HAUTE AUTORITÉ DE SANTÉ

COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

RECOMMANDER
LES BONNES PRATIQUES

GUIDE

Accompagner le bon usage des systèmes d'intelligence artificielle en contexte de soins

Document de travail - 16 février 2026

Descriptif de la publication

Titre	Accompagner le bon usage des systèmes d'intelligence artificielle en contexte de soins
Méthode de travail	La méthodologie de travail inclut : – des auditions ciblées de parties prenantes, appel à contribution et revue systématique de la littérature ; – un groupe de travail ; – une consultation publique.
Objectif(s)	Ce document a pour objectif d'accompagner les établissements et professionnels dans le bon usage des systèmes d'intelligence artificielle (SIA) utilisés en contexte de soins ainsi que la mise en application du 6e cycle de certification des établissements de santé. Il sera utile également à tout établissement, décideur, professionnel utilisateur d'un SIA exerçant dans un autre contexte de soins.
Cibles concernées	Professionnels de santé et établissements de santé.
Demandeur	Auto-saisine HAS
Promoteur(s)	Haute Autorité de santé (HAS)
Pilotage du projet	Mission Numérique en Santé (MNS)
Recherche documentaire	Estelle DIVOL FABRE et Marina RENNESSON
Auteurs	**HAS** **MNS :** Simon RENNER (chef de projet), Paul Valois (chef de projet), Aude ROCHEREAU (cheffe de projet), Aubry SAINT-CAST (stagiaire), Julie MARC (adjointe à la cheffe de service), Corinne COLLIGNON (cheffe de service) **Service Juridique :** Adriane LOUYER (juriste, déléguée à la protection des données), Maxence LYONNET (chef de service). **CNIL** **Service de la Santé :** Aurore GAIGNON (juriste) ; **Service de l'IA :** Charlotte BAROT (analyste).
Conflits d'intérêts	Les membres du groupe de travail ont communiqué leurs déclarations publiques d'intérêts à la HAS. Elles sont consultables sur le site https://dpi.sante.gouv.fr. Elles ont été analysées selon la grille d'analyse du guide des déclarations d'intérêts et de gestion des conflits d'intérêts de la HAS. Pour son analyse la HAS a également pris en compte la base «Transparence-Santé» qui impose aux industriels du secteur de la santé de rendre publics les conventions, les rémunérations et les avantages les liants aux acteurs du secteur de la santé. Les intérêts déclarés par les membres du groupe de travail et les informations figurant dans la base «Transparence-Santé» ont été considérés comme étant compatibles avec la participation des experts au groupe de travail.
Validation	Version du 16 février 2026

Ce document ainsi que sa référence bibliographique sont téléchargeables sur www.has-sante.fr

Haute Autorité de santé – Service communication information
5 avenue du Stade de France – 93218 SAINT-DENIS LA PLAINE CEDEX. Tél. : +33 (0)1 55 93 70 00

Sommaire

Introduction

Contexte

L'intelligence artificielle (IA), dans ses multiples formes, s'intègre progressivement et concrètement dans les organisations de soins : aide à la rédaction de comptes rendus médicaux, algorithmes embarqués dans les chaînes de biologie ou d'imagerie, systèmes de tri des patients ou d'aide à la décision médicale, etc. Une enquête de la Fédération hospitalière de France (FHF), datant de juillet 2025, a ainsi mis en évidence que 65 % des établissements de santé publics utilisaient déjà des technologies d'IA en production (sur 110 établissements participant à l'enquête)[1]. Certains systèmes d'intelligence artificielle (SIA)[2] sont clairement identifiables comme tels, d'autres peuvent être intégrés de manière plus subtile au sein des dispositifs médicaux ou technologies numériques.

Un SIA peut revêtir différents rôles selon la place qu'il occupe par rapport à l'activité humaine initiale :

- **un rôle supplétif**, permettant par exemple d'accompagner un professionnel dans la réalisation d'un acte ou geste ;
- **un rôle substitutif**, permettant par exemple de remplacer un professionnel en automatisant une tâche administrative sans valeur médicale ajoutée ;
- **un rôle palliatif**, venant par exemple compenser une absence de prise en charge ou d'activité réalisée par un professionnel de santé[3].

Quel que soit le rôle du SIA, aucun régime de responsabilité juridique spécifique n'a, à ce jour, été établi pour les professionnels de santé utilisateurs d'IA[4]. La responsabilité du professionnel de santé demeure appréciée au regard du droit commun, ce qui implique que celui-ci répond non seulement de l'usage qu'il fait de l'IA, mais également du degré d'autonomie qu'il accorde à cet outil dans l'exécution de ses gestes ou dans ses décisions médicales.

Ainsi, le professionnel de santé reste entièrement responsable, même lorsque l'acte est accompli avec l'assistance d'un SIA.

Dans ce contexte, l'ajout d'un SIA en contexte de soins et l'organisation associée doivent être accompagnés dans une logique d'amélioration de la qualité et de la sécurité des soins. Deux premiers critères dédiés aux SIA ont été ajouté dans le 6e cycle de certification des établissements de santé, applicable aux établissements depuis septembre 2025.

[1] FHF, Livre blanc L'IA en santé : qui est le maître ? https://www.calameo.com/fhf/read/0037957021bc5deb3eade?page=11

[2] Un système d'IA est défini comme « un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels »

[3] DREES, Les transformations par les technologies numériques vues par les SHS. Quels usages dans les champs de la santé, du handicap, de l'autonomie et de l'accès aux prestations sociales ? – Site web

[4] Maître Lina WILLIATTE-PELLITTERI, Avocat au Barreau de Lille « L'intelligence artificielle et la responsabilité du médecin : quel impact ? », Avocats Grands Lille, mars 2025

Dans cette même logique, ce document vise ainsi à :

1. **clarifier les obligations** que les professionnels de santé, les établissements et les structures de soins doivent mettre en œuvre pour utiliser un SIA en contexte de soins (par exemple, liées à l'utilisation d'un SIA à haut risque) ;
2. **fournir des recommandations de bonnes pratiques**, modulables selon les contextes d'exercice, pour sécuriser et favoriser le bon usage des SIA, sans freiner l'innovation ni le déploiement de ces technologies.

Ces recommandations s'appuient sur le contexte légal et réglementaire qui se met en place tant au niveau français qu'européen, et notamment le règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (RIA). Une mise au point sur ce règlement, qui entre en application de manière progressive, est disponible en Annexe 1.

Par ailleurs, lorsque l'utilisation d'un SIA implique un traitement de données à caractère personnel, le Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) est applicable. Ainsi, **un établissement ou professionnel de santé, déployeur d'un SIA, sera qualifié de responsable de traitement et sera notamment tenu de s'assurer que le SIA utilisé permet un traitement de données conforme à la réglementation**. Il sera également tenu à un devoir de loyauté et de transparence vis-à-vis de la personne dont les données sont concernées (a fortiori lorsqu'il s'agit de données de santé d'un patient).

