

PÔLE D'EXCELLENCE CYBER

GUIDE OPÉRATIONNEL

Pour l'acquisition et l'exploitation de systèmes d'IA en santé

Novembre 2026

EDiH GREEN POWER IT
EUROPEAN DIGITAL INNOVATION HUB
HAUTS-DE-FRANCE

Cofinancé par l'Union européenne



Présentation de Julien Coisne

Julien est Responsable Secteur Public au CITC EuraRFID, où il pilote la cible acteurs publics du projet européen EDIH GreenPowerIT. Attaché territorial hors classe, fort de plus de 20 ans d'expérience dans la fonction publique territoriale, il accompagne collectivités, EPCI et opérateurs publics dans l'adoption d'une IA de confiance, en les aidant à passer de l'idée au projet. Son action articule stratégie, usages, gouvernance des données, conformité réglementaire et cybersécurité, avec l'objectif de rendre ces enjeux lisibles pour les décideurs publics. Son ambition est de faire de ces technologies (IA, Data, IoT, Cyber) des leviers de transformation au service de la conception et de la mise en œuvre des politiques publiques territoriales.



Présentation de Thomas Kernem-Om

Thomas est Responsable de l'adoption sectorielle de l'IA au sein du Hub France IA. Il pilote et accompagne l'adoption d'une IA de confiance en articulant stratégie, usages, gouvernance, conformité réglementaire, sûreté et cybersécurité. Egalement Responsable de l'IA en Santé et des sujets relatifs à l'IA & Cybersécurité, son parcours combine le pilotage de projets de refonte, d'urbanisation et de digitalisation des systèmes d'information, la gestion d'enjeux IT / OT / Cybersécurité en environnements réglementés (Energie et Santé) ainsi que depuis 2023 au sein du Hub France IA, la participation et contribution à différents projets européens (EDIH CYBIAH, AI Factory France et LLM Bridge) dédiés à l'Intelligence Artificielle et comportant un volet IA en Santé (accompagnement technique et réglementaire de startups sur les aspects Cyber & IA, implication dans l'écosystème Innovation & Financement, etc...).

CONTEXTE

À l'occasion de l'European Cyber Week 2025, les partenaires du Corridor Cyber des EDIH France se sont réunis afin d'échanger sur la place croissante de l'intelligence artificielle dans les établissements de santé et médico-sociaux.

Ces échanges se sont notamment appuyés sur deux analyses conduites respectivement par le Pôle d'Excellence Cyber, membre de l'EDIH Bretagne, et par CYBIAH. Menés auprès d'établissements, ces travaux visaient à mieux comprendre leur niveau de connaissance des outils et fonctionnalités d'intelligence artificielle, les usages déjà présents dans leur environnement numérique ainsi que les mesures de sécurité et de gouvernance mises en place pour les encadrer.

La restitution de ces analyses a fait apparaître un constat partagé : l'intelligence artificielle s'intègre rapidement dans les pratiques et les logiciels métiers, alors que sa présence, son fonctionnement et les risques associés restent encore insuffisamment identifiés. Le niveau de maturité des organisations apparaît hétérogène et les dispositifs existants ne permettent pas toujours de connaître les solutions utilisées, les données auxquelles elles accèdent, les services tiers mobilisés ou les responsabilités des différents acteurs.

Cette situation ne traduit pas une absence d'intérêt ou d'engagement des établissements. Elle révèle surtout la difficulté à appréhender une technologie nouvelle, évolutive et parfois intégrée de manière peu visible aux outils déjà en service. Elle confirme également la nécessité de proposer des repères accessibles et des ressources opérationnelles adaptées aux réalités du terrain.

À l'issue de cette rencontre, quatre chantiers prioritaires ont été définis. Pour les mettre en œuvre, les EDIH des Hauts-de-France, d'Île-de-France et de Bretagne ont constitué, avec d'autres partenaires institutionnels, juridiques, industriels et professionnels, le GT Cyber & IA en Santé.

Deux de ces chantiers ont désormais abouti.

Le premier a consisté à conduire une enquête auprès d'établissements sanitaires et médico-sociaux afin d'évaluer leur capacité à identifier et à maîtriser les usages de l'intelligence artificielle dans leur environnement. Cette démarche a permis de mieux caractériser les pratiques, les niveaux de connaissance et les principaux besoins d'accompagnement.

Le second chantier a porté sur la sécurisation de l'acquisition et de l'exploitation des systèmes d'IA. Il a conduit à l'élaboration d'un clausier destiné à aider les établissements à préciser leurs exigences, à mieux répartir les responsabilités et à encadrer leurs relations avec les fournisseurs tout au long du cycle de vie des solutions.

Les travaux du GT ont ainsi donné naissance à deux livrables complémentaires :

- le livre blanc « **Cyber & IA en Santé — Comprendre les usages, garder la maîtrise, construire la confiance** », qui présente les constats, les enjeux et les retours d'expérience issus du terrain ;
- le présent « **Guide opérationnel pour l'acquisition et l'exploitation de systèmes d'IA en santé** », accompagné de son clausier, qui traduit ces enseignements en questions, points de vigilance et dispositions mobilisables par les établissements.

Ces deux documents poursuivent une même ambition : permettre aux acteurs de santé de bénéficier des apports de l'intelligence artificielle tout en conservant la maîtrise de leurs données, de leurs systèmes, de leurs fournisseurs et de leurs responsabilités.

Ils constituent une première étape d'un travail collectif appelé à se poursuivre. Les deux autres chantiers identifiés lors de l'European Cyber Week 2025 sont toujours en cours et viendront compléter progressivement les ressources proposées aux acteurs de l'écosystème.



MICHAEL BENOIT
Directeur de projet Cybersécurité et RSSI
Pôle d'excellence Cyber – EDIH Bretagne

REPRENDRE LA MAIN SUR L'IA EN SANTÉ : SÉCURISER L'ACHAT PLUTÔT QUE SUBIR LA TECHNOLOGIE

Comment les European Digital Innovation Hubs (EDIH) peuvent aider les établissements de santé à acquérir des solutions d'intelligence artificielle maîtrisées, sûres et conformes. Ce travail est conçu comme un bien commun, appelé à évoluer au rythme du terrain et de la réglementation.

1. L'IA s'invite dans les soins… parfois sans être choisie

En tant qu'EDIH, notre mission est d'accompagner nos partenaires dans leur transformation numérique. Dans la santé, cette mission se confronte à une réalité paradoxale.

D'un côté, l'intelligence artificielle s'immisce progressivement dans les solutions déjà utilisées (mise à jour d'un logiciel métier qui active un assistant, nouvelle brique d'aide à la décision médicale, module de tri ou de prédiction), sans que l'établissement ait pu donner un accord explicite ni cadrer précisément les usages. C'est ce que l'on pourrait appeler une « IA subie » : elle arrive par la porte de la mise à jour plutôt que par celle du choix et du marché public.

De l'autre, les équipes médicales et soignantes expriment une demande forte pour ces outils, porteurs de promesses en matière de dépistage, de gain de temps médical et de suivi plus fin des patients. La question n'est donc pas de savoir s'il faut recourir à l'IA mais comment le faire dans un cadre de confiance clair, stable et compréhensible par tous les acteurs.

2. Acheter de l'IA n'est pas acheter un logiciel comme un autre

Entre l'IA qui s'installe « toute seule » et l'IA que l'on souhaite acheter de manière volontaire, un enjeu majeur apparaît : acquérir une solution d'IA est plus complexe que l'achat d'un logiciel classique.

Les établissements publics de santé produisent et gèrent des données de santé qui constituent un actif stratégique et extrêmement sensible, encadré par un corpus réglementaire dense. Les questions de cybersécurité, de souveraineté et de confidentialité ne sont plus des clauses annexes : elles conditionnent directement la capacité de l'établissement à rester maître de son patrimoine informationnel et à protéger les droits des patients.

Concrètement, il ne suffit plus de décrire des fonctionnalités attendues. Il faut cadrer, dès la définition du besoin et la procédure d'achat, **ce que la solution d'IA pourra faire et ce qu'elle ne pourra pas faire :**

- où et sous quelles conditions les données sont hébergées ;
- qui peut accéder aux données et les réutiliser ;
- à quelles fins et dans quel périmètre ;
- avec quelles garanties de réversibilité ;
- sous quel niveau de supervision humaine et de contrôle clinique ;
- avec quelles protections contre une captation de la valeur par le fournisseur.

C'est à cette condition que l'IA reste un outil au service de la mission de soin et non un vecteur de dépendance ou de perte de maîtrise.

3. Un kit pour sécuriser les achats de solutions d'IA en santé

Pour répondre à ces besoins très concrets, nous avons développé, dans le cadre de nos missions d'EDIH, un kit de renforcement de la sécurisation des achats de solutions d'IA en santé.
Ce kit se compose de deux ressources complémentaires et opérationnelles :

- **Un clausier IA prêt à l'emploi**
  Un ensemble de clauses à intégrer dans les contrats de la commande publique des établissements de santé, couvrant notamment :
  - la souveraineté et la localisation des données ;
  - l'hébergement certifié et les exigences de cybersécurité (NIS2, cyberrésilience) ;
  - la protection des données à caractère personnel ;
  - la réversibilité et la portabilité ;
  - l'encadrement de l'IA générative et des algorithmes prédictifs ;
  - la propriété intellectuelle et la valorisation des résultats.

Chaque exigence est traduite en langage contractuel activable, avec des points de vigilance pour les acheteurs et les DSI.

- **Un guide opérationnel pas à pas**
  Un guide pratique qui accompagne l'acheteur public ou la direction des systèmes d'information tout au long du cycle de vie d'un projet d'IA : qualification du besoin, compréhension du cadre juridique applicable, conduite de la due diligence fournisseur, organisation de la supervision humaine et technique de la solution ainsi que le suivi des incidents et des mises à jour.

L'objectif n'est pas d'ajouter de la complexité mais de donner aux établissements les moyens concrets de reprendre la main : passer d'une IA subie à une IA choisie, documentée et cadrée.

4. Des outils conçus comme des Communs, au rythme des textes européens

Un clausier et un guide ne valent que par leur usage. Pour qu'ils soient réellement utiles, ils doivent être confrontés à la réalité du terrain dans les établissements de santé.

C'est pourquoi ces ressources sont pensées comme des Communs : elles ne sont ni figées ni exhaustives. Elles ont vocation à être régulièrement enrichies par les retours des acheteurs publics et des DSI qui les utiliseront dans leurs marchés, confronteront les clauses aux réponses des fournisseurs et nous indiqueront ce qui fonctionne, ce qui bloque ou ce qui manque.

Elles devront également intégrer les évolutions réglementaires européennes en matière d'IA, de données de santé et de cybersécurité. *Le Digital Omnibus* adopté en 2026 modifie les calendriers d'application de certaines obligations du règlement sur l'IA, en particulier pour les systèmes à haut risque et l'IA embarquée dans les dispositifs médicaux, tout en maintenant l'architecture fondée sur les risques. À cela s'ajoutent l'entrée en vigueur progressive de l'espace européen des données de santé et le renforcement des exigences NIS2 et de la cyberrésilience des systèmes.

Nos ressources seront donc régulièrement mises à jour pour rester justes, utilisables et alignées sur le droit en vigueur.

5. De la clause au dialogue avec les offreurs de solutions

Poser des clauses est nécessaire, mais insuffisant. Un cadre contractuel ne produit ses effets que s'il rencontre une offre capable et désireuse de s'y conformer.

Nous sommes attentifs à deux écueils :

- des exigences trop rigides, mal expliquées qui peuvent conduire à des appels d'offres infructueux faute de candidats en mesure d'y répondre ;
- des clauses ignorées ou systématiquement renégociées à la baisse perdent toute portée.

C'est pourquoi nous souhaitons prolonger ce travail par une démarche de dialogue avec les prestataires. Il s'agit de :

- présenter clairement la logique du clausier et du guide ;
- expliciter les points non négociables (base légale des traitements, hébergement certifié, interdiction de transferts de données hors cadre maîtrisé, obligations liées aux systèmes à haut risque) ;
- écouter les contraintes techniques et économiques des offreurs ;
- identifier ce qui peut être gradué, articulé avec un calendrier ou accompagné d'outils de mise en conformité.

L'ambition est de faire converger l'offre et la demande : donner aux acheteurs un cadre lisible et donner aux fournisseurs de la visibilité sur ce que le secteur public de santé attend d'eux. En tant qu'EDIH, notre position de tiers neutre et d'animateur d'écosystème nous place idéalement pour faciliter ce dialogue, sans nous substituer ni aux établissements ni aux industriels.

