Act, si l'hébergeur fournit lui-même des services IA — MLOps, plateformes d'entraînement, inférence en tant que service — il peut être qualifié de fournisseur de système IA à haut risque et soumis à toutes les obligations correspondantes. Les contrats cloud santé en 2026 doivent explicitement répartir les responsabilités entre l'hébergeur HDS, les équipes IA du client, et les éditeurs des modèles tiers utilisés. Notre analyse des nouvelles exigences de la certification HDS 2026 détaille les clauses contractuelles recommandées pour ces situations multi-acteurs.

Pourquoi les biais algorithmiques représentent-ils un risque réglementaire majeur en santé ?

Les biais algorithmiques dans les systèmes IA médicaux ne sont pas seulement un enjeu éthique : ils constituent en 2026 un risque réglementaire majeur susceptible d'engager la responsabilité pénale et civile des établissements de santé. L'AI Act impose explicitement l'évaluation des biais dans les systèmes à haut risque. Le RGPD interdit les discriminations fondées sur des données sensibles, dont l'état de santé. La HAS intègre l'évaluation des biais dans son cadre méthodologique pour les outils IA en santé, et l'ANSM exige cette évaluation pour les dispositifs médicaux intégrant de l'IA. Concrètement, un modèle de prédiction de risque cardiaque entraîné

principalement sur des données de patients masculins caucasiens produira des prédictions moins fiables pour des patientes ou des patients d'autres origines ethniques. Si cet outil est déployé en production sans évaluation des biais par sous-groupe de population, l'établissement s'expose à des plaintes de patients, des investigations CNIL, et des contrôles ANSM. La documentation de la remédiation des biais doit figurer dans l'AIPD et dans le registre des systèmes IA, actualisée à chaque ré-entraînement du modèle.

Conclusion

La **conformité IA santé HDS 2026** représente un chantier de transformation organisationnelle et technique majeur pour l'ensemble des acteurs de la santé numérique française. Le triptyque réglementaire AI Act, certification HDS et RGPD impose des standards élevés qui, s'ils peuvent paraître contraignants, constituent en réalité une opportunité de renforcer la confiance des patients et des professionnels de santé dans les technologies IA. Les établissements qui investissent dès maintenant dans leur gouvernance algorithmique, leur architecture de sécurité et leur documentation de conformité se positionnent favorablement pour les audits réglementaires et pour l'adoption pérenne de l'IA dans leurs pratiques cliniques.

Les points de vigilance les plus critiques en 2026 restent l'AIPD systématique pour tout traitement IA sur des données de santé, le maintien d'un contrôle humain effectif sur les décisions cliniques assistées par IA, et la sécurisation des pipelines d'entraînement et d'inférence contre les attaques adversariales spécifiques aux systèmes IA médicaux. Pour approfondir la dimension juridique de ces enjeux, notre article sur les agents IA et l'audit de conformité en 2026 propose des grilles d'évaluation prêtes à l'emploi. L'investissement dans la conformité n'est pas une charge administrative : c'est la condition sine qua non d'un déploiement de l'IA en santé qui soit à la fois éthique, sûr et durable pour tous les acteurs de l'écosystème.

Auditez votre conformité IA santé HDS 2026 dès aujourd'hui

Nos experts certifiés OSCP/CRTO accompagnent les établissements de santé et les hébergeurs HDS dans leur mise en conformité AI Act, RGPD et certification HDS 2026. De l'audit initial à la mise en place de la gouvernance algorithmique, nous couvrons l'ensemble du spectre réglementaire applicable à vos systèmes IA médicaux.

Demander un audit de conformité IA santé