Dans cette logique, la HAS et la Commission nationale de l'informatique et des libertés (CNIL) ont mis en œuvre un partenariat afin d'accompagner le bon usage des SIA en contexte de soins à travers des travaux conjoints. Le détail des stratégies respectives de la HAS et de la CNIL sur l'intelligence artificielle est disponible en Annexe 2 Erreur ! Source du renvoi introuvable.**.**

Objectifs du document

Ce document vise à favoriser le bon usage des SIA en contexte de soins et à soutenir les professionnels et les établissements de santé dans l'application des nouveaux critères dédiés aux SIA au sein du 6e cycle de certification des établissements de santé.

Périmètre des recommandations

À qui s'adressent ces recommandations ?

Ces recommandations s'adressent aux professionnels de santé[5], établissements de santé ou structures d'exercice libérale souhaitant déployer et utiliser un SIA en contexte de soins.

[5] Articles L. 4001-1 à L4444-3 du CSP

Deux types d'acteurs principaux sont concernés par ces recommandations :

- le **déployeur**[6] (tel que défini dans le RIA) : il prend la décision d'utiliser un SIA. Il met en place une gouvernance, une politique d'information, des actions de formation, etc. ;
- **l'utilisateur** : la personne physique qui utilise le SIA et qui doit disposer des qualifications nécessaires pour s'assurer qu'il l'utilise conformément à la destination du produit et selon les instructions qui lui sont données par le fournisseur et sa structure d'exercice.

Dans le cas d'un exercice libéral, ces deux acteurs sont souvent une seule et même personne.

Pour quels SIA ?

Ces recommandations s'appliquent à l'ensemble des SIA ayant un impact direct sur la prise en charge d'un patient et les pratiques de soins, notamment les activités de prévention, de diagnostic, de soins ou à des interventions nécessaires à la coordination de plusieurs de ces activités[7]. C'est par exemple le cas des SIA d'aide à la détection de fractures osseuses aux urgences ou au contourage en radiothérapie, d'assistant de rédaction de comptes-rendus, d'aides à l'organisation des flux de patients au bloc opératoire ou aux urgences, etc. Ils seront regroupés sous la dénomination des « SIA utilisés en contexte de soins ».

L'ensemble des SIA utilisés en contexte de soins seront concernés par ces recommandations, quel que soit le type de SIA et sa qualification (dispositif médical - DM/DMDIV - ou non DM/DMDIV), sa finalité et destination d'usage (aide au diagnostic ou à la décision médicale) et son niveau de risque selon le RIA. À noter toutefois qu'en fonction de la classe de risque du SIA (SIA à haut risque, SIA à risque limité ou SIA à risque minimal), les obligations du déployeur au titre du RIA seront différentes.

Les SIA utilisés en contexte de soin mais qui ne relèvent pas de la définition d'un dispositif médical ou dispositif médical de diagnostic in vitro au sens des règlements UE 2017/745 (RDM) ou UE 2017/746 (RDIV) et basés sur de l'IA générative peuvent présenter des spécificités rendant certaines recommandations non applicables (par exemple, pour traduire un échange entre un patient et un professionnel de santé).

Les SIA utilisés en dehors du contexte de soins, comme aide à la facturation ou la gestion des ressources humaines (gestion du planning hospitalier par exemple), sont hors du périmètre des présentes recommandations.

[6] Un déployeur est défini dans le Règlement européen sur l'IA comme étant « une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel ». Les professionnels de santé, établissements de santé ou structure d'exercice libérale utilisant un système d'IA en contexte de soins seront ainsi qualifiés de déployeurs

[7] Article L. 1470-1 du CSP

À quel moment ?

Ces recommandations interviennent une fois que le déployeur s'est assuré que le SIA répond à un besoin et qu'il a choisi le SIA qu'il souhaite utiliser. En amont, si le choix n'est pas encore fait, un guide d'aide aux choix des dispositifs médicaux numériques à usage professionnel[8] est disponible sur le site de la HAS pour guider cette étape. Ce guide est applicable pour éclairer les choix de technologies qui ne sont pas des dispositifs médicaux.

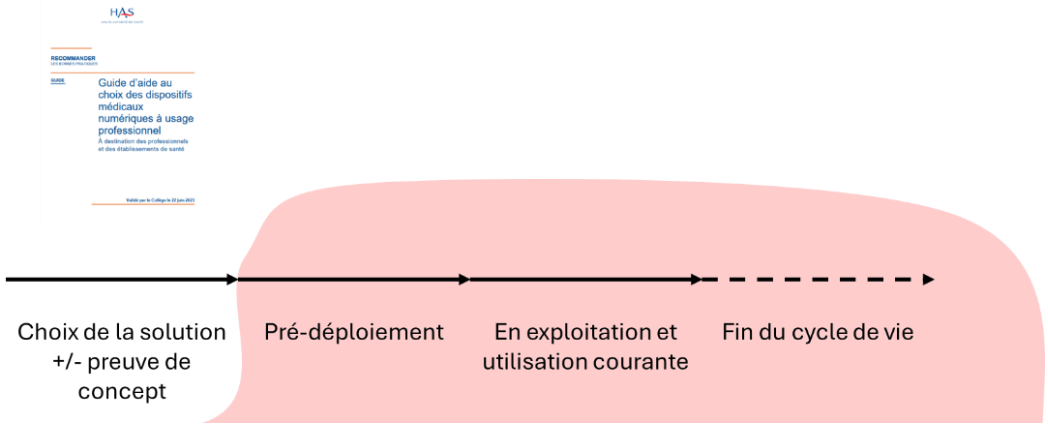

Figure 1 : Périmètre des recommandations – Version provisoire avant mise en forme

Ainsi, ces recommandations s'adressent en priorité :

- au secteur sanitaire, où l'usage des SIA est aujourd'hui le plus développé et encadré. Néanmoins, de nombreux principes présentés ici sont susceptibles d'être pertinents pour le secteur médico-social ou social (accompagnement des personnes âgées, du handicap, aide à l'autonomie, etc.). À mesure que l'IA s'intègre dans ces nouveaux champs, il pourra être nécessaire d'adapter les recommandations aux spécificités de chaque contexte, afin d'assurer une appropriation progressive et sécurisée de ces outils par l'ensemble des acteurs concernés ;
- aux déployeurs de SIA en contexte de soins : établissements et professionnels de santé, quel que soit leur lieu d'exercice. Les équipes de soins comme les fonctions de gouvernance et de soutien, telles que la direction, la direction des systèmes d'informations (DSI), le délégué à la protection des données (DPO), l'équipe qualité/gestion des risques sont concernées par ces recommandations.

Ces recommandations ne visent pas les éditeurs (ou fournisseurs[9] de SIA) et ne se substituent pas aux exigences de mise sur le marché, qui sont du ressort des autorités réglementaires compétentes. Au même titre, ces recommandations n'ont pas pour vocation d'imposer de nouvelles obligations au déployeur.