6. Une première étape vers une culture commune de l'IA en santé

Nous assumons ces livrables comme une première étape et non comme un aboutissement.
Dans le cadre du projet EDIH 2.0, ils pourront être challengés et enrichis par de nouveaux partenaires spécialistes de la filière santé, comme Eura-santé en Hauts-de-France ou Paris Santé Campus en Île-de-France, dont l'expertise sectorielle permettra de tester la robustesse des outils et d'en élargir la portée.

Au-delà de la seule sécurité des achats, l'enjeu est de contribuer à une culture commune de l'IA en santé, fondée sur des pratiques partagées, des exigences lisibles et des actions collectives cohérentes, plutôt que sur une succession d'initiatives isolées.

SOMMAIRE

CHAPITRE 1. QUEL EST L'ÉTAT DES LIEUX DE L'IA DANS LA SANTÉ ? 14

1. RAPPEL DU CONTEXTE 16

1.1. L'utilisation croissante de l'IA dans les établissements publics de santé 16

1.2. Deux modalités d'intégration des SIA aux enjeux distincts 16

1.3. Un cadre institutionnel national en cours de structuration 16

1.4. Un secteur très exposé aux cybermenaces 17

1.5. Une typologie complexe de données de santé 17

2. RAPPEL DES ENJEUX STRATÉGIQUES 21

2.1. Enjeux de souveraineté et de maîtrise des données de santé 21

2.2. Enjeux opérationnels : supervision humaine et traçabilité des décisions médicales assistées 22

2.3. Enjeux de gouvernance et d'organisation interne 22

2.4. Enjeux économiques et prospectifs 23

3. RAPPEL DES ENJEUX JURIDIQUES 24

3.1. Présentation globale du cadre juridique applicable 24

3.2. L'articulation des textes sur les données de santé et les SIA 27

3.3. Les obligations spécifiques aux établissements publics de santé en qualité d'organismes de droit public 28

3.4. Quels droits des patients sur leurs données ? 28

3.5. Qui est propriétaire des données de santé et quelle est la portabilité des données des patients ? 29

CHAPITRE 2. COMMENT ACHETER UN SYSTÈME D'IA EN SANTÉ SANS PRENDRE DE RISQUES JURIDIQUES OU OPÉRATIONNELS ? 32

1. LES BONNES PRATIQUES À METTRE EN PLACE AVANT L'ACHAT 34

1.1. Anticiper les besoins de l'établissement public de santé 34

1.2. Due diligence du fournisseur 34

1.3. Adapter les documents contractuels de l'établissement public de santé 35

2. COMMENT PARTAGER MES DONNÉES EN TANT QU'ACTEUR PUBLIC DE SANTÉ ? 37

2.1 Cas n° 1 — Partage à des fins de soins (utilisation primaire) 37

2.2 Cas n° 2 — Partage à des fins de recherche ou d'innovation (utilisation secondaire) 37

2.3 Cas n° 3 — Partage avec un fournisseur de SIA dans le cadre d'un contrat 38

2.4 Cas n° 4 — Partage dans le cadre d'un groupement hospitalier de territoire (GHT) 38

3. **LES BONNES PRATIQUES À METTRE EN PLACE PENDANT L'ACHAT** **39**

3.1 Information et conformité réglementaire 39

3.2 Interopérabilité avec le système d'information 39

3.3 Clauses contractuelles spécifiques 39

3.4 Encadrement des données à caractère personnel 40

4. **LES BONNES PRATIQUES À METTRE EN PLACE POUR L'EXPLOITATION DU SIA** **41**

4.1 Gouvernance interne : mettre en place un comité de suivi dédié 41

4.2 Tenir un registre des SIA déployés 41

4.3 Encadrer les mises à jour intégrant des briques d'IA 41

4.4 Assurer une supervision humaine effective 42

4.5 Traçabilité des usages 42

4.6 Gérer les incidents spécifiques à l'IA 42

CHAPITRE 3. POURQUOI LES CONTRATS STANDARDS NE SUFFISENT-ILS PAS FACE AUX SYSTÈMES D'IA EN SANTÉ 44

Pourquoi le clausier IA et santé est-il nécessaire ? 46

Quels enjeux ce clausier traite-t-il ? 46

Comment utiliser ce clausier ? 47

CHAPITRE 4. QUELS SONT LES PRINCIPAUX CONTENTIEUX AUXQUELS SONT CONFRONTÉS LES ÉTABLISSEMENTS DE SANTÉ DANS L'USAGE DU NUMÉRIQUE ? 48

Thème n° 1 - Les grandes bases nationales de données de santé 50

Thème n° 2 - La sécurité des systèmes informatiques et les fuites de données 50

Thème n° 3 - L'hébergement et l'externalisation : le cas du Cloud Act 50

Thème n° 4 - La recherche, l'IA et l'accès aux données 51

Thème n° 5 - Les outils numériques de soin : télémédecine, espace numérique de santé 51

ANNEXES 52

Annexe n° 1 – Frise chronologique de l'entrée en application des principales législations françaises et européennes sur les données 52

Annexe n° 2 – Recommandations à destination des établissements publics de santé (HAS, CNIL et ANSSI) 52

OBJECTIF

Identifier les risques et donner les bonnes pratiques pour acheter ou intégrer des systèmes d'IA (SIA) dans un établissement de santé.

DESTINATAIRES

Les établissements publics de santé (centres hospitaliers, groupements hospitaliers de territoire) et leurs services (directions générales, directions des systèmes d'information, directions des affaires juridiques, directions des achats, délégués à la protection des données, professionnels de santé, etc.)

USAGE

À mobiliser avant un projet d'acquisition ou d'intégration d'un SIA, et tout au long de son cycle de vie.

DOCUMENTS ASSOCIÉS

Ce guide complète :

- Le Clausier IA et Santé qui contient un ensemble de clauses à adapter et insérer dans les contrats des établissements publics de santé
- La note de cadrage qui expose les enjeux juridiques pour les établissements publics de santé.

L'intelligence artificielle s'intègre rapidement dans les hôpitaux : aide au diagnostic, optimisation des parcours patients, assistants conversationnels, modules prédictifs dans les dossiers patients informatisés (DPI).

Selon une enquête de la Fédération hospitalière de France (juillet 2025), 65 % des établissements publics de santé utilisent déjà des technologies d'IA (sur 110 établissements répondants).

Face à cette évolution, les établissements publics de santé doivent maîtriser trois types d'enjeux :

- **Souveraineté :** maîtriser les données de santé, garantir la réversibilité des solutions et ne pas dépendre d'un seul fournisseur ;
- **Juridique :** naviguer dans un corpus dense de textes européens et français qui s'appliquent simultanément ;
- **Opérationnel :** organiser la supervision humaine des SIA et assurer la traçabilité des décisions médicales assistées.

Ce guide recense les enjeux, les réflexes et les bonnes pratiques pour accompagner les établissements de l'achat d'un SIA jusqu'à la fin du contrat.

Il s'appuie sur les référentiels de la Haute Autorité de Santé **(HAS)**, la Commission Nationale de l'Informatique et des Libertés **(CNIL)**, l'Agence du Numérique en Santé **(ANS)** et l'Agence Nationale de la Sécurité des Systèmes d'Information **(ANSSI)**.

Le guide est structuré en quatre chapitres :

- **Chapitre 1 — État des lieux** : contexte de déploiement, modalités d'intégration et enjeux stratégiques et juridiques ;
- **Chapitre 2 — Bonnes pratiques à l'achat** : qualification du besoin, due diligence fournisseur, cahier des charges et sécurisation contractuelle ;
- **Chapitre 3 — Le clausier IA et santé** : pourquoi des clauses spécifiques sont indispensables dans les contrats des établissements publics de santé ;
- **Chapitre 4 — Contentieux** : panorama des litiges auxquels sont confrontés les établissements dans l'usage du numérique et des enjeux juridiques concrets qui en découlent.

CHAPITRE 1

QUEL EST L'ÉTAT DES LIEUX DE L'IA DANS LA SANTÉ ?

01

1. RAPPEL DU CONTEXTE

1.1 L'utilisation croissante de l'IA dans les établissements publics de santé

Les établissements publics de santé intègrent l'IA selon deux modalités principales (détaillées à la section 1.2) : l'achat délibéré d'un SIA dédié (logiciels d'aide au diagnostic, outils de prescription assistée, etc.) et l'intégration progressive de briques d'IA dans des outils existants (mise à jour activant un assistant IA, modules prédictifs dans le DPI, agents conversationnels, etc.).
Ce déploiement répond à des défis bien identifiés : contraintes financières, vieillissement démographique, pénurie de personnel soignant.

En contrepartie, l'IA apporte des avancées concrètes : meilleur dépistage, prédiction d'événements cliniques, aide à l'interprétation des examens, personnalisation du suivi et restitution de temps médical aux soignants.

1.2 Deux modalités d'intégration des SIA aux enjeux distincts

Les établissements de santé intègrent des SIA selon deux modalités aux enjeux distincts :

- **L'acquisition délibérée d'un SIA dédié** : l'établissement achète un logiciel dont la fonction principale est une brique d'IA (détection de nodules pulmonaires, aide à la prescription, génération de comptes rendus, etc.). L'établissement dispose généralement d'informations sur le produit et peut structurer son évaluation en amont.
- **L'intégration progressive de briques d'IA dans des outils existants** : une mise à jour active une fonctionnalité d'IA sur un logiciel déjà déployé (suite bureautique, logiciel de gestion hospitalière, etc.). C'est la situation dite d'« IA subie » : l'établissement n'a pas choisi d'intégrer l'IA. Cette situation soulève les enjeux juridiques et opérationnels les plus importants.

ILLUSTRATION
En août 2025, un CHU de Nancy a recensé 440 000 connexions à des IA génératives personnelles (non validées par l'établissement) effectuées par des agents hospitaliers. Un volume similaire a été mesuré au CHU de Montpellier. Ces usages non maîtrisés (« shadow IT ») exposent les établissements à de sérieux risques : atteinte au secret médical, vulnérabilités du système d'information, violation du RGPD.

1.3 Un cadre institutionnel national en cours de structuration

Face à la diffusion rapide de l'IA dans la santé, les pouvoirs publics ont mis en place une politique nationale coordonnée.

Sur le plan politique, la stratégie « Santé numérique » de France 2030 a investi 500 millions d'euros, dont la moitié sur des projets embarquant de l'IA. La Plateforme des données de santé (Health Data Hub), opérationnelle depuis 2020, soutient 168 projets de recherche dont 40 % environ utilisent des méthodes d'IA. La feuille de route du numérique en santé 2023-2027 structure cette dynamique autour de quatre axes : prévention, prise en charge, accès à la santé et cadre propice.

Sur le plan juridique, la HAS et la CNIL ont formalisé en 2026 un partenariat stratégique, qui s'est traduit

par la publication en février 2026 d'un guide de recommandations conjoint couvrant douze thématiques et l'ensemble du cycle de vie d'un SIA (gouvernance, acquisition, formation, supervision humaine, traçabilité, vigilance, désinstallation). La HAS a également intégré deux nouveaux critères dédiés aux SIA dans le 6e cycle de certification des établissements de santé, applicable depuis septembre 2025.

La stratégie IA de la CNIL pour 2025-2028 s'articule autour de quatre axes :

- comprendre le fonctionnement des SIA et leurs impacts ;
- favoriser le développement d'IA respectueuses de la vie privée ;
- accompagner les acteurs innovants ;
- auditer et contrôler les SIA pour protéger les personnes.

1.4 Un secteur très exposé aux cybermenaces

Les établissements publics de santé sont des cibles privilégiées des cyberattaques. L'intégration d'un SIA élargit la surface d'attaque : tout audit de sécurité doit couvrir les dépendances du SIA (API tierces, sous-traitants du fournisseur). Le plan de continuité d'activités (PCA) doit inclure un scénario d'indisponibilité du SIA et une procédure de mode dégradé pour chaque SIA critique (cf. Chapitre 2, section 3.4).

ILLUSTRATION
Les cyberattaques du Centre Hospitalier Sud Francilien de Corbeil-Essonnes (août 2022), du Centre Hospitalier de Versailles (décembre 2022) et du Centre Hospitalier Universitaire de Rennes (mars 2023) ont démontré les conséquences concrètes d'une compromission du système d'information hospitalier : indisponibilité prolongée des systèmes, perturbation de la prise en charge et transferts d'urgence de patients vers d'autres établissements.

1.5 Une typologie complexe de données de santé

Un établissement public de santé traite quotidiennement de nombreux types de données. Leur qualification juridique détermine les obligations applicables.

1.5.1 Questions à se poser pour qualifier vos données avant tout projet SIA

Avant de lancer un projet d'acquisition ou d'intégration d'un SIA, l'établissement doit savoir précisément quelles données ce système va traiter.
Cette qualification conditionne les obligations contractuelles, les certifications exigées et les droits des patients.
Posez-vous les questions suivantes avant tout projet SIA :

- **Quelle(s) catégorie(s) de données ce SIA va-t-il traiter ?**
  - Données cliniques (imagerie, biologie, comptes rendus, DPI, etc.) : données « sensibles » au sens de l'article 9 du RGPD (protection maximale, certification HDS obligatoire) ;
  - Données administratives (identité, numéro de sécurité sociale, facturation, etc.) : données « ordinaires » au sens de l'article 6 du RGPD (comprenant toutefois un risque de requalification en cas de croisement avec des données cliniques) ;
  - Données issues de dispositifs médicaux connectés (capteurs, oxymètres, glucomètres, etc.) : données sensibles dès qu'elles permettent de tirer une conclusion sur l'état de santé d'une personne ;
  - Données génomiques (séquences ADN, tests prédictifs) : données sensibles, soumises en outre aux lois de bioéthique.

- **Ce SIA va-t-il croiser des catégories de données initialement ordinaires ?**
  Croiser des données ordinaires peut les requalifier en données sensibles (ex. : poids + nombre de pas + facturation). Cette requalification déclenche l'ensemble des obligations liées aux données sensibles : base légale renforcée, certification HDS, etc.

- **Ce SIA génère-t-il des résultats (scores de risque, diagnostics assistés, comptes rendus automatiques) ?**
  Les résultats du SIA (scores de risque, diagnostics assistés, comptes rendus automatiques) sont des données de santé du patient à part entière. Ils doivent être intégrés au dossier médical avec un marquage identifiant leur origine algorithmique (art. L. 4001-3 CSP) et sont accessibles au patient sur demande.

- **Ce SIA entraîne-t-il ou perfectionne-t-il un modèle à partir de nos données ?**
  Les modèles dérivés de l'apprentissage sur vos données représentent un enjeu de propriété intellectuelle et de souveraineté. Sans clause contractuelle, le fournisseur peut revendiquer la pleine propriété des améliorations apportées à son modèle (voir clauses 2.3 et 10.1 du clausier).

- **Nos données seront-elles pseudonymisées ou anonymisées avant tout transfert au fournisseur ?**
  La pseudonymisation (remplacement de l'identifiant par un code) maintient l'applicabilité du RGPD et de la certification HDS. Seule l'anonymisation réelle — difficile à atteindre en pratique hospitalière — permet de sortir du champ du RGPD. La CNIL insiste sur l'obligation d'évaluer rigoureusement le risque résiduel de réidentification avant de qualifier des données d'« anonymes ».

1.5.2 Cartographie des données hospitalières

La distinction entre données sensibles (art. 9 RGPD) et données ordinaires (art. 6) est déterminante pour fixer les exigences contractuelles imposées aux fournisseurs de SIA.

Le tableau ci-dessous présente les principales catégories de données rencontrées en santé, avec leur qualification juridique et leurs principales contraintes.

CATÉGORIE DE DONNÉES	EXEMPLES CONCRETS	QUALIFICATION RGPD	CONTRAINTES SPÉCIFIQUES
Données cliniques	Imagerie médicale (IRM, scanner, radiographies), résultats biologiques, comptes rendus médicaux, DPI, ordonnances, diagnostics	**Données sensibles** (art. 9 RGPD)	– Traitement interdit sauf exceptions légales (soins, santé publique, recherche, etc.) – Base légale : art. 9, § 2, h RGPD. – Certification HDS obligatoire (art. L. 1111-8 CSP)
Données administratives	Numéro de sécurité sociale, identité du patient, données de facturation et d'admission	**Données ordinaires** (art. 6 RGPD)	Point de vigilance sur les croisements de données et le risque de qualification de données à caractère personnel de santé.
Données de dispositifs connectés (IoT médical)	Données de capteurs (tensiomètre, glucomètre, oxymètre connecté)	**Données sensibles** (art. 9 RGPD) dès qu'elles permettent de tirer une conclusion sur l'état de santé d'une personne	– Traitement interdit sauf exceptions légales (soins, santé publique, recherche, etc.) – Base légale : art. 9, § 2, h RGPD. – Certification HDS obligatoire (art. L. 1111-8 CSP) – Droit d'accès de l'établissement aux données générées garanti (art. 4 du Data Act)

Données génomiques	Séquences ADN, données de pharmacogénomique, résultats de tests génétiques prédictifs	**Données sensibles** (art. 9 RGPD)	– Traitement interdit sauf exceptions légales (soins, santé publique, recherche, etc.) – Base légale : art. 9, § 2, h RGPD. – Certification HDS obligatoire (art. L. 1111-8 CSP) – Réglementations sectorielles applicables (lois bioéthique)
Données comportementales	Habitudes de vie, activité physique, observations thérapeutiques, données issues d'applications de santé	– **Données ordinaires** si non liées à un usage médical (art. 6 RGPD) – **Données sensibles** (art. 9 RGPD) si la finalité médicale de l'usage est démontrée	Selon la qualification des données
Données pseudonymisées	Données dont l'identifiant direct est remplacé par un code (clé de réidentification existante dans un fichier distinct)	– **Données à caractère personnel** (art. 4 RGPD) – **Données sensibles** (art. 9 RGPD) si issues de données de santé Attention, le risque de réidentification maintient l'applicabilité du RGPD.	Certification HDS obligatoire (art. L. 1111-8 CSP) tant que la clé de réidentification est accessible
Données générées par un SIA (outputs et modèles dérivés)	Scores de risque algorithmique, diagnostics assistés, comptes rendus automatiques, modèles d'IA entraînés sur les données de l'établissement	Même régime que les **données sources** (données ordinaires ou données sensibles).	Certification HDS obligatoire (art. L. 1111-8 CSP)

1.5.3 La distinction entre données sensibles et données ordinaires

L'article 9 du RGPD soumet les données de santé à un régime renforcé : leur traitement est en principe interdit, sauf exceptions légales strictes. Pour un établissement public de santé, les bases légales les plus souvent applicables sont la nécessité de soins ou de médecine préventive (art. 9, § 2, h RGPD) et, pour les usages secondaires, l'intérêt public en matière de santé publique (art. 9, § 2, i RGPD).

Les données administratives des patients relèvent du régime ordinaire de l'article 6 du RGPD — sauf si elles sont croisées avec des données cliniques, ce croisement pouvant les requalifier en données de santé sensibles.
Cette distinction est essentielle pour calibrer les exigences contractuelles : un outil traitant des données ordinaires n'est pas soumis aux mêmes obligations qu'un outil traitant des données cliniques.

1.5.4 Données pseudonymisées et données anonymisées : une distinction déterminante pour les usages secondaires

La pseudonymisation remplace les identifiants directs (nom, numéro de patient) par un code, tout en conservant une clé de réidentification dans un fichier séparé. Ces données restent des données à caractère personnel au sens du RGPD et, si elles sont issues de données de santé, demeurent soumises à l'article 9 et à l'obligation HDS. Elles ne peuvent donc pas circuler librement pour des usages secondaires.

L'anonymisation supprime définitivement tout lien avec une personne identifiable. Les données ainsi traitées sortent du champ du RGPD et peuvent être réutilisées plus librement. Mais en pratique hospitalière — notamment pour les données génomiques ou d'imagerie — l'anonymisation réelle est difficile à atteindre. La CNIL insiste

sur l'obligation d'évaluer rigoureusement le risque résiduel de réidentification avant de qualifier des données d'« anonymes ».

Pour les usages secondaires (recherche, développement de SIA), la pseudonymisation est le standard minimal exigé par l'EEDS, qui impose en outre le recours à des **environnements sécurisés** d'analyse. L'établissement doit contractualiser avec les fournisseurs de SIA les conditions de pseudonymisation ou d'anonymisation avant tout transfert, et exiger la preuve des techniques employées.

1.5.5 Le sort des données générées par un SIA : un angle mort à encadrer contractuellement

Quand un SIA traite des données de patients, il génère deux catégories de résultats souvent mal encadrés dans les contrats standards :

- **Les résultats directs** (scores de risque, diagnostics assistés, comptes rendus automatiques) : ce sont des données de santé du patient au sens de l'article 9 RGPD, soumis à la certification HDS et au secret médical. Ils doivent être intégrés au dossier médical avec un marquage identifiant leur origine algorithmique (art. L. 4001-3 CSP) et conservés pendant la durée applicable au dossier médical ;
- **Les modèles dérivés** de l'apprentissage continu du SIA sur vos données : sans clause contractuelle explicite, le fournisseur peut revendiquer la pleine propriété des améliorations apportées à son modèle. L'établissement finance ainsi, via ses données patients, l'amélioration d'un outil commercial dont il ne maîtrise ni le fonctionnement ni la valorisation.

Pour prévenir ces risques, le contrat doit impérativement :

- qualifier les outputs du SIA de données de santé des patients soumises à l'art. 9 RGPD ;
- interdire toute réutilisation des données brutes ou des outputs à des fins propres au fournisseur sans accord écrit préalable de l'établissement ;
- préciser à qui appartiennent les modèles dérivés issus de l'apprentissage sur les données de l'établissement (co-propriété ou licence de retour).

Ces enjeux sont traités aux sections 9 et 10 du clausier associé à ce guide.

2. RAPPEL DES ENJEUX STRATÉGIQUES

2.1 Enjeux de souveraineté et de maîtrise des données de santé

Les données sont le carburant des SIA. Leur exploitation par des acteurs privés, parfois établis hors de l'UE, soulève des questions fondamentales de souveraineté. Un établissement qui déploie un SIA confié à un prestataire étranger sans audit des flux ni clause de localisation perd le contrôle effectif de ses données et s'expose à une dépendance technologique structurelle.

Les enjeux de souveraineté s'articulent autour de trois dimensions :

- **Maîtrise des données de santé :** l'établissement est responsable de traitement (art. 4(7) RGPD). Il doit pouvoir démontrer à tout moment que les données de ses patients sont traitées conformément aux finalités définies, par des sous-traitants certifiés HDS, situés dans l'UE. Le Règlement EEDS (n° 2025/327) renforce ces exigences en harmonisant les règles de partage et de réutilisation des données de santé à l'échelle européenne.
- **Réversibilité des SIA :** la dépendance à un fournisseur unique (lock-in technologique) est un risque stratégique et juridique majeur. Sans clause de réversibilité opérationnelle, l'établissement peut être dans l'impossibilité de changer de prestataire ou de récupérer ses données dans un format exploitable — situation incompatible avec le droit à l'effacement (art. 17 RGPD), les obligations de conservation des dossiers médicaux (art. R. 1112-7 CSP) et le Data Act (Règlement n° 2023/2854), qui interdit les obstacles au changement de fournisseur.
- **Indépendance vis-à-vis des fournisseurs** : si le contrat ne précise pas le régime de propriété intellectuelle des modèles développés à partir de vos données, le fournisseur peut en revendiquer la pleine propriété. L'établissement finance ainsi, via ses données, l'amélioration d'un outil dont il ne maîtrise ni le fonctionnement ni la valorisation commerciale.

POINT D'ATTENTION
L'établissement public de santé n'est pas « propriétaire » des données de santé qu'il détient. En **droit français, les données à caractère personnel ne sont pas des biens appropriables.** L'établissement est responsable de traitement au sens de l'article 4(7) du RGPD : il a des obligations de protection, de conservation et de conformité, mais pas un droit d'usage discrétionnaire des données.

Le patient est titulaire de droits fondamentaux inaliénables sur ses données :
- droit d'accès (art. 15 RGPD et art. L. 1111-7 CSP) ;
- droit de rectification (art. 16 RGPD) ;
- droit à la portabilité (art. 20 RGPD) ;
- droit d'opposition à certains traitements (art. 21 RGPD) ;
- sous conditions, droit à l'effacement (art. 17 RGPD) qui est limité par les obligations légales de conservation du dossier médical posées par l'article R. 1112-7 du CSP (20 ans à compter de la dernière prise en charge).

ILLUSTRATION
Un éditeur français de logiciel d'aide au diagnostic peut utiliser un modèle d'IA de base fourni par un acteur américain ou asiatique, dont les données transitent par des serveurs non certifiés HDS. Sans audit préalable des dépendances, l'établissement ignore ce flux transfrontalier, en violation des exigences HDS et de localisation des données dans l'UE.

2.2 Enjeux opérationnels : supervision humaine et traçabilité des décisions médicales assistées

Un SIA peut occuper différents rôles selon sa fonction :

- **supplétif** : il assiste le professionnel de santé ;
- **substitutif** : il remplace une tâche sans valeur médicale ajoutée ;
- **palliatif** : il comble une absence de prise en charge.

Quel que soit ce rôle, la responsabilité du professionnel de santé reste entière : aucun régime spécifique de responsabilité pour les utilisateurs de SIA n'existe à ce jour. Le professionnel répond de l'usage qu'il fait de l'IA et du degré d'autonomie qu'il lui accorde. Les modalités de supervision humaine et de traçabilité sont détaillées au Chapitre 2, sections 3.4 et 3.5.