[8] Haute Autorité de Santé, Guide d'aide au choix des dispositifs médicaux numérique à usage professionnel, 2023

[9] Un fournisseur est défini dans le RIA comme « une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, que ce soit à titre onéreux ou gratuit »

Cas spécifique des établissements développant des SIA « maison » ou « in-house »

Les articles 5.5 des Règlement UE 2017/745 (RDM) et UE 2017/746 (RDIV) relatifs aux dispositifs médicaux et dispositifs médicaux de diagnostic in vitro introduisent des dispositions spécifiques, sous conditions, valables pour les établissements de santé établis dans l'Union européenne fabriquant et utilisant des DM ou DMDIV pour les besoins spécifiques d'un groupe cible de patients non satisfaits par un dispositif équivalent disponible sur le marché. Ces DM ou DMDIV « in-house » peuvent être des SIA ou des adaptations de SIA à usage général pour une utilisation non prévue par le fournisseur initial. Ces établissements ont à la fois le statut de déployeur et de fournisseur au sens du RIA : il est notamment prévu que l'établissement endosse la responsabilité de fournisseur ou a minima que les obligations et la responsabilité soient partagées.

Ainsi, à l'exception des dispositifs « in house » précités et de ceux destinés à des investigations cliniques, un SIA ayant une finalité médicale au sens du RDM et du RDIV peut être utilisé en routine par un établissement de santé sans marquage CE uniquement s'il entre dans un des cadres strictement encadrés (article 5.5 du RDM ou RDIV)

Dans tous les autres cas, un marquage CE est nécessaire avant usage clinique.

Au final, ces recommandations sont destinées à être directement mobilisables par les professionnels de santé, établissements de santé ou structures d'exercice libéral.

Une extension à d'autres cas d'usage ou profils d'acteurs, notamment du secteur social et médico-social, devra être envisagée, au fur et à mesure de l'évolution du cadre juridique et des pratiques.

Structuration des recommandations

Identification des thématiques

L'introduction d'un SIA implique de réinterroger certains fondements organisationnels, notamment en matière de responsabilité, d'information du patient, d'interprétation des résultats ou encore d'articulation entre humain et technologie. Le déploiement des SIA n'est jamais neutre : il modifie les chaînes décisionnelles, transforme les organisations et les usages, et nécessite une réflexion collective sur leurs modalités d'intégration.

L'utilisation en routine d'un SIA implique la mise en œuvre de stratégies complémentaires pour sécuriser les usages, renforcer les compétences et structurer la gouvernance.

La nécessité de disposer de recommandations a été identifiée, à partir des retours d'expériences terrain, des remontées de l'écosystème (professionnels de santé, établissements de santé, industriels, etc.), de l'analyse juridique et de la littérature scientifique, pour 11 thématiques regroupées en différentes catégories correspondant aux différentes phases de déploiement et d'utilisation des SIA dans les soins.

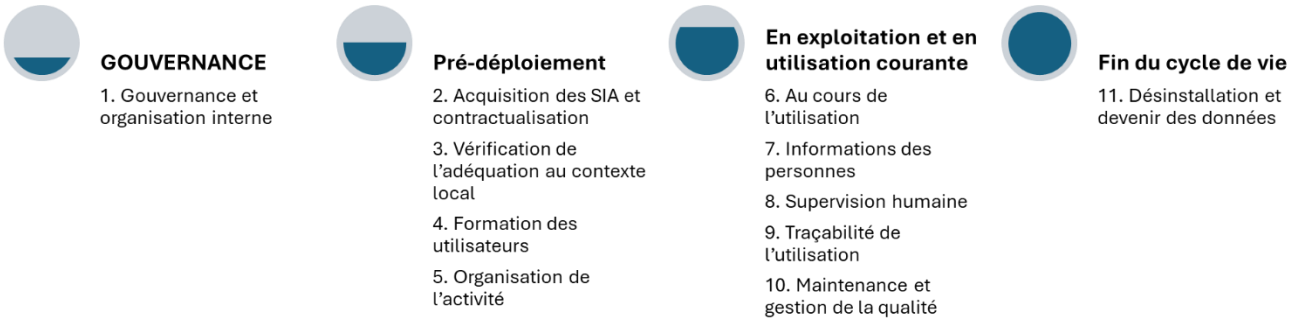

Figure 2 : Structuration des recommandations par thématiques – Proposition de schéma provisoire

La « Gouvernance » regroupe l'ensemble des actions devant être portées au niveau institutionnel dans la structure de soins.

Pour chaque thématique, plusieurs recommandations sont formulées.

Hiérarchisation des recommandations

Afin de favoriser une appropriation effective par les professionnels et les établissements des recommandations, une classification graduée en quatre niveaux est proposée selon leur impact direct sur la qualité et la sécurité des soins. Cette hiérarchisation permet de distinguer :

- les obligations légales, devant impérativement être mises en œuvre ;
- des recommandations standards, qui doivent être appliquées dans la majorité des contextes ;
- des recommandations avancées, destinées aux établissements et professionnels souhaitant mettre en œuvre des exigences renforcées pour sécuriser leurs usages. Ces recommandations sont optionnelles ;
- les réflexes à adopter systématiquement.

Les recommandations de ce guide visent à accompagner les établissements et les professionnels dans la construction d'une démarche structurée d'intégration des SIA et d'optimisation de leurs usages. Cette structuration a pour objectif d'offrir un cadre adaptable, tenant compte du fait que le niveau de maturité organisationnelle varie fortement selon les acteurs : certains établissements hospitaliers disposent déjà d'une organisation avancée pour l'intégration de l'IA, tandis que d'autres structures, notamment en exercice libéral ou en secteur médico-social, entament cette démarche.

En reconnaissant cette diversité, les recommandations cherchent à accompagner avec agilité tous les professionnels et établissements, en s'ajustant aux spécificités et aux réalités concrètes de chaque contexte d'exercice.

Il est toutefois rappelé que la structure qui décide de l'utilisation d'un SIA dans un contexte de soins devra respecter les obligations légales et réglementaires qui lui incombent, comme le professionnel utilisateur. À titre d'exemple, ces structures seront qualifiées de responsables des traitements de données personnelles liés à l'utilisation de SIA. Au même titre, un professionnel de santé exerçant en libéral est responsable du ou des SIA qu'il décide d'utiliser et doit respecter les obligations associées.

Chaque recommandation thématique est qualifiée selon le niveau suivant :

Niveau	Pictogramme associé	Définition	Conséquences attendues
Obligation légale		Obligation issue d'un texte législatif ou réglementaire en vigueur (ex. : RGPD, RIA, code de la santé publique).	Doit impérativement être mise en œuvre. Le non-respect peut entraîner des conséquences juridiques, administratives ou contentieuses.
Recommandation standard	★★★	Recommandation consensuelle, fondée sur les données probantes, les retours du terrain et les principes de qualité et de sécurité.	Devrait être appliquée dans la majorité des contextes. Peut servir de référence en cas d'audit, de certification ou de contentieux.
Recommandation avancée	★☆☆	Pratique identifiée à partir des retours d'expérience et recommandée en fonction de la faisabilité locale.	Peut être appliquée selon les ressources et l'organisation. Sert de levier d'amélioration continue ou d'anticipation.
Les réflexes à adopter systématiquement		Comportements ou configurations identifiés comme inappropriés, dangereux, ou non conformes.	Leur maintien expose à des risques, soit pour la qualité et la sécurité des soins, soit pour la conformité légale.