Les enjeux de supervision humaine se traduisent concrètement par :

- La nécessité de définir des protocoles internes précisant les modalités de contrôle humain pour chaque SIA, adaptés au niveau de risque clinique : supervision totale pour les décisions à fort impact, supervision allégée pour les situations à risque réduit.
- L'obligation de traçabilité : les résultats du SIA intégrés au DPI doivent être conservés pendant la durée du dossier médical (art. R. 1112-7 CSP) avec un marquage identifiant leur source. La décision du professionnel — y compris lorsqu'il s'écarte des recommandations du SIA — doit également être documentée.
- La nécessité d'anticiper les procédures de mode dégradé : un SIA intégré dans les flux cliniques courants crée un risque de rupture de prise en charge en cas d'indisponibilité. Chaque SIA critique doit être classé selon sa criticité clinique et faire l'objet d'une procédure de mode dégradé formalisée, testée et intégrée dans le PCA (cf. Chapitre 2, section 3.4).

2.3 Enjeux de gouvernance et d'organisation interne

Un déploiement maîtrisé des SIA exige une gouvernance institutionnelle structurée, adaptée à la taille et aux ressources de chaque établissement. Les modalités concrètes (composition du comité pluridisciplinaire, rôle du référent IA, fonctionnement du comité de suivi) sont détaillées au Chapitre 2, section 3.1.

Cette gouvernance repose sur quatre piliers opérationnels :

- **Une cartographie dynamique des SIA déployés** : recenser tous les SIA utilisés (acquis délibérément ou intégrés progressivement), avec leur qualification réglementaire, leur niveau de risque au sens du RIA, les catégories de données traitées, le référent interne et les modalités de suivi. Ce registre, mis à jour au moins annuellement, est détaillé au Chapitre 2, section 3.2.
- **Un guichet unique de gestion des projets innovants** : centraliser toutes les propositions de projets IA (à l'échelle de l'établissement ou du GHT) pour assurer une validation institutionnelle préalable, maîtriser le déploiement et alimenter la cartographie.
- **Un circuit de signalement des incidents spécifique aux SIA** : permettre aux professionnels de santé de signaler tout dysfonctionnement, résultat inattendu ou suspicion d'attaque, articulé avec les circuits de vigilance existants (matériovigilance, réactovigilance) et les obligations de notification à la CNIL (art. 33 RGPD), à l'ANSSI (directive NIS2) et aux autorités compétentes au titre du RIA (art. 26, § 5).
- **Une mutualisation à l'échelle des GHT** : les GHT sont invités à harmoniser leurs pratiques et à partager expertises et outils pour accompagner les établissements les moins dotés (cf. Chapitre 2, sections 1.2.1 et 3.1).

RÉFLEXE PRATIQUE
Un établissement sans registre des SIA déployés se trouve, lors d'un contrôle de la CNIL ou d'un incident de sécurité, dans l'impossibilité de prouver qu'il maîtrise ses traitements de données. L'absence de cartographie constitue en elle-même une violation du principe d'accountability (art. 5, § 2, RGPD).

2.4 Enjeux économiques et prospectifs

Les données de santé à caractère personnel ne peuvent pas être monétisées directement : leur traitement est en principe interdit par l'article 9 du RGPD. Des formes de valorisation restent néanmoins possibles, non par vente directe, mais par échange et partage régulés. Le Règlement EEDS crée un système d'accès structuré aux données via des organismes habilités et des conditions strictes d'utilisation, notamment pour l'innovation et le développement d'algorithmes.

Le Règlement (UE) n° 2025/327 relatif à l'EEDS confirme que la donnée de santé est une **ressource régulée** — son accès n'est pas librement ouvert —, organisée pour concilier innovation et protection des droits fondamentaux.

3. RAPPEL DES ENJEUX JURIDIQUES

L'exploitation d'un SIA par un établissement public de santé est encadrée par un corpus juridique dense, composé de textes européens et nationaux qui se superposent et se complètent. Connaître ce paysage juridique est indispensable pour identifier les obligations applicables à chaque étape du cycle de vie : acquisition, déploiement, exploitation, fin de contrat.
Une frise chronologique des principales législations françaises et européennes figure en Annexe 1.

POINT D'ATTENTION
Les obligations des établissements publics de santé vont bientôt évoluer avec deux *Omnibus* européens en cours de négociation : le premier sur l'IA a fait l'objet d'un accord en mai 2026 (en attente de confirmation par le législateur européen) ; le second est toujours en négociation.

3.1 Présentation globale du cadre juridique applicable

3.1.1 Les règles applicables aux données de santé

3.1.1.1 Les règles européennes

3.1.1.1.1 Le RGPD

Le RGPD définit les « données concernant la santé » largement. Selon la CNIL, elles couvrent trois catégories :

- données de santé par nature (antécédents médicaux, maladies, etc.) ;
- données devenant de santé par croisement avec d'autres sources (ex. : poids + nombre de pas), permettant de tirer une conclusion sur l'état de santé d'une personne ;
- données devenant de santé en raison de leur utilisation à des fins médicales.

Les données de santé sont une catégorie particulière soumise à des règles plus strictes (art. 9 RGPD). Leur traitement est en principe interdit, sauf exceptions légales. Pour un établissement de santé, la base légale principale est la nécessité de soins ou de médecine préventive (art. 9, § 2, h RGPD).

Concrètement, l'établissement doit : informer les patients sur l'utilisation de leurs données, leur garantir l'accès à ces données et le droit de rectification, et désigner un délégué à la protection des données (DPO).

POINT D'ATTENTION
Les données collectées pour les soins peuvent être utilisées à d'autres fins (recherche, pilotage des politiques de santé, développement d'algorithmes), **mais** uniquement à condition de fonder ce traitement sur **une base légale autonome et distincte de la collecte initiale**. C'est ce que le Règlement EEDS appelle l'« utilisation secondaire ».

Les bases légales mobilisables sont :
- dans certains cas, le consentement explicite du patient (art. 9, § 2, a RGPD) ;
- l'intérêt public en matière de santé publique (art. 9, § 2, i RGPD) ;
- la recherche scientifique ou médicale (art. 9, § 2, j RGPD).

3.1.1.1.2 L'EEDS

L'EEDS retient une **définition extensive des données de santé.** Il s'applique :

- aux données à caractère personnel (dossiers médicaux électroniques, données de soins, données génétiques, etc.) ;
- aux données à caractère non personnel (données administratives de santé, données anonymisées, etc.).

Son objectif est de faciliter la circulation des données de santé selon deux modalités :

- **L'utilisation « primaire »** correspond à l'utilisation des données pour les soins (prescriptions médicales, etc.). L'établissement doit permettre aux patients d'accéder à leurs données de santé de manière immédiate, gratuite et en format électronique. Avec le consentement du patient, les professionnels de santé de l'UE pourront accéder aux dossiers médicaux pour assurer la continuité des soins transfrontaliers.
- **L'utilisation « secondaire »** désigne l'utilisation des données à des fins d'intérêt général (recherche, statistiques, politique de santé publique). Les établissements de santé sont soumis à des obligations de mise à disposition de leurs données à cet effet.

3.1.1.1.3 Le Data Act

Le Data Act régit l'accès et le partage des **données des objets connectés**. Il concerne les établissements de deux manières :

- En tant qu'**utilisateurs de dispositifs médicaux connectés** (capteurs, moniteurs de patient, implants connectés, etc.) : ils ont le droit d'accéder aux données générées par ces équipements gratuitement, de manière sécurisée et dans un format réutilisable ; et ils peuvent exiger que ces données soient partagées avec un tiers de leur choix (application de santé, professionnel, prestataire d'analyse, etc.).
- En tant qu'utilisateurs de **services Cloud pour l'hébergement des données de santé** : ils bénéficient des obligations imposées aux fournisseurs Cloud :
  - réversibilité du contrat (possibilité de changer de fournisseur sans obstacle contractuel) ;
  - suppression progressive des frais de sortie d'ici au 12 janvier 2027 ;
  - portabilité des données dans un format lisible.

3.1.1.2 Les règles françaises

Le Code de la santé publique (CSP) prévoit trois obligations particulières pour les données de santé :

- **Secret médical** (art. L. 1110-4 CSP) : toute donnée patient est confidentielle par nature, y compris lorsqu'elle est traitée par un algorithme ;
- **Hébergement certifié HDS** (art. L. 1111-8 CSP) : tout traitement de données de santé à caractère personnel doit être confié à un hébergeur titulaire de la certification HDS. C'est une condition obligatoire pour tout SIA exploitant des données de patients ;
- **Recherche impliquant la personne humaine** (art. L. 1121-1 CSP) : les projets d'IA à visée de recherche médicale sont soumis à l'avis du Comité de protection des personnes et, le cas échéant, à l'autorisation de l'ANSM.

Deux initiatives législatives françaises complètent ce cadre :

- Le Système **national des données de santé (SNDS)** (art. L. 1461-1 CSP ; loi n° 2016-41 du 26 janv. 2016) :

regroupe les grandes bases publiques (Assurance maladie, hôpitaux, causes de décès, etc.). Son accès est conditionné à l'autorisation de la CNIL et à l'avis du comité éthique et scientifique compétent.
- **La Plateforme des données de santé** (GIP créé par la loi n° 2019-774 du 24 juil. 2019) facilite l'accès au SNDS pour les projets de recherche et d'IA, sous contrôle de la CNIL et du Conseil d'État.

3.1.2 Les règles applicables à l'IA

3.1.2.1 La définition du système d'IA (SIA)

Le RIA définit un SIA comme un système automatisé qui fonctionne avec une certaine autonomie et peut s'adapter après son déploiement. À partir des entrées qu'il reçoit, il déduit comment générer des sorties — prédictions, contenus, recommandations, décisions — pouvant influencer les environnements physiques ou virtuels.

En pratique, cette définition couvre notamment :

- les algorithmes d'aide au diagnostic ou à la décision médicale (détection de fractures, dépistage sur imagerie, aide à la prescription, etc.) ;
- les systèmes d'IA générative utilisés pour la rédaction de comptes rendus médicaux ou le résumé de dossiers patients ;
- les dispositifs médicaux intégrant de l'IA : robots chirurgicaux, analyseurs automatisés de biologie, etc.

3.1.2.2 La classification des SIA

Le RIA classe les SIA selon leur niveau de risque et attribue à chaque catégorie des exigences spécifiques.
Il distingue quatre niveaux de risque :

- **Risque inacceptable** : SIA portant atteinte aux droits fondamentaux (notation sociale, exploitation de vulnérabilités, techniques subliminales) — interdits depuis le 2 février 2025.
- **Haut risque** : SIA susceptibles de porter atteinte à la santé, à la sécurité ou aux droits fondamentaux. Ils sont soumis à des exigences renforcées et à un marquage CE. Entrent dans cette catégorie : les dispositifs médicaux intégrant de l'IA, les systèmes de tri aux urgences, les outils d'évaluation de l'éligibilité aux prestations de santé.
- **Risque limité** : SIA interagissant directement avec des personnes (chatbots, assistants de rédaction de comptes rendus génératifs). Obligation de transparence : l'utilisateur doit être informé qu'il interagit avec un SIA.
- **Risque minimal** : la grande majorité des SIA actuellement utilisés dans l'UE. Aucune obligation spécifique prévue par le RIA.

POINT D'ATTENTION
Les SIA à finalité médicale sont souvent qualifiés de « dispositif médical » (DM) ou « dispositif médical de diagnostic in vitro » (DMDIV) au sens des Règlements (UE) n° 2017/745 et 2017/746, et relèvent à ce titre de la catégorie des SIA à haut risque (annexe III du RIA), avec l'application d'un ensemble d'obligations renforcées.

3.1.2.3 Les obligations de conformité du fournisseur et déployeur du SIA

Le RIA impose des exigences de conformité au fournisseur et au déployeur du SIA, dont les rôles et responsabilités diffèrent.
Le fournisseur du SIA est la personne physique ou morale qui développe ou fait développer le SIA en vue de sa

commercialisation (art. 3 RIA).
Ses principales obligations sont de :

- concevoir et tester le SIA pour satisfaire aux exigences de sa catégorie de risque ;
- établir la documentation technique requise et, pour les SIA à haut risque, réaliser une évaluation de conformité avant mise sur le marché ;
- apposer le marquage CE pour les SIA à haut risque et enregistrer le système dans la base de données de l'UE ;
- mettre en place un système de surveillance post-commercialisation et signaler tout incident grave aux autorités de surveillance.