Cette hiérarchisation vise à établir une doctrine harmonisée à l'échelle nationale, tout en restant adaptable aux contextes cliniques, organisationnels et technologiques locaux. Elle constituera également un repère pour les cycles de certification, les politiques internes relatives à la qualité et la mise en œuvre des obligations du RIA.

1. Organisation interne et gouvernance

La maîtrise institutionnelle du déploiement des SIA est indispensable pour assurer le bon usage de ces technologies, autant par un établissement qu'un professionnel de santé. Cette maîtrise n'est possible qu'en mobilisant l'ensemble des parties prenantes concernées (par exemple, dans le cadre d'un établissement de santé : direction, professionnels de santé, ingénieurs biomédicaux, informaticiens, juristes, délégué à la protection des données, responsable de la sécurité des systèmes d'information, représentants des usagers, etc.), sous l'impulsion du responsable de l'établissement de santé ou de la structure d'exercice libéral.

Quel que soit le contexte d'exercice, chaque déployeur doit assumer cette responsabilité et veiller à la conformité et à la sécurité de l'utilisation des SIA en contexte de soins.

Cadre légal et réglementaire - Rappel

Le cadre juridique rend indispensable l'instauration d'une gouvernance adaptée pour garantir que le déploiement et le suivi d'un SIA répondent aux obligations du déployeur. Ces obligations varient selon le niveau de risque du SIA[10]. À ce titre, l'article 26 du RIA impose aux déployeurs de SIA à haut risque un certain nombre d'obligations spécifiques qui impliquent la mise en place d'une organisation interne structurée. Parmi ces obligations, figurent notamment :

- la mise en place de mesures techniques et organisationnelles garantissant une utilisation conforme à la destination d'usage du SIA et à la notice d'utilisation établie par le fournisseur ;
- la vérification que les personnes chargées du contrôle humain disposent des compétences, de la formation, de l'autorité et du soutien nécessaire à l'exercice de leur mission ;
- la réalisation de contrôles sur les données utilisées pour le fonctionnement d'un SIA (données d'entrée) afin de s'assurer qu'elles sont pertinentes et suffisamment représentatives ;
- la surveillance du fonctionnement du SIA à haut risque, sur la base des indications fournies dans la notice d'utilisation ;
- l'information du fournisseur et de l'autorité compétente s'il considère que le SIA présente un risque pour la santé, la sécurité ou pour les droits fondamentaux des personnes ou s'il a détecté un incident grave ;
- la réalisation d'une analyse d'impact sur les droits fondamentaux (AIDF) prévue à l'article 27 du RIA pour les déployeurs de droit public ou fournissant des services publics.

Lorsque l'utilisation d'un SIA implique le traitement de données personnelles, le responsable de traitement est, par ailleurs, tenu de :

- réaliser une analyse d'impact relative à la protection des données (AIPD[11]), le cas échéant ;
- tenir un registre des traitements mis en œuvre (article 30).

Il est précisé que le responsable de traitement sera dans la majorité des cas le déployeur du SIA pour les traitements de données personnelles liées à son utilisation.

[10] cf. Annexe 1 pour plus de détails sur la classification des SIA selon leur niveau de risque, telle que retrouvée dans le Règlement européen sur l'IA.

[11] Article 35 du RGPD

Les SIA à haut risque, dont les DM, sont soumis à l'obligation d'obtenir un marquage CE au sens du RIA avant leur mise sur le marché. Ce marquage CE n'exonère pas les déployeurs de leur obligation de mettre en place une surveillance locale et continue du système en conditions réelles d'utilisation, conformément à l'article 26 du RIA. En d'autres termes, le marquage CE ne dispense pas le déployeur d'un devoir de vigilance in situ.

En synthèse, quelles sont les obligations du déployeur ?

- mettre en place une gouvernance adaptée ;
- tenir un registre des traitements en application de l'article 30 du RGPD ;
- réaliser une AIPD en application de l'article 35 du RGPD ;
- réaliser une AIDF, le cas échéant, en application de l'article 27 du RIA ;
- informer les autorités de surveillance en cas d'incidents ou dysfonctionnements.

Recommandations sur les principes de fonctionnement de la gouvernance

Recommandation 1.1. Gouvernance de l'IA

★★★

Afin d'assurer un déploiement maîtrisé et conforme des SIA en santé, il est **recommandé que chaque structure de soins – publique, privée, libérale ou territoriale – mette en place une gouvernance de l'IA claire et structurée**. Cette gouvernance constitue le socle stratégique et opérationnel d'un usage responsable des SIA, garantissant à la fois la sécurité des usages, la traçabilité des responsabilités, l'alignement réglementaire, l'acculturation des professionnels et la transparence à l'égard des patients. Cette gouvernance doit être adaptée en fonction de la structure et de ses ressources :

- pour **les établissements de grande taille** (CHU, ESPIC de référence, etc.), un **comité pluridisciplinaire dédié à l'IA**, rattaché par exemple à la direction générale ou à une cellule innovation, peut être constitué. Ce comité doit notamment inclure professionnels de santé, juristes, ingénieurs biomédicaux, experts en application/intégration SIH et experts en sécurité des systèmes d'information (notamment le RSSI), représentants des usagers et, lorsque disponibles, un référent éthique et le DPO. Ce comité devrait notamment définir la stratégie IA, évaluer les projets, valider les cas d'usage, suivre la performance des SIA et organiser la transparence vis-à-vis des usagers (ex. : portail, comptes-rendus).
- pour **les établissements de taille intermédiaire et/ou les structures privées isolées**, la **nomination d'un référent IA** peut être envisagée (clinicien, cadre, qualiticien, etc.). Ce référent IA peut par exemple être chargé de centraliser les initiatives relatives à l'IA, en lien avec les instances existantes (CME, DSI, qualité, CDU, etc.) et le DPO.
- pour **les professionnels exerçant en structure libérale**, la **responsabilité du déploiement et de la gestion des SIA leur incombe directement**. Il n'est pas nécessaire de mettre en place une gouvernance formelle, sauf s'ils choisissent éventuellement de déléguer certaines tâches, mais la responsabilité finale reste la leur. Ainsi, même si l'organisation diffère de celle de structures de grandes tailles, les exigences réglementaires et les principes de vigilance s'appliquent pleinement.

Recommandation 1.2. Mutualisation des réflexions sur un territoire/groupe (GHT, etc.)