Le déployeur du SIA est la personne physique ou morale qui utilise un SIA sous sa propre autorité dans un contexte professionnel (art. 3 RIA).
Ses principales obligations sont de :

- utiliser le SIA conformément aux instructions du fournisseur et veiller à ce que les données d'entrée soient pertinentes ;
- désigner un référent IA interne et s'assurer que les personnes chargées du contrôle humain ont les compétences nécessaires (art. 26, § 4 RIA) ;
- réaliser une analyse d'impact sur les droits fondamentaux (AIDF) en tant qu'organisme de droit public déployant un SIA à haut risque (art. 27 RIA) ;
- tenir un registre des SIA déployés, surveiller leur fonctionnement et signaler tout incident grave au fournisseur et à l'autorité de surveillance.

POINT D'ATTENTION
Dans la grande majorité des cas, l'établissement public de santé est considéré comme le déployeur du SIA au sens du RIA.

3.2 L'articulation des textes sur les données de santé et les SIA

Les règles sur les données et l'IA s'appliquent de manière cumulative. Un même SIA déployé par un établissement de santé peut ainsi relever simultanément du RGPD (données de santé à caractère personnel), du RIA (système d'IA), des règlements DM et DMDIV (finalité médicale), du CSP (HDS et information du patient) et, à partir de 2027, du Règlement EEDS (interopérabilité des données).

- **Articulation RGPD / Règlement EEDS :**
  - pour l'utilisation primaire des données de santé prévue par le Règlement EEDS, le RGPD s'applique pleinement et les droits des patients sont même renforcés ;
  - pour l'utilisation secondaire (recherche, développement de SIA, etc.), le Règlement EEDS aménage certaines dispositions du RGPD, tout en imposant le recours à des technologies de protection des données (pseudonymisation, anonymisation, etc.).
- **Articulation RGPD / Data Act :** en cas de contradiction portant sur des données à caractère personnel, le RGPD prévaut (art. 1, § 5, Data Act). Le Data Act ne crée pas de nouvelle base légale : il étend les droits d'accès et de partage des données issues des objets connectés, en complément du RGPD.
- **Articulation RIA / DM et DMDIV :** les dispositifs médicaux intégrant de l'IA sont soumis au double régime du RIA et des règlements DM et DMDIV. Les obligations du fournisseur au titre du RIA s'ajoutent à celles prévues par les règlements DM et DMDIV et ne s'y substituent pas.

3.3 Les obligations spécifiques aux établissements publics de santé en qualité d'organismes de droit public

Le statut d'organisme de droit public confère aux établissements publics de santé des obligations renforcées par rapport aux déployeurs privés :

- **AIDF** : l'article 27 du RIA impose aux organismes de droit public déployant un SIA à haut risque de réaliser, avant tout déploiement, une analyse d'impact sur les droits fondamentaux (AIDF). Cette obligation s'ajoute à l'AIPD prévue par le RGPD.
- **Information renforcée du patient** : l'article L. 4001-3 du CSP oblige les professionnels de santé utilisant un traitement algorithmique à en informer le patient et à lui communiquer l'interprétation qui en résulte.
- **Hébergement certifié HDS** : toute donnée de santé collectée dans le cadre de la prévention, du diagnostic ou des soins doit être hébergée par un prestataire certifié HDS (art. L. 1111-8 CSP). Cette obligation s'étend aux sous-traitants du fournisseur de SIA pour l'inférence, le stockage ou le traitement des données, même si ceux-ci ne sont pas mentionnés dans le contrat principal.
- **Responsabilité administrative du service public hospitalier** : la responsabilité de l'établissement est engagée en cas de faute de service (art. L. 1142-1 CSP). Utiliser un SIA sans qualification juridique préalable, sans supervision humaine formalisée ou sans procédure de mode dégradé documentée peut constituer une faute d'organisation.

ILLUSTRATION
Un établissement public de santé qui déploie un SIA d'aide au diagnostic par imagerie (détection de fractures aux urgences, contourage en radiothérapie, etc.) doit notamment :

- vérifier que le système dispose d'un marquage CE valide (Règlements DM/DMDIV) ;
- qualifier le niveau de risque du SIA et, si haut risque, réaliser une AIDF (art. 27 RIA) ;
- s'assurer que le fournisseur est qualifié sous-traitant au sens du RGPD et qu'il héberge les données sur un serveur certifié HDS ;
- informer le patient de l'utilisation de l'outil algorithmique (art. L. 4001-3 CSP) ;
- mettre en place un contrôle humain effectif (art. 14 RIA).

3.4 Quels droits des patients sur leurs données ?

En droit français et européen, le patient ne dispose pas d'un droit de propriété au sens civil sur ses données de santé : les données à caractère personnel ne sont pas des biens appropriables.

L'établissement en est le responsable de traitement (art. 4(7) RGPD). Cette absence de propriété au sens strict n'exclut pas des droits fondamentaux inaliénables : droit d'accès (art. 15 RGPD et art. L. 1111-7 CSP), droit de rectification (art. 16 RGPD), droit à la portabilité (art. 20 RGPD), droit d'opposition (art. 21 RGPD) et droit à l'effacement (art. 17 RGPD), sous réserve des obligations de conservation du dossier médical (art. R. 1112-7 CSP : 20 ans à compter de la dernière prise en charge).

En pratique, le dispositif « Mon espace santé » est le principal vecteur de portabilité des données vers le patient, et le Règlement EEDS généralisera ce droit à l'échelle européenne. Lorsqu'un SIA est utilisé dans la prise en charge, l'établissement doit en informer le patient (art. L. 4001-3 CSP). Les résultats générés par l'algorithme (scores de risque, diagnostics assistés, comptes rendus automatiques) sont des données de santé du patient à part entière, accessibles sur demande, et ne peuvent pas être réutilisés à des fins commerciales ou d'entraînement de modèles sans base légale explicite et information préalable de l'intéressé.

3.5 Qui est propriétaire des données de santé et quelle est la portabilité des données des patients ?

La propriété et la portabilité des données sont au cœur de la relation entre le patient, l'établissement et les fournisseurs de SIA.
Voici les réponses aux principales questions des acheteurs sur le sujet.

3.5.1 Q1. L'établissement public de santé est-il propriétaire des données de ses patients ?

Non.
En droit français, les données à caractère personnel ne sont pas des biens appropriables : aucun texte ne confère à l'établissement un droit de propriété sur les informations médicales de ses patients.
L'établissement est responsable de traitement au sens de l'article 4(7) RGPD : il peut utiliser les données pour les finalités pour lesquelles elles ont été collectées (soins, gestion administrative), mais pas en disposer librement.
Néanmoins, le clausier prévoit une clause de maîtrise de l'établissement sur l'ensemble des données, afin de le protéger contre le risque de réappropriation par des entreprises privées.

3.5.2 Q2. Le fournisseur de SIA peut-il utiliser nos données pour améliorer son modèle commercial ?

Non, sauf autorisation écrite expresse et préalable de l'établissement. Cette interdiction doit figurer explicitement dans le contrat (voir clause 2.2 du clausier).
Sans clause adéquate, l'établissement risque de financer, via les données de ses patients, l'amélioration d'un outil commercial dont il ne maîtrise ni le fonctionnement ni la valorisation.

3.5.3 Q3. L'établissement peut-il valoriser ses données, par exemple pour la recherche ou l'innovation ?

Les données de santé à caractère personnel ne peuvent pas être monétisées directement (art. 9 RGPD).
Des formes de valorisation restent néanmoins possibles telles que l'échange et partage régulés dans le cadre de l'EEDS (via des organismes habilités, avec des conditions strictes), ou mise à disposition à des fins de recherche publique sous contrôle de la CNIL.
L'établissement peut également négocier contractuellement un droit de retour sur les modèles entraînés à partir de ses données (voir clause 10.1 du clausier).

3.5.4 Q4. Le patient est-il propriétaire de ses données de santé ?

Non au sens du droit civil, mais le patient dispose de **droits fondamentaux inaliénables** que l'établissement doit garantir en permanence :

- **Droit d'accès** : le patient peut obtenir l'ensemble de son dossier médical, y compris les outputs du SIA (diagnostics assistés, comptes rendus automatiques) — art. 15 RGPD et art. L. 1111-7 CSP ;
- **Droit de rectification** : il peut demander la correction de données inexactes — art. 16 RGPD ;
- **Droit à la portabilité** : il peut recevoir ses données dans un format structuré et lisible et les transmettre à tout professionnel de santé de son choix — art. 20 RGPD (voir Q5) ;
- **Droit d'opposition** : il peut s'opposer à certains traitements, notamment à des fins de recherche — art. 21 RGPD ;

- **Droit à l'effacement** : sous réserve des obligations de conservation du dossier médical (20 ans à compter de la dernière prise en charge — art. R. 1112-7 CSP), le patient peut demander la suppression de ses données — art. 17 RGPD.

3.5.5 Q5. Qu'est-ce que la portabilité des données des patients et qui peut y avoir recours ?

La portabilité permet au patient de récupérer ses données de santé dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre professionnel de santé ou à une application de santé de son choix (art. 20 RGPD).

Ce droit s'applique aux données fournies par le patient et à celles résultant de son activité, y compris les outputs d'un SIA intégré dans sa prise en charge.
L'établissement peut également, avec le consentement du patient, partager ses données avec d'autres professionnels de santé de l'UE dans le cadre de la continuité des soins transfrontaliers.

3.5.6 Q6. Quels formats techniques garantissent la portabilité ?

En pratique, « Mon espace santé » est le principal vecteur de portabilité vers le patient. Les standards techniques applicables sont :

- **HL7 FHIR** : standard socle pour les échanges de données cliniques structurées (résumés patients, prescriptions, comptes rendus) — format cible du Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS) publié par l'ANS ;
- **DICOM :** standard pour l'échange et la gestion des images médicales ;
- **EHRxF** (European Health Record exchange Format) : format européen d'échange des dossiers de santé électroniques, dont les spécifications seront produites en FHIR et dont la conformité sera exigée dans le cadre du Règlement EEDS.

Le cahier des charges doit exiger du fournisseur la prise en charge de ces standards et interdire tout format propriétaire ou toute mesure entravant la portabilité effective des données (art. L. 1470-5 CSP).

3.5.7 Q7. La portabilité s'applique-t-elle aux résultats générés par un SIA ?

Oui.
Les résultats du SIA (diagnostics assistés, comptes rendus automatiques, notamment) sont des données de santé du patient à part entière.
Ils doivent être intégrés au dossier médical avec un marquage identifiant leur origine algorithmique (art. L. 4001-3 CSP), et sont soumis aux mêmes droits d'accès et de portabilité que les données cliniques classiques.

3.5.8 Q8. À quel horizon le Règlement EEDS renforcera-t-il ces droits ?

Le Règlement (UE) n° 2025/327 relatif à l'EEDS généralisera le droit d'accès et de portabilité à l'échelle de l'UE.
Avec le consentement du patient, les professionnels de santé européens pourront accéder aux dossiers médicaux pour assurer la continuité des soins transfrontaliers.

Les établissements seront soumis à des obligations de mise à disposition des données en format interopérable.
Le calendrier d'entrée en vigueur est à suivre attentivement (voir frise chronologique, Annexe 1).

CHAPITRE 2

COMMENT ACHETER UN SYSTÈME D'IA EN SANTÉ SANS PRENDRE DE RISQUES JURIDIQUES OU OPÉRATIONNELS ?

1. LES BONNES PRATIQUES À METTRE EN PLACE AVANT L'ACHAT

1.1 Anticiper les besoins de l'établissement public de santé

1.1.1 Qualification du besoin et du SIA

La qualification du besoin est la première étape structurante de tout projet d'acquisition. Elle conditionne l'ensemble des choix ultérieurs : rédaction du cahier des charges, sélection du fournisseur, obligations de conformité.

Un besoin mal qualifié expose l'établissement à acquérir un système inadapté à son contexte clinique, à être requalifié en fournisseur au sens du RIA ou à méconnaître ses obligations juridiques.

POINT D'ATTENTION
Avant toute acquisition d'un SIA, posez-vous les questions suivantes :
- Ce système a-t-il été conçu et validé pour mon contexte spécifique (type de patients, équipement technique, flux de données, etc.) ?
- Si je l'utilise dans un contexte différent de sa destination initiale, suis-je requalifié en fournisseur au sens du RIA ? Si oui, quelles obligations de conformité en découlent ?
- Qui, en interne, est chargé de valider cette qualification avant la consultation des fournisseurs ?

1.2 Due diligence du fournisseur

La due diligence vise à évaluer la capacité du fournisseur à respecter les exigences réglementaires et contractuelles avant la signature du contrat. L'établissement doit effectuer plusieurs vérifications avant d'attribuer le marché.

1.2.1 Vérifications formelles préalables obligatoires

L'établissement doit exiger que le fournisseur communique :

- la preuve de la certification HDS de l'hébergeur pour les données de santé (la qualification SecNumCloud est recommandée pour les données de niveau de sensibilité critique) ;
- la déclaration du niveau de risque du SIA au sens du RIA, accompagnée de la documentation technique (notice d'utilisation, rapport de tests) ;
- le certificat de marquage CE en tant que DM ou DMDIV, le cas échéant ;
- la politique de sécurité des systèmes d'information (PSSI) et les résultats d'audits de sécurité récents (tests d'intrusion, audits de code) ;
- la liste exhaustive des sous-traitants et leur localisation, avec vérification de l'absence d'accès depuis des pays soumis à des législations extraterritoriales (Cloud Act, FISA, etc.) ;
- la documentation relative à la base légale retenue pour le traitement des données de santé et la preuve de la réalisation d'une AIPD.

1.2.2 Évaluation de la maturité IA responsable

Au-delà des vérifications formelles, l'établissement doit évaluer la capacité du fournisseur à : documenter le fonctionnement de son SIA (transparence, explicabilité), détecter et prévenir les biais, intégrer des mécanismes de supervision humaine, assurer une veille réglementaire et disposer d'une gouvernance interne dédiée à l'IA.

1.3 Adapter les documents contractuels de l'établissement public de santé

1.3.1 Adapter le sourcing dans l'achat public

Les achats de SIA sont des achats stratégiques : marché concentré, enjeux financiers et juridiques élevés. Conformément à l'article R. 2111-1 du Code de la commande publique, l'établissement doit organiser un sourcing formalisé en amont de toute consultation, en conduisant des entretiens approfondis avec un panel représentatif de fournisseurs (en présentiel ou en visioconférence, sur une durée de trois à six mois minimum).

Tous les échanges doivent être tracés par comptes rendus écrits, et l'analyse doit couvrir systématiquement :

- le coût global (acquisition, intégration, maintenance, fin de marché) ;
- la propriété intellectuelle sur les modèles et les conditions de réversibilité ;
- la souveraineté numérique (hébergement HDS, absence de dépendance extra-européenne).

Pour identifier des solutions éprouvées, l'établissement peut mobiliser la plateforme de l'ANAP (ia.anap.fr), le portail APProch (Direction des achats de l'État) et les publications d'Interop'Santé pour vérifier la conformité aux standards d'interopérabilité. Le parangonnage — échanges avec des établissements ayant déjà déployé des solutions comparables — est recommandé pour affiner la stratégie contractuelle.
Les GHT sont invités à mutualiser leur sourcing via des marchés portés par l'établissement support ou une plateforme régionale d'achat : partage des comptes rendus, harmonisation des questionnaires fournisseurs, levier tarifaire par agrégation des volumes. Cette mutualisation s'inscrit dans la gouvernance partagée à l'échelle des GHT (cf. Chapitre 1, section 2.3 et Chapitre 2, section 3.1).

Pour un achat stratégique comme un SIA en santé, le rétroplanning doit prévoir au minimum un an, pour permettre si nécessaire une phase de sourcing complémentaire.

1.3.2 Élaborer un cahier des charges conforme aux exigences réglementaires

L'établissement doit intégrer dans son cahier des charges les exigences suivantes :

- **Transparence et documentation** : information claire sur la destination d'usage du SIA, ses données d'entraînement, ses performances (sensibilité, spécificité, robustesse), ses biais connus, les populations éligibles et celles pour lesquelles le système n'est pas validé, le principe de fonctionnement, les dispositions de contrôle humain et l'impact environnemental ;
- **Répartition des responsabilités** : qualification explicite des rôles (sous-traitant / responsable de traitement / responsable conjoint) et engagement du fournisseur à signer un accord de sous-traitance conforme à l'article 28 du RGPD ;
- **Sécurité de la chaîne d'approvisionnement** : liste des sous-traitants du fournisseur, capacité de détection et de réponse aux incidents dans des délais compatibles avec les obligations de notification, et réalisation d'audits de sécurité réguliers ;
- **Obligations des déployeurs publics (art. 27 RIA)** : le cahier des charges doit indiquer que l'établissement

réalisera une AIDF avant le déploiement du SIA et exiger du fournisseur la mise à disposition des informations nécessaires ;
- **Portabilité et interopérabilité** : conformité avec le CI-SIS (ANS), impliquant la prise en charge des standards suivants selon leur fonction respective :
  - « HL7 FHIR » : standard socle pour les échanges structurés de données cliniques et format cible de l'ensemble des volets CI-SIS ;
  - « DICOM » : pour l'échange et la gestion des images médicales ;
  - « CDA » : pour les documents cliniques structurés en phase transitoire.

Dans le cadre du Règlement EEDS, les solutions devront également supporter le format européen « EHRxF », dont les spécifications seront produites en FHIR. Le cahier des charges doit en outre interdire tout format propriétaire ou toute mesure technique entravant la portabilité effective des données (art. L. 1470-5 CSP).

1.3.3 Définir des critères d'analyse des offres spécifiques à l'IA

L'établissement doit adapter ses critères d'analyse des offres pour valoriser la conformité réglementaire et la qualité de la documentation, pas seulement le prix. Critères recommandés :

- **Conformité réglementaire (30 %)** : certification HDS de l'hébergeur, documentation du niveau de risque au sens du RIA, marquage CE, AIPD et AIDF réalisées ; conformité NIS2 de la chaîne d'approvisionnement ;
- **Qualité technique et performance (25 %)** : performances algorithmiques documentées (sensibilité, spécificité, robustesse), gouvernance des données, limitation et détection des biais, plan de surveillance post-déploiement ;
- **Transparence et explicabilité (20 %)** : documentation complète et accessible aux utilisateurs, mécanismes d'explicabilité des décisions, engagement de mise à jour de la documentation en cas d'évolution ;
- **Souveraineté et sécurité (15 %)** : hébergement en France ou dans l'UE, absence de dépendance technologique extra-européenne ;
- **Réversibilité et interopérabilité (10 %)** : formats d'export ouverts, procédure de réversibilité opérationnelle, absence de formats propriétaires.

1.3.4 Assurer le suivi de la performance en exploitation du SIA

Le suivi de la performance d'un SIA ne peut pas se limiter aux indicateurs classiques de disponibilité et de temps de réponse. L'établissement doit définir contractuellement des indicateurs spécifiques :

- **Indicateurs algorithmiques** : taux de précision, sensibilité, spécificité, taux de faux positifs et faux négatifs ;
- **Indicateurs de dérive** : évolution des performances dans le temps, notamment après mises à jour du système ou changements des données d'entrée ;
- **Indicateurs de biais** : analyse différenciée par sous-population (genre, âge, origine, pathologie) ;
- **Indicateurs d'usage** : taux d'adoption, taux de rejet des suggestions de l'IA par les professionnels, taux d'intervention humaine corrective.

Le contrat doit prévoir des revues de performance périodiques, des seuils minimaux déclenchant une procédure d'alerte, la possibilité de suspendre l'utilisation en cas de risque pour la sécurité des patients, et un plan d'amélioration continue.

2. COMMENT PARTAGER MES DONNÉES EN TANT QU'ACTEUR PUBLIC DE SANTÉ ?

Le partage des données de santé est encadré : ni librement cessibles, ni totalement fermées, ces données peuvent circuler sous conditions strictes selon les cas d'usage. Voici les quatre situations principales pour un acheteur public de santé.

2.1 Cas n° 1 — Partage à des fins de soins (utilisation primaire)

L'utilisation primaire désigne l'exploitation directe des données pour les soins du patient. C'est l'usage principal et légalement le plus simple.

Qui peut partager ?
L'établissement de santé, en qualité de responsable de traitement, peut partager les données d'un patient avec d'autres professionnels de santé intervenant dans sa prise en charge.

Sous quelles conditions ?
- Consentement du patient ou nécessité de soins (base légale art. 9, § 2, h RGPD) ;
- Secret médical préservé : seuls les professionnels de santé concernés par la prise en charge accèdent aux données (art. L. 1110-4 CSP) ;
- Hébergement sur infrastructure certifiée HDS : même pour un échange entre professionnels, le système portant les données doit être certifié HDS (art. L. 1111-8 CSP) ;
- Dans le cadre de l'EEDS : avec le consentement du patient, les données de santé peuvent être partagées avec des professionnels de santé d'autres États membres de l'UE en format interopérable (HL7 FHIR, EHRxF).

2.2 Cas n° 2 — Partage à des fins de recherche ou d'innovation (utilisation secondaire)

L'utilisation secondaire désigne la réutilisation des données à des fins d'intérêt général (recherche, épidémiologie, développement d'algorithmes, pilotage des politiques de santé publique). C'est le champ réglé par l'EEDS et le SNDS.

Qui peut en bénéficier ?
Des chercheurs, agences de santé publique, entreprises ou établissements, sous réserve d'autorisation. En France, l'accès aux données se fait principalement via le Health Data Hub dans le cadre des règles du SNDS.

Sous quelles conditions ?
- Base légale autonome et distincte de la collecte initiale : consentement explicite (art. 9, § 2, a RGPD), intérêt public en santé publique (art. 9, § 2, i RGPD) ou recherche scientifique (art. 9, § 2, j RGPD) ;
- Pseudonymisation obligatoire : les données transmises à des fins de recherche doivent au minimum être pseudonymisées. L'anonymisation réelle, si elle peut être atteinte, fait sortir les données du champ du RGPD ;
- Environnement sécurisé d'analyse : le Règlement EEDS impose le recours à des « trusted research environments » pour les usages secondaires ;
- Autorisation de la CNIL ou des organismes responsables désignés par l'EEDS (art. 36 du Règlement EEDS). En France, c'est principalement le Health Data Hub qui instruit ces demandes.

2.3 Cas n° 3 — Partage avec un fournisseur de SIA dans le cadre d'un contrat

Lorsqu'un établissement confie des données à un fournisseur de SIA dans le cadre d'un contrat, il ne s'agit pas d'un partage libre mais d'une mise à disposition strictement encadrée.

Conditions indispensables :

- Le fournisseur agit en qualité de **sous-traitant** au sens de l'article 28 du RGPD : il ne peut traiter les données qu'aux fins prévues au contrat, sur instruction de l'établissement, et sans réutilisation à ses propres fins ;
- Un **accord de sous-traitance conforme à l'article 28 du RGPD** doit être signé (voir clause 5 du clausier) ;
- La **certification HDS** du fournisseur (et de ses sous-traitants) est obligatoire pour toutes les données de santé à caractère personnel (art. L. 1111-8 CSP) ;
- Les données doivent être **hébergées et traitées dans l'UE** : tout transfert vers un pays tiers est soumis à l'accord écrit de l'établissement et à des garanties adéquates (voir clause 4 du clausier) ;
- Toute **réutilisation des données ou des outputs** par le fournisseur à des fins propres (notamment pour réentraîner son modèle) doit être **explicitement interdite** sans autorisation écrite préalable (voir clause 2.2 du clausier).

2.4 Cas n° 4 — Partage dans le cadre d'un groupement hospitalier de territoire (GHT)

Les GHT sont une opportunité de mutualisation des données et des SIA entre établissements membres, sous réserve d'un cadre de gouvernance adapté.

Ce qui est possible :

- Mutualisation du sourcing et des marchés : les établissements du GHT peuvent négocier collectivement et partager les résultats des évaluations fournisseurs ;
- Harmonisation des pratiques de gouvernance IA et de gestion des incidents : les GHT peuvent mettre en place un registre commun des SIA et des protocoles partagés de supervision humaine ;
- Partage de données entre établissements membres pour la continuité des soins : possible sous réserve de respecter les conditions de l'utilisation primaire (consentement ou nécessité de soins, HDS, secret médical).

Les interdictions à retenir :

- Monétisation directe des données de santé : **interdite** — les données de santé à caractère personnel ne peuvent pas faire l'objet d'une vente ou cession commerciale ;
- Transfert vers un prestataire non certifié HDS : **interdit** sans certification valide couvrant les activités concernées ;
- Hébergement ou traitement hors de l'UE sans garanties adéquates : **interdit** — tout accès depuis un pays tiers (y compris pour maintenance ou mise à jour) est soumis à accord écrit de l'établissement ;
- Réutilisation des données par le fournisseur sans autorisation : interdite — une clause contractuelle explicite est indispensable (voir clause 2.2 du clausier) ;
- Partage de données non pseudonymisées à des fins de recherche : **interdit** — la pseudonymisation est le standard minimal exigé par l'EEDS pour l'utilisation secondaire.

La phase de rédaction du contrat est le principal levier pour sécuriser l'acquisition d'un SIA. Elle doit mobiliser le DPO en amont et s'articuler autour de quatre exigences principales.

3. LES BONNES PRATIQUES À METTRE EN PLACE PENDANT L'ACHAT

3.1 Information et conformité réglementaire

Le contrat doit exiger du fournisseur une documentation claire et précise, notamment sur :

- la destination d'usage et la classification du SIA (haut risque, risque limité, etc.) ;
- les données d'entraînement, les performances validées (sensibilité, spécificité, etc.) et les règles de gouvernance des données ;
- les limites et biais connus ;
- le principe de fonctionnement de manière compréhensible pour les utilisateurs ;
- les modalités de supervision humaine du SIA ;
- les flux de données et API tierces.