★☆☆ Il est recommandé que les Groupements hospitaliers de territoire (GHT) ou groupes privés **adoptent une réflexion, des comités et des outils communs**, afin d'harmoniser les pratiques et d'accompagner les établissements les moins dotés, et au besoin, mutualisent certaines expertises. Les GHT peuvent par exemple s'appuyer sur un établissement support pour la mise en place de cette gouvernance. Au même titre, il est préconisé de solliciter les instances professionnelles ou institutionnelles locales (ex. : URPS, CPTS, GRADES, Conférence régionale de la santé et de l'autonomie), notamment en cas d'exercice isolé, afin d'assurer à l'échelle locale la pertinence de certains déploiements de SIA et de soutenir le cas échéant, l'appropriation des bonnes pratiques par tous les acteurs, quels que soient leur contexte d'exercice ou leurs ressources.

Recommandation 1.3. Appui sur les CNP et sociétés savantes

★★★ Par ailleurs, il est recommandé que l'ensemble des structures et des professionnels **s'appuient sur les conseils nationaux professionnels (CNP), sociétés savantes, ordres professionnels et tout autre acteur pertinent**, afin de disposer de référentiels et socles communs, de modèles d'information patient et de grilles d'évaluation. À ce titre, ces référentiels devront intégrer explicitement les spécificités des structures de médecine libérale, des cabinets de groupe et des petites organisations de soins.

Recommandations sur les actions à porter par la gouvernance

Recommandation 1.4. Cartographie des SIA

★★★ Il est recommandé que la première mission de toute gouvernance IA soit la **mise en œuvre d'une cartographie des SIA** utilisés ou en projet ; cette cartographie doit être dynamique et mise à jour au moins annuellement. En effet, si le RIA ne prévoit pas directement cette cartographie, la détermination des obligations découlant de l'usage de SIA nécessite d'identifier les SIA utilisés au sein d'une structure.

Cette cartographie **doit inclure notamment, pour chaque outil** :

- son nom et sa version ;
- le nom du fournisseur ;
- une description générale du SIA et de ses fonctionnalités ;
- ses finalités (clinique, organisationnelle, etc.) ;
- son statut réglementaire (dispositif médical ou non) et les textes applicables ;
- son niveau de risque en vertu de la classification RIA ;
- son niveau de déploiement (ex. : pilote, usage courant) ;
- les services utilisateurs ;
- l'identité du référent local ;
- le niveau de criticité du SIA pour l'organisation des soins et la prise en charge des patients ;
- les catégories de données nécessaires au fonctionnement du SIA ;
- les catégories de personnes susceptibles d'être concernées et, si possible, une approximation du nombre de personnes concernées par l'usage (ex. sur un an) ;
- les modalités de suivi (indicateurs, incidents, traçabilité, retour d'expérience, etc.).

Cette cartographie constitue le socle afin d'identifier l'ensemble des actions à conduire par la gouvernance. Elle doit intervenir en priorité pour les SIA ayant un impact direct sur les soins et la prise en charge des patients, et dans un second temps au besoin, également pour les SIA embarqués ou intégrés depuis longtemps au sein du matériel biomédical, par exemple pour améliorer l'acquisition d'images.

Par ailleurs, il est recommandé que cette cartographie soit :

- exploitée comme un outil d'analyse des risques, servant de base à l'orientation des politiques d'usage, d'information des patients, de supervision humaine et de conformité ;
- mutualisée avec celle du SIH et soit articulée avec la gouvernance des données et la documentation interne prévue par le RGPD (registre des traitements, AIPD).

Recommandation 1.5. Guichet unique pour les SIA/projets innovants

★★★ Il est recommandé de structurer à l'échelle d'un établissement, le cas échéant d'un GHT, ou d'une structure d'exercice libéral un **guichet unique** visant à :

- centraliser l'ensemble des propositions de projets innovants à l'échelle d'une structure ;
- permettre la sélection éclairée des projets par un comité adapté et maîtriser leur déploiement dans le respect des bonnes pratiques ;
- alimenter au fil de l'eau la cartographie.

Ce guichet unique peut par exemple, pour sa forme la plus simple, consister en une adresse électronique unique, dédiée aux sollicitations des entreprises et aux demandes internes.

Recommandation 1. 6. Validation institutionnelle

★★★ Il est recommandé que chaque SIA soit déployé après une **validation institutionnelle**, avec un responsable clinique ou technique identifié, et en prévoyant un dispositif de suivi à moyen terme (indicateurs, traçabilité, revue régulière). À cette fin, la gouvernance doit mettre en place les actions suivantes pour chaque SIA :

- vérifier la conformité réglementaire des SIA (notamment ceux à haut risque) ;
- s'articuler avec les vigilances réglementaires : matériovigilance, cybersécurité, protection des données, etc. ;
- être transparente sur les critères de sélection, les justifications cliniques et éthiques (si applicable) des outils retenus, en les partageant avec les équipes concernées pour favoriser la confiance, la compréhension et l'appropriation des SIA ;
- développer une dynamique d'acculturation : sensibilisation, formation, intégration dans les parcours de développement professionnel continu, etc. ;
- mettre en place un mécanisme d'alerte ou de recours (ex. : comité d'éthique interne, cellule qualité ou direction médicale) mobilisable lorsqu'un professionnel identifie qu'un SIA engendre une altération de la qualité et/ou de la sécurité des soins, ou constate un conflit entre recommandations algorithmiques et jugement clinique. Afin de faire le lien avec la gestion des plaintes et réclamations par la Commission des usagers, un bilan annuel de ce mécanisme d'alerte ou de recours (nombre de signalements concernant un SIA, résolutions et mesures déployées) peut être partagé au sein de l'établissement ;
- vérifier auprès de son assureur que l'usage de SIA est bien couvert par son contrat et informe explicitement les professionnels concernés des éventuelles conditions ou exclusions de garantie spécifiques liées à l'utilisation de SIA.

Recommandations à destination des directions

Recommandation 1. 7. Portage de la direction de la structure

★★★

La mise en place d'une gouvernance dédiée à l'IA doit être **portée par la direction générale** de l'établissement. À ce titre, il est recommandé de l'intégrer à la stratégie de l'établissement, en lui assurant un portage institutionnel fort, et en mobilisant les leviers budgétaires nécessaires.

Recommandation 1.8. Démarche RSE

★★★

Par ailleurs, l'intégration croissante des SIA dans une organisation, bien que potentiellement vectrice d'innovations majeures, impose une gestion rigoureuse des risques éthiques, sociaux et environnementaux. **L'adoption d'une démarche de Responsabilité Sociale des Entreprises (RSE) structurée et outillée** est, dans ce contexte, un levier fondamental de sécurisation et de performance éthique qui doit être encouragée. Elle doit notamment impliquer la sollicitation des organisations syndicales et représentants du personnel. Ce type de démarche vise à prendre une place de plus en plus importante, notamment en raison de la jurisprudence récente[12] concernant la non-information auprès des employés de l'usage d'un SIA.