Plus globalement, le fournisseur doit fournir les preuves de sa conformité (certification HDS, identification des sous-traitants, localisation des données dans l'UE, etc.).

3.2 Interopérabilité avec le système d'information

Les établissements doivent vérifier et contractualiser les garanties d'interopérabilité du SIA avec leurs différents systèmes d'information (DPI, système d'information radiologique, etc.).
Ils doivent également exiger une cartographie des installations techniques et des flux de données.

POINT D'ATTENTION
L'absence d'interopérabilité du SIA avec les systèmes d'information de l'établissement peut engendrer des risques pour la prise en charge des patients : doubles saisies, erreurs de transcription, etc.

3.3 Clauses contractuelles spécifiques

Il est recommandé de prévoir un accord de niveau de service (SLA) précisant :

- les délais de résolution des incidents, les engagements de disponibilité et les modalités de validation des mises à jour logicielles ;
- une période de calibrage (POC) avec possibilité de rétractation sans pénalité si le SIA s'avère inadapté au contexte ;
- une clause de performance conditionnant le paiement à la satisfaction d'un seuil défini ;
- des conditions de fin de contrat garantissant la restitution des données dans un format exploitable et la certification de suppression chez le fournisseur ;
- une sortie sans obstacle technique ni financier.

Ces enjeux sont traités par le clausier associé à ce guide (cf. Chapitre 3).

3.4 Encadrement des données à caractère personnel

Le contrat doit préciser la répartition des rôles RGPD (responsable de traitement, sous-traitant, etc.), les catégories de données traitées, les mesures de sécurité, les conditions de recours à des sous-traitants ultimes (obligation de localisation dans l'UE), les modalités d'exercice des droits des personnes, et interdire toute réutilisation des données à des fins propres au fournisseur sans accord écrit préalable.
Ces enjeux sont couverts par les clauses du clausier (cf. Chapitre 3, sections 5 et 6).

POINT D'ATTENTION
L'établissement ne doit pas contractualiser si :
- la conformité juridique pour l'usage prévu du SIA n'est pas documentée ;
- le fonctionnement ou le circuit des données reste opaque ;
- il persiste un risque de biais sur l'usage du SIA.

4. LES BONNES PRATIQUES À METTRE EN PLACE POUR L'EXPLOITATION DU SIA

4.1 Gouvernance interne : mettre en place un comité de suivi dédié

L'établissement doit mettre en place une gouvernance de l'IA adaptée à sa taille et à ses ressources.

- **Pour les grands établissements** (CHU, etc.) : un comité pluridisciplinaire associant a minima la DSI, le DPO, le RSSI, un représentant des utilisateurs métier, un représentant des usagers et, si nécessaire, un référent éthique et des juristes.
- **Pour les établissements de taille intermédiaire** : désigner un référent IA en lien avec les instances existantes.

Ce comité se réunit au moins une fois par trimestre et examine :

- les indicateurs de performance du SIA ;
- les incidents survenus et les mesures correctives ;
- les mises à jour effectuées par le fournisseur ;
- l'évolution du cadre réglementaire ;
- les retours des utilisateurs.

Les GHT sont invités à mutualiser cette gouvernance et à harmoniser les pratiques entre établissements membres.

4.2 Tenir un registre des SIA déployés

L'établissement doit tenir à jour un registre recensant l'ensemble des SIA utilisés — qu'ils aient été acquis délibérément ou intégrés progressivement — et mentionner pour chaque système :

- dénomination, version, fournisseur et sous-traitants impliqués ;
- qualification juridique (niveau de risque au sens du RIA, statut de dispositif médical, etc.) ;
- catégories de données traitées et finalités ;
- utilisateurs concernés et référent interne désigné ;
- date de déploiement, mises à jour effectuées et conséquences évaluées ;
- niveau de criticité clinique et modalités de suivi (indicateurs, incidents, traçabilité).

4.3 Encadrer les mises à jour intégrant des briques d'IA

Les mises à jour logicielles sont le principal vecteur de l'« IA subie ».

Pour s'en prémunir, l'établissement doit :

- exiger une information préalable détaillée sur le contenu de chaque mise à jour ;
- subordonner l'activation de toute nouvelle fonctionnalité d'IA à une validation formelle interne ;
- prévoir un environnement de test pour évaluer l'impact avant déploiement en production ;
- documenter les mises à jour et leurs impacts dans le registre.

POINT D'ATTENTION
Toute évolution significative du système doit faire l'objet d'une réévaluation :
- le niveau de risque au sens du RIA a-t-il changé ?
- l'AIPD et l'AIDF doivent-elles être mises à jour ?
- les informations fournies aux patients sont-elles toujours exactes ?

4.4 Assurer une supervision humaine effective

La supervision humaine des SIA en contexte de soins repose sur deux fondements juridiques distincts et complémentaires :
- **L'article 22 du RGPD** interdit toute décision automatisée produisant des effets juridiques ou affectant significativement une personne, prise sans intervention humaine, dès lors qu'elle repose exclusivement sur un traitement automatisé de données à caractère personnel. Cette interdiction s'applique notamment lorsqu'un SIA prend seul une décision relative à la prise en charge d'un patient.
- **Le RIA** impose aux déployeurs de SIA à haut risque des mesures de contrôle humain effectif (art. 26, § 2, et art. 14 RIA) permettant d'intervenir sur le SIA, d'ignorer ou de passer outre ses résultats, ou de l'arrêter. Le clausier consacre ce principe à la clause 9.4 : les SIA « ne peuvent se substituer à la décision médicale ni à la responsabilité des professionnels de santé ».

Ces deux obligations se cumulent et s'appliquent simultanément aux établissements publics de santé.

Pour respecter ces obligations, l'établissement doit :
- désigner les personnes chargées de la supervision et s'assurer de leur compétence ;
- définir les cas imposant une intervention humaine obligatoire avant toute décision ;
- mettre en place des procédures permettant d'ignorer, corriger ou annuler les résultats du système ; documenter les décisions prises sur la base des résultats de l'IA ;
- garantir la liberté de décision du praticien (art. R. 4127-5 CSP).

4.5 Traçabilité des usages

La traçabilité est à la fois un outil de prévention des risques et un support à la redevabilité en cas de litige ou de contrôle. L'établissement doit :
- intégrer la traçabilité (« IA utilisée : oui/non ») dans les procédures internes et dans le dossier patient ;
- conserver les logs techniques et garantir contractuellement l'accès de l'établissement à ces journaux ;
- former les professionnels au signalement des incidents IA via un circuit dédié (type « algorithmovigilance »).

4.6 Gérer les incidents spécifiques à l'IA

Les SIA peuvent générer des incidents spécifiques : dysfonctionnements algorithmiques, biais détectés en exploitation, dérives de performance, attaques adverses, utilisation non conforme, etc.

L'établissement doit articuler les obligations de notification multiples :
- Notification à la CNIL dans les 72 heures en cas de violation de données (art. 33 RGPD) ;
- Notification à l'ANSSI en cas d'incident significatif (directive NIS2) ;
- Signalement aux autorités compétentes en cas d'incident grave impliquant un SIA à haut risque (art. 26, § 5 RIA) ;
- Signalement en cas d'incident impliquant un dispositif médical embarquant de l'IA.

CHAPITRE 3

POURQUOI LES CONTRATS STANDARDS NE SUFFISENT-ILS PAS FACE AUX SYSTÈMES D'IA EN SANTÉ ?

POURQUOI LE CLAUSIER IA ET SANTÉ EST-IL NÉCESSAIRE ?

Les établissements publics de santé produisent et gèrent des volumes considérables de données. Ces données sont un actif stratégique au service des patients, des professionnels de santé, de la recherche et des politiques de santé publique.

Pourtant, les contrats standards proposés par les prestataires privés sont rarement adaptés aux exigences spécifiques de la santé. Ils peuvent conduire à :

- une captation des données de santé à des fins d'entraînement de modèles d'IA au profit du prestataire, sans autorisation de l'établissement ;
- une dépendance technique excessive rendant tout changement de prestataire coûteux et risqué pour la continuité des soins ;
- un hébergement de données sensibles hors de l'UE, en violation du RGPD ou des règles HDS ;
- l'absence de supervision humaine effective sur des décisions médicales partiellement automatisées.

À cela s'ajoute une inflation normative sans précédent : RGPD, RIA, Règlement EEDS, Directive NIS2, Règlements sur les DM et les DMDIV. Tous ces textes s'appliquent simultanément et leurs exigences doivent se traduire concrètement dans les contrats de la commande publique.
Le clausier répond à ce besoin en proposant des clauses types, prêtes à l'emploi, qui permettent aux établissements de contractualiser dans le respect de leurs obligations légales et de préserver leur souveraineté sur leurs données.

Quels enjeux ce clausier traite-t-il ?

Le clausier couvre dix thématiques structurantes, organisées en blocs cohérents :

THÉMATIQUE	ENJEU PRINCIPAL
1. Définitions et garanties de conformité	Sécuriser le périmètre contractuel et garantir la conformité continue du prestataire à l'ensemble du cadre légal applicable.
2. Souveraineté des données	Interdire toute appropriation ou réutilisation des données - notamment pour entraîner des modèles d'IA - sans autorisation expresse de l'établissement.
3. Interopérabilité et ouverture des données	Garantir l'accès aux données dans des formats ouverts et assurer la conformité aux obligations du Règlement EEDS (portabilité, utilisation secondaire, etc.).
4. Hébergement et localisation	Imposer la certification HDS (et optionnellement SecNumCloud) et localiser les données au sein de l'UE.
5. Protection des données personnelles (RGPD)	Clarifier les rôles (responsable de traitement / sous-traitant) et fixer les engagements du prestataire conformément à l'article 28 du RGPD.
6. Sécurité et cybersécurité	Imposer un niveau de sécurité adapté aux entités essentielles (Directive NIS2), encadrer la gestion des incidents - y compris les incidents propres aux SIA - et prévoir un droit d'audit.
7. Réversibilité et continuité de service	Garantir la restitution des données et des modèles d'IA à tout moment, sans rupture de la prise en charge des patients.
8. IA générative et services d'IA externes	Interdire tout recours non autorisé à des outils d'IA tiers (Copilot, ChatGPT, etc.) et tout transfert de données vers ces services.

9 & 10. Encadrement de l'IA et propriété intellectuelle	Qualifier le niveau de risque du SIA, garantir la supervision humaine de la décision médicale et définir à qui appartiennent les modèles entraînés sur les données de l'établissement.

ILLUSTRATION
Un centre hospitalier universitaire déploie un outil d'aide au diagnostic par imagerie médicale fourni par une start-up. Sans clausier adapté : les données d'imagerie sont utilisées pour réentraîner le modèle commercial du prestataire, et en cas de faillite, l'hôpital ne peut récupérer ni ses données ni l'outil. Avec les clauses du clausier (sections 2, 7, 9 et 10) : l'usage des données est strictement limité à la prestation, la réversibilité est garantie sous 30 jours, et les modèles entraînés sur les données de l'établissement restent sous sa maîtrise.

Un hôpital souscrit à un logiciel de gestion des dossiers patients intégrant des fonctionnalités d'IA générative. Sans clause d'encadrement : des données de patients sont transmises à une plateforme d'IA hébergée aux États-Unis (soumise au Cloud Act), en violation du RGPD et du CSP. Les clauses des sections 4 et 8 permettent d'imposer la localisation européenne et de subordonner tout usage d'IA générative à une autorisation expresse de l'établissement.

Comment utiliser ce clausier ?

Le clausier est un outil opérationnel, et non un modèle de contrat clé en main. Voici comment l'utiliser efficacement.

Étape 1 - Identifier les clauses pertinentes pour votre projet
Toutes les clauses ne s'appliquent pas à tous les contrats. La pertinence de chaque section dépend de la nature de la solution (SaaS, prestation de service, développement sur mesure, dispositif médical logiciel) et des données traitées. Un marché portant sur un simple outil RH sans traitement de données de santé n'appelle pas les mêmes exigences qu'un contrat relatif à un SIA d'aide au diagnostic.

Étape 2 - Adapter les clauses au contexte du marché
Chaque clause type comporte des zones à compléter (délais, formats techniques, modalités d'audit, conditions tarifaires de réversibilité, etc.), signalées par la mention [à compléter]. Ces éléments doivent être précisés dans les pièces techniques et financières du marché. Le clausier indique également, pour chaque section, les limites et points de vigilance à prendre en compte lors de l'adaptation.

Étape 3 - Articuler avec les autres pièces du marché
Les clauses du clausier ont une portée générale. Elles doivent être complétées par :
- un cahier des charges fonctionnel et technique précisant les exigences propres au projet ;
- une annexe relative à la protection des données à caractère personnel (RGPD), structurée conformément aux clauses contractuelles types de la Commission européenne ;
- le cas échéant, un accord spécifique sur la propriété intellectuelle des modèles d'IA entraînés sur données mixtes.

Étape 4 - Assurer la veille réglementaire
Le cadre juridique évolue rapidement. Le RIA entre en application progressivement depuis 2026 ; le Règlement EEDS prévoit également un calendrier échelonné au cours des prochains mois et années.

Une frise chronologique de l'entrée en application des principales législations est disponible en annexe. Il est recommandé d'inclure dans chaque contrat une clause de veille réglementaire imposant au prestataire d'informer l'établissement de toute évolution susceptible d'affecter les conditions d'exécution (voir clause 1.2 du clausier).

CHAPITRE 4

QUELS SONT LES PRINCIPAUX CONTENTIEUX AUXQUELS SONT CONFRONTÉS LES ÉTABLISSEMENTS DE SANTÉ DANS L'USAGE DU NUMÉRIQUE ?

Les établissements publics de santé gèrent des quantités considérables de données de santé et s'appuient sur des solutions numériques de plus en plus complexes. Cette évolution génère de nouveaux enjeux juridiques : contentieux, sanctions des autorités de contrôle, engagement de la responsabilité de l'établissement.

Cinq grandes problématiques juridiques se dégagent.

Thème n° 1 - Les grandes bases nationales de données de santé

La France a mis en place plusieurs grandes plateformes qui centralisent les données de santé de millions de patients : le SNDS et la Plateforme des données de santé.

Ces outils sont indispensables pour la recherche médicale et le pilotage des politiques de santé, mais leur création et leur fonctionnement ont donné lieu à des contentieux.

- **Choix de l'hébergeur** : la décision de confier la Plateforme des données de santé à Microsoft (serveurs en France, mais société américaine) a été contestée. Des associations ont soutenu que le Cloud Act permettait aux autorités américaines d'accéder aux données, en violation du droit de l'UE.
- **Élargissement du SNDS** : le décret de 2021 élargissant le périmètre du SNDS et le nombre d'organismes y ayant accès a également fait l'objet d'un recours.

Le Conseil d'État a validé l'utilisation d'urgence de la Plateforme des données de santé pendant la crise Covid (CE, ord. 19 juin 2020, n° 440916) tout en imposant des garde-fous : interdiction des transferts de données hors UE et engagements contractuels renforcés (CE, ord. 13 oct. 2020, n° 444937). Il a également confirmé la légalité du décret élargissant le SNDS au regard du RGPD en 2022 (CE, 23 nov. 2022, n° 456162).

Thème n° 2 - La sécurité des systèmes informatiques et les fuites de données

Les établissements publics de santé sont des cibles privilégiées des cyberattaques. Lorsqu'une fuite de données survient ou qu'une faille de sécurité est détectée, l'établissement et ses prestataires peuvent être mis en cause.

- **Sanctions de la CNIL** : l'autorité peut mettre en demeure un établissement ou son prestataire lorsque des données de patients ont été exposées (serveur mal configuré, accès non autorisé, etc.). Les données de santé bénéficient d'une protection renforcée.
- **Hébergeur non certifié HDS** : la loi SREN oblige à confier les données de santé à un hébergeur disposant de la certification HDS. Recourir à un prestataire non certifié expose l'établissement à des sanctions.
- **Droits de la défense** : une décision du Conseil constitutionnel d'août 2025 a rappelé que toute personne visée par une procédure de sanction CNIL doit être informée de son droit de ne pas s'auto-incriminer.

Thème n° 3 - L'hébergement et l'externalisation : le cas du Cloud Act

De nombreux établissements publics de santé recourent à des services Cloud proposés par de grandes entreprises américaines (Microsoft Azure, etc.), faute d'alternative européenne suffisamment puissante.
Cette pratique soulève une question centrale : les données des patients français peuvent-elles être réclamées par les autorités américaines ?

Pour les autorités françaises, le risque d'accès des autorités américaines ne peut pas être totalement exclu, mais reste acceptable si des mesures concrètes sont prises : pseudonymisation des données, certification HDS de l'hébergeur, interdiction contractuelle des transferts hors UE. La CNIL a adopté cette position sur l'entrepôt EMC2 hébergé sur Azure en France par plusieurs CHU et cliniques (CNIL, délib. n° 2023-146 du 21 déc. 2023), confirmée par le Conseil d'État (CE, ord. 19 nov. 2024, n° 491644).

Thème n° 4 – La recherche, l'IA et l'accès aux données

Les données de santé ont une valeur considérable pour la recherche médicale et le développement de l'IA. Des chercheurs, autorités publiques et entreprises souhaitent y accéder. L'encadrement de ces accès est à l'origine de nombreux litiges.

- **Accès par des acteurs extérieurs :** la CNIL a autorisé en février 2025 l'Agence européenne des médicaments à accéder aux données du SNDS, en limitant la durée (3 ans) et la taille des données transmises. Ces autorisations font l'objet de recours devant le Conseil d'État.
- **Risque de réidentification :** même anonymisées, les données peuvent en théorie permettre d'identifier un patient si elles sont croisées avec d'autres sources. La robustesse des techniques d'anonymisation est au cœur des débats.
- **Respect des finalités légales :** le SNDS ne peut être utilisé qu'à des fins précises (recherche, politiques de santé, évaluation des soins). Tout usage en dehors de ce cadre est illicite.

Thème n° 5 – Les outils numériques de soin : télémédecine, espace numérique de santé

L'Espace Numérique de Santé (« Mon espace santé ») a été ouvert pour chaque citoyen à partir de janvier 2022. La télémédecine et les plateformes de télésoin se développent rapidement.

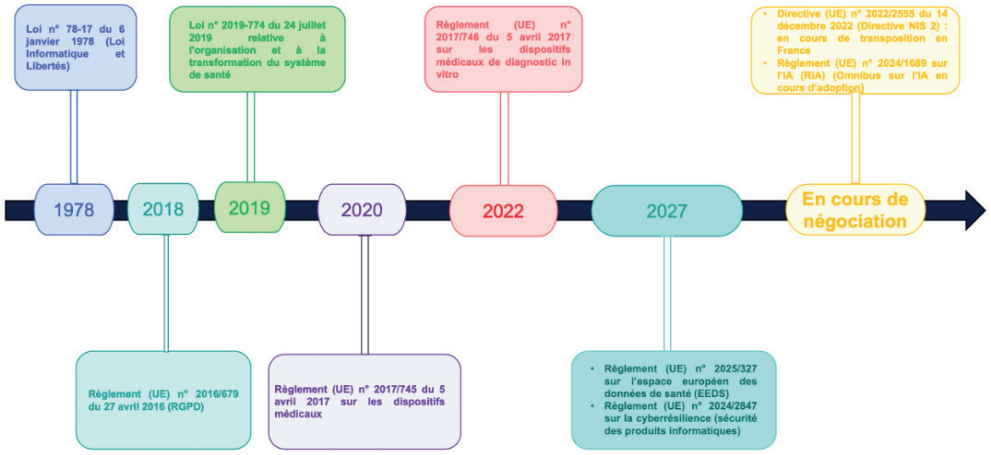
Ces outils soulèvent de nouvelles questions juridiques.

- **Consentement et information** : l'ouverture automatique de l'Espace Numérique de Santé soulève des questions sur l'information réelle des patients et leurs droits d'opposition ou de paramétrage.
- **Sécurité des plateformes de télémédecine** : les risques sont identiques à ceux des systèmes hospitaliers classiques (hébergeur non certifié, fuite de données, cloud étranger).

À ce jour, aucune décision de justice emblématique ne porte spécifiquement sur ces outils : les contentieux s'appuient sur les mêmes règles que pour les autres systèmes d'information hospitaliers.

ANNEXES

Annexe n° 1 – Frise chronologique de l'entrée en application des principales législations françaises et européennes sur les données



Annexe n° 2 – Recommandations à destination des établissements publics de santé (HAS, CNIL et ANSSI)

THÈME	BON USAGE DES SIA EN CONTEXTE DE SOINS (HAS-CNIL / FEV. 2026)	PREMIERES CLEFS D'USAGE DE L'IA GENERATIVE EN SANTE (HAS / OCT. 2025)	RISQUES CYBER LIES A L'IA (ANSSI / FEV. 2025)
Gouvernance & organisation	– Désigner un référent IA et un comité pluridisciplinaire (DSI, DPO, RSSI). – Cartographier les SIA déployés dans un registre. Créer un guichet unique de validation des projets IA.	– Valider toute expérimentation IA par la gouvernance de l'établissement (DSI, juridique, qualité). – Privilégier les usages collectifs et structurés.	– Impliquer les directions dans les décisions d'implémentation IA. – Favoriser le dialogue entre gouvernances cyber et IA.
Acquisition & conformité réglementaire	– Vérifier le marquage CE, la classification RIA (haut risque / limité) et la certification HDS de l'hébergeur. – Réaliser l'AIPD et l'AIDF. Adapter les contrats (réversibilité, clauses data, droit d'audit).	– Vérifier la conformité réglementaire du système (marquage CE, RGPD). – Interroger l'entité responsable sur les conditions d'hébergement, le modèle économique et les limites identifiées.	– Réaliser une analyse de risque avant tout déploiement. – Évaluer la sensibilité du cas d'usage, la maturité cyber, l'auditabilité et l'explicabilité du SIA.
Formation & acculturation	– Former les professionnels à l'utilisation du SIA et aux procédures de mode dégradé. – Vérifier la compétence des superviseurs (art. 26 RIA).	– Se former aux modalités d'utilisation, aux enjeux réglementaires et aux règles de confidentialité des données de santé. – Expérimenter de façon structurée.	Former et sensibiliser aux risques liés à l'IA, notamment au niveau des directions, pour garantir des décisions d'implémentation éclairées.

Supervision humaine & décision médicale	– Garantir le contrôle humain effectif (art. 22 RGPD ; art. 14 RIA) sur les décisions médicales. Le SIA ne peut se substituer à la décision médicale. – Calibrer la supervision selon le niveau de risque clinique.	– Considérer chaque contenu généré comme une proposition à contrôler. – Conserver ses compétences et la qualité de sa pratique. – Interroger la pertinence de chaque usage.	– Intégrer la validation humaine dès que nécessaire. – Ajuster le niveau d'autonomie du SIA en fonction de la criticité des actions et de l'analyse de risque.
Protection des données & confidentialité	– Informer le patient de l'utilisation d'un algorithme (art. L. 4001-3 CSP). – Héberger les données chez un prestataire certifié HDS. Formaliser les rôles RGPD (responsable de traitement / sous-traitant).	– Ne partager aucune information identifiante ni relevant du secret médical dans les requêtes. – Vérifier les conditions d'hébergement des données du système.	– Cartographier la chaîne d'approvisionnement et la nature des données traitées. – Évaluer les risques d'extraction et de fuite de données confidentielles.
Sécurité & cybersecurité	– Auditer la chaîne d'approvisionnement du SIA (API tierces, sous-traitants). – Prévoir un PCA avec scénario d'indisponibilité du SIA. – Mettre en place un circuit de signalement des incidents IA.	– Privilégier les systèmes disposant d'un point de contact support accessible. – Rester attentif aux évolutions réglementaires et aux communications institutionnelles.	– Limiter les interconnexions entre le SIA et les autres systèmes d'information. – Détecter les attaques spécifiques à l'IA (empoisonnement, extraction, évasion). – Mettre en place une veille sur les menaces émergentes.
Traçabilité & vigilance	– Tracer les usages du SIA dans le dossier patient (« IA utilisée : oui/non »). – Surveiller les performances et encadrer les mises à jour. – Prévoir une procédure de désinstallation et de restitution des données.	– Définir des objectifs et critères d'évaluation périodique du système (Évaluer). – Partager les retours d'expérience dans l'organisation et l'écosystème.	– Superviser et maintenir le SIA en continu pour détecter biais et vulnérabilités. – Assurer une veille technologique et réglementaire pour anticiper les évolutions du contexte.

NOTES :

CE GUIDE A ÉTÉ RÉDIGÉ PAR :

ALÉRIONS AVOCATS
t. +33 (0)1 58 56 97 00 | f. +33 (0)1 58 56 97 01 | paris@alerionavocats.com
137, rue de l'Université – 75007 Paris, France
Sarl au capital de 44 520 € | Toque N° KO126 | RCS Paris 450 237 854
N° TVA Intracommunautaire FR 20 450 237 854 | N° Siret 450 237 854 000 28
www.alerionavocats.com

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org
02 23 06 10 30 | contact@pole-excellence-cyber.org