[12] TJ Nanterre, référé, 14 février 2025, n° 24/01457 et TJ Créteil, référé, 15 juillet 2025, n° 25/00851

2. Acquisition des SIA et contractualisation

La contractualisation avec le fournisseur permet de :

- **vérifier la conformité réglementaire du SIA** ;
- **formaliser et clarifier plusieurs éléments essentiels** : chaînes des responsabilités, transparence sur les performances et le devenir des données à caractère personnel, etc ;
- in fine, **préciser les actions et obligations devant être réalisées par la structure de soins et les professionnels** pour gérer la qualité et le risque en mettant en responsabilité selon les cas le fournisseur du SIA et l'établissement ou le professionnel utilisateur.

Les recommandations suivantes n'ont pas vocation à se substituer aux procédures d'achat, exigences et bonnes pratiques habituelles, mais à faciliter l'identification des éléments à prendre en compte lors de la contractualisation. Ces recommandations ont également vocation à permettre aux structures de soins de répondre à leurs obligations, notamment s'agissant des traitements de données personnelles liés à l'utilisation d'un SIA dont elles seront responsables.

Cadre légal et réglementaire - Rappel

Le RIA ne prévoit pas de cadre contractuel spécifique entre le fournisseur et le déployeur permettant de définir clairement les obligations respectives de chaque partie l'une envers l'autre. Néanmoins celui-ci impose dans certains cas aux déployeurs de réaliser une analyse d'impact sur les droits fondamentaux, ou AIDF (article 27). La réalisation de cette analyse suppose de recueillir au préalable certaines informations sur le SIA dont l'utilisation est envisagée.

Lorsque l'utilisation d'un SIA implique le traitement de données à caractère personnel, un encadrement contractuel sera requis :

- en cas de sous-traitance[13] (par exemple avec le fournisseur ou le prestataire d'hébergement des données) en application de l'article 28 du RGPD. Sur ce point, il est rappelé que le responsable de traitement (le déployeur du SIA) devra s'assurer, avant la conclusion du contrat et pendant toute sa durée, que son sous-traitant présente des garanties suffisantes en matière de protection des données ;
- en cas de responsabilité conjointe en application de l'article 26 du RGPD.

Dans certains cas, une analyse d'impact sur la protection des données ou AIPD devra être réalisée par le responsable de traitement[14]. Afin de réaliser cette analyse, il doit disposer de certaines informations concernant les mesures mises en œuvre par ses sous-traitants ou le fournisseur du SIA utilisé.

[13] Voir notamment : Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les données personnelles | CNIL. Les acteurs peuvent également se reporter aux clauses contractuelles types établies par la Commission européenne, sous réserve de prendre en compte les dispositions nationales applicables.

[14] Voir notamment les lignes directrices concernant l'analyse d'impact relative à la protection des données ainsi que les listes des traitements pour lesquels une AIPD est requise ou non élaborées par la CNIL.

En cas d'hébergement des données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi réalisé dans le cadre social et médico-social sur les serveurs d'un tiers (ex. informatique en nuage/cloud), ce dernier devra être certifié hébergeur de données de santé. La prestation réalisée et le contrat conclu devront respecter les obligations imposées à l'article le L. 1111-8 et aux articles R. 1111-8-8 et suivants du code de la santé publique (CSP).

En synthèse, quelles sont les obligations du déployeur ?

- mettre en place une gouvernance adaptée ;
- tenir un registre des traitements en application de l'article 30 du RGPD ;
- réaliser une AIPD en application de l'article 35 du RGPD ;
- réaliser une AIDF, le cas échéant, en application de l'article 27 du RIA ;
- informer les autorités de surveillance en cas d'incidents ou dysfonctionnements.

Il est recommandé de mutualiser, autant que possible, les étapes de contractualisation en s'appuyant sur les outils et procédures existants, afin de limiter les risques et d'optimiser les ressources.

Dans cette logique, les centrales d'achats peuvent jouer un rôle de facilitateur, par exemple via la mise à disposition de modèles de contrats (clausiers de sécurité) ou de cahiers des charges spécifiques aux SIA. Également, ces réflexions devraient être portées à l'échelle des territoires en cas de coopération entres structures (par exemple, à l 'échelle d'un GHT ou Groupements Hospitaliers de Territoire), pour harmoniser les pratiques et faciliter l'accès à des outils contractuels de qualité pour tous les établissements du territoire.

Recommandations sur les prérequis

Recommandation 2.1. Contrat avec information claire, accessible et documentée

★★★

Lors de **la contractualisation avec un fournisseur de SIA,** différents prérequis sont indispensables à la transparence sur le SIA et à son bon usage dans le contexte d'utilisation envisagé. Il est recommandé que le **contrat contienne une information élaborée par le fournisseur/fabricant, claire, accessible et documentée** sur :

- la finalité ou destination d'usage du SIA, le cas échéant (ex., « aide à la détection de nodules pulmonaires ») ; le statut réglementaire (ex., dispositif médical ou non, classe de risque CE) ;
- le développement du SIA (ex. : les principes algorithmiques, l'origine et la nature des données d'entraînement, les modalités d'évaluation algorithmique, la gestion des biais algorithmiques identifiés et les stratégies d'atténuation prévues, la date de commercialisation) ;
- les performances du SIA (ex. : sensibilité, spécificité, robustesse, etc.) et le contexte de leur validation (ex. : validation interne, validation externe sur des données indépendantes n'ayant pas servi à l'entraînement, validation par l'expérimentation en conditions réelles lors d'une étude clinique). À ce titre, les professionnels ou établissements peuvent vérifier les preuves disponibles pour savoir si le SIA a été validé sur une population équivalente à celle dans laquelle le SIA sera déployé ;
- les limites et biais connus du SIA ;

- une description précise des populations de patients éligibles à l'utilisation du SIA, des populations de patients pour lesquelles les performances du SIA ont été testées et validées, et les populations de patients pour lesquelles le SIA n'est pas validé (ex. : « le SIA ne doit pas être utilisé chez les moins de 18 ans car les performances n'ont pas été vérifiées ») ;
- le principe de fonctionnement compréhensible par les utilisateurs, pour limiter l'effet « boîte noire » ;
- les dispositions minimales de contrôle humain à mettre en œuvre par le déployeur ;
- la mise à disposition par le fournisseur d'un accompagnement à la formation des utilisateurs initiaux pouvant aller jusqu'à un objectif d'habilitation à l'usage du SIA (a minima, via la mise à disposition de supports de formation, avec un contrôle des connaissances acquises), mais également pendant toute la durée de l'exploitation du SIA (en cas de mise à jour du SIA, etc.) ;
- les éléments nécessaires au fonctionnement du SIA (données nécessaires, infrastructure(s) technique(s), etc.) et sa capacité à fonctionner dans un environnement dégradé ;
- les procédures en cas de dysfonctionnement ou d'incident (par exemple, entraînant une vigilance sanitaire ou une violation de données) ;
- une information concernant les flux de données et les moteurs algorithmiques utilisés, notamment tiers utilisés par le SIA. Dans le contexte où de plus en plus de SIA s'appuient sur des interfaces de programmation applicative (API) tierces, la description claire du circuit complet des flux de données est essentielle ;
- l'impact environnemental du SIA (coût carbone, etc.).

Ces éléments peuvent être annexés sous forme de dossier technique, en complément de la notice d'utilisation qui doit être claire. Ils sont utiles à la fois pour le professionnel (pour comprendre l'outil, l'utiliser de manière adaptée et lui permettre de délivrer une information adaptée au patient) et pour la gouvernance de la structure en permettant d'établir des spécifications techniques d'installation garantissant le bon fonctionnement du SIA et la définition du bon cadre d'utilisation.

★★★ Recommandation 2.2. Conformité règlementaire

Il est recommandé de s'assurer de la **conformité réglementaire** du SIA, notamment aux Règlements (UE) 2017/745 et 2017/746, au RGPD et au RIA :

- **s'il s'agit d'un SIA ayant le statut de dispositif médical, le SIA doit disposer d'une documentation CE valide dans les situations d'usage prévues**. En effet, l'utilisation d'un SIA avec une finalité médicale au sens des Règlements (UE) 2017/745 et 2017/746, non marqué CE alors qu'il devrait l'être, peut engager la responsabilité de l'établissement ou du professionnel utilisateur ;
- la **conformité au RGPD du SIA**, en demandant au fournisseur la communication de documents démontrant que les mesures mises en œuvre permettent de garantir une conformité au RGPD, le cas échéant d'un certificat d'hébergement HDS (hébergement de données de santé), etc. Le fournisseur, s'il est qualité de sous-traitant, doit par ailleurs permettre au responsable de traitement (le déployeur du SIA) de répondre à ses obligations (ex. : procédure sur l'exercice des droits, flux de données, identification de ses propres prestataires/sous-traitants) ;

Recommandation 2.3. Interopérabilité avec le système d'information existant

★★★ L'intérêt d'un SIA étant dépendant de son intégration au système d'information, il est recommandé de s'assurer de l'interopérabilité du SIA avec le système d'information existant (ex. : dossier patient informatisé ou DPI, système d'information radiologique ou RIS) et d'anticiper les conditions et coûts d'interopérabilité avec le fournisseur. En effet, au-delà de la perte de temps ou d'intérêt engendrée par la non-interopérabilité d'un SIA, celle-ci peut engendrer des risques pour la bonne prise en charge des patients (double saisie, erreurs de transcription). Une cartographie des installations techniques mais également fonctionnelle (avec une identification claire des flux de données) doit être fournie.

> **La contractualisation permet de clarifier les chaînes des responsabilités**
>
> À ce titre, le contrat ne peut déléguer la responsabilité médicale, mais doit :
>
> - préciser les obligations de coopération du fournisseur en cas d'incident ou de violation de données (accès aux logs, transparence technique) ;
> - encadrer les périmètres d'utilisation : si le SIA est utilisé en dehors de sa destination et des conditions générales d'utilisation, la responsabilité du fournisseur ne saurait être engagée ;
> - prévoir une clause d'alerte du fournisseur en cas d'usage inadapté au sein de l'établissement (surveillance mutuelle).

Recommandations sur les clauses contractuelles spécifiques

Des clauses contractuelles spécifiques peuvent permettre de sécuriser les usages.

Recommandation 2.4. Contrat de niveau de service (SLA)

★★★ Ainsi, il est recommandé de prévoir **un contrat de niveau de service** (Service Level Agreement ou SLA) permettant de définir les différentes garanties associées au service et la maintenance prévue, notamment :

- les délais de résolution en cas d'incident (ex. : nombre d'heures pour corriger un incident) ;
- les engagements de disponibilité (ex. : 99,9 % en cas d'outil critique) ;
- les modalités de maintenance et mises à jour : fréquence, notification préalable, validation locale, support technique (assistance, horaires, etc.) ;
- les modalités d'installation et de validation des mises à jour : certaines doivent passer par des bacs à sable, avec contrôle de compatibilité avec l'environnement d'utilisation.

Recommandation 2.5. Période de calibrage

★★★ Il est également recommandé de prévoir une **période de calibrage permettant la validation locale et technique de l'outil** (par exemple dans un environnement de test), avec possibilité de rétractation sans pénalité si l'outil s'avère inadapté à l'environnement dans lequel il est déployé. Les conditions de réalisation doivent être précisées (durée, données concernées, conditions de passage à un déploiement à plus large échelle). La mise en place d'une preuve de concept (POC ou Proof Of Concept) courte (ex. : 1 mois) peut ainsi permettre de vérifier l'intégration technique et recueillir un premier retour utilisateur. À ce titre, l'implication de soignants et de représentants d'usagers et/ou éthiques lors de l'évaluation de la pertinence et de la sécurité des algorithmes à haut impact clinique est importante. Même courtes, ces preuves de concept peuvent être contractualisées.

Recommandation 2.6. Clause de performance

★☆☆ Il est préconisé de prévoir, lorsque cela est pertinent, **une clause de performance**. Par exemple, un engagement contractuel de performance du fournisseur peut permettre de conditionner le paiement à l'atteinte d'un seuil de performance préalablement défini dans le cadre de l'approche de l'achat par la valeur (value-based procurement), notamment en cas de contractualisation avec une start-up ou une PME.

Recommandation 2.7. Conditions de fin de contrat

★★★ Il est recommandé d'anticiper les **conditions de fin de contrat, notamment de réversibilité des données**, pour s'assurer qu'un export des données peut être réalisé pour éviter un enfermement technologique. Notamment, afin de :

- prévoir la restitution des données permettant l'exploitation effective des données migrées ;
- prévoir la certification de suppression des données hébergées chez le fournisseur ;
- définir les modalités de sortie propre en cas de rupture anticipée ou changement de solution.

Recommandation 2.8. DPO associé dès que possible

★★★ L'utilisation de SIA dans le contexte de soins peut impliquer le traitement de données à caractère personnel concernant notamment les patients et/ou les professionnels participant à la prise en charge. Dans cette hypothèse, il est recommandé que le **DPO soit associé dès que possible afin d'accompagner l'organisme**.

Focus sur le traitement de données personnelles et leur réutilisation

Le contrat avec le fournisseur doit préciser :

- la répartition des rôles et responsabilités entre le fournisseur et le déployeur (établissement ou professionnel de santé) au sens du RGPD. Dans la majorité des cas, l'établissement ou le professionnel de santé ayant décidé de recourir à un SIA sera qualifié de responsable de traitement ;
- les catégories de données à caractère personnel nécessaires pour le fonctionnement du service ainsi que celles qui ne sont pas nécessaires lors de l'utilisation d'un SIA (ex. : les données d'identité du patient, l'identité nationale de santé).

En complément, si le fournisseur peut être qualifié de sous-traitant de données personnelles :

- des éléments sur la prestation du fournisseur et le traitement de données concerné ;
- une clause de confidentialité spécifique applicable au fournisseur et à son personnel habilité, adaptée à la sensibilité des données et leur protection (par exemple, les données couvertes par le secret professionnel) ;
- les mesures techniques et organisationnelles mises en œuvre par le fournisseur afin de garantir la sécurité des données et les conditions de modification de ces mesures ;
- si le fournisseur peut faire appel à des sous-traitants ultérieurs et selon quelles conditions (autorisation préalable du responsable de traitement ou information préalable de celui-ci dans un délai lui permettant de s'y opposer le cas échéant).

- **Un point de vigilance important concerne le recours à des sous-traitants (y compris des sous-traitants ultérieurs) soumis à un droit extra-européen**, notamment en cas de recours à un service d'informatique en nuage (ou « cloud »). À ce titre, il est recommandé de **demander au fournisseur la liste des sous-traitants auxquels il fait appel ainsi que leur lieu d'établissement. La transmission de cette information constitue une obligation pour les hébergeurs de données de santé, qui sont également tenus de stocker les données sur le territoire de l'Espace économique européen** ;
- les mesures envisagées pour donner suite aux demandes d'exercice des droits des personnes concernées ;
- les possibles réutilisations des données (traitées initialement pour le fonctionnement du SIA) par le fournisseur pour son propre compte. Ces réutilisations supposent l'accord écrit et préalable du responsable de traitement. À ce titre, il recommandé que le contrat indique **la liste précise et limitative des finalités** pour lesquelles une réutilisation des données par le fournisseur et/ou ses éventuels sous-traitants pourraient intervenir ainsi que tout élément permettant à l'établissement ou au professionnel de santé de garantir que cette/ces finalité(s) est/sont compatible(s) avec la finalité pour laquelle elles sont initialement traitées. Ces informations sont à mettre à jour régulièrement.

NB : toute réutilisation secondaire des données (apprentissage, annotation, étude, etc.) constitue un traitement de données personnelles distinct devant être conforme aux textes applicables (RGPD et la loi « informatique et libertés »). Les acteurs peuvent se reporter aux contenus publiés par la CNIL concernant l'IA et le secteur de la santé.

Ces recommandations s'appliquent aux achats de SIA mais certaines IA peuvent être intégrées dans des équipements ou logiciels déjà présents au sein de l'établissement, sans achat supplémentaire dédié (ex. : échographe avec un module IA). Ainsi, il est essentiel d'alerter les services (notamment achats, biomédicaux, comme informatiques/numériques) et de préciser dans les appels d'offre que toute composante IA devra faire l'objet :

- d'un signalement explicite par le fournisseur ;
- d'une évaluation transparente par la structure souhaitant utiliser le SIA ;
- d'une conformité avec les critères réglementaires applicables.

Les réflexes à adopter systématiquement :

Il est conseillé **de ne pas contractualiser** avec un fournisseur si :

- la conformité réglementaire pour l'usage prévu ne semble pas assurée ;
- les principes de fonctionnement, d'explicabilité ou d'apprentissage du SIA restent opaques pour l'établissement ou le professionnel utilisateur ;
- il n'existe pas de preuves de validation dans la population d'usage prévu ;
- le circuit des données n'est pas clairement explicité.

3. Vérification de l'adéquation au contexte local

Le déploiement d'un SIA dans un nouvel environnement peut nécessiter :

- la **vérification des performances du SIA dans l'écosystème d'utilisation local** ;
- la **validation de son bon positionnement dans l'organisation des soins du lieu de déploiement**, au regard des usages prévus par le concepteur (pré-tri, aide en temps réel, etc.).

Cette étape est d'autant plus importante dans les cas où le SIA n'a pas fait l'objet d'une validation externe sur un jeu de données indépendant.

Cadre légal et réglementaire - Rappel

Le RIA n'impose pas au déployeur de mettre en place un contrôle des performances du SIA en amont du son déploiement. Toutefois des phases de test sont fortement recommandées notamment afin de vérifier l'adéquation du SIA au contexte d'une structure et au positionnement parcours de soins des personnes. Ces tests doivent, dans la mesure du possible, être effectués dans un environnement informatique distinct de celui de la production et sur des données fictives ou anonymisées[15]. Ces tests doivent par ailleurs être distingués des essais en conditions réelles visés par le RIA[16], qui ne seront pas abordés dans ce guide.

Les recommandations présentées ci-dessous peuvent conduire le déployeur à traiter des données personnelles de santé pour une autre finalité que la prise en charge de leurs patients. Ces traitements pourront être soumis au régime de formalités préalables auprès de la CNIL prévu aux articles 65 et suivants de la loi « informatique et libertés »17.

En synthèse, quelles sont les obligations du déployeur ?

- mettre en place une gouvernance adaptée ;
- tenir un registre des traitements en application de l'article 30 du RGPD ;
- réaliser une AIPD en application de l'article 35 du RGPD ;
- réaliser une AIDF, le cas échéant, en application de l'article 27 du RIA ;
- informer les autorités de surveillance en cas d'incidents ou dysfonctionnements.

★★★ Recommandation 3.1. Vérification de l'adéquation au besoin

Il est recommandé d'effectuer au minimum une **vérification de l'adéquation au contexte local avant l'utilisation effective du SIA et son déploiement en routine clinique**[18].

[15] https://www.cnil.fr/fr/securite-encadrer-les-developpements-informatiques

[16] Il s'agit des essais en conditions réelles réalisés dans le cadre d'un bac à sable réglementaire ou non (article 58 et 60 du RIA)

[17] voir : Formalités préalables | CNIL

[18] PS : il ne s'agit pas ici de réaliser des évaluations médico-techniques complètes du SIA mais bien de réaliser une vérification pragmatique, adaptée aux ressources de chaque établissement, des performances du SIA et de son intérêt.

Même pour des SIA ayant le statut de DM ou de DM-DIV et donc marqués CE selon le RDM/RDIV ou des SIA non-DM dont l'usage est largement répandu, un contrôle local reste pertinent afin d'identifier d'éventuels biais spécifiques à la population ou à la configuration technique locale. Ce contrôle peut prendre différentes formes, selon la taille et les ressources des établissements ou des utilisateurs. Il est recommandé d'effectuer a minima un test d'utilisation sur un jeu de données local présentant des cas représentatifs de la population de patients (en matière de genres, de tranches d'âges, etc.) et sur des cas cliniques atypiques (par exemple sur des maladies rares). Ce test d'utilisation permet de vérifier que le SIA répond bien aux besoins identifiés. Chaque fois que cela est possible, il est recommandé de **standardiser les tests réalisés** en fonction du type de SIA afin de pouvoir les répliquer si nécessaire (par exemple après une mise à jour conséquente du modèle).

Ces tests d'utilisation peuvent être réalisés au sein de sites pilotes lors du déploiement à large échelle d'un SIA (par exemple, au sein d'un service pour un établissement ou au sein de l'établissement support pour un GHT). Certains organismes (notamment certains CNP) ou certaines structures locales (par exemple, tiers lieux d'expérimentations ou établissements de santé) pourront jouer un rôle pour tester les SIA ou proposer des jeux de données à tester selon les indications du SIA.

Dans le cas d'un modèle d'IA non figé et auto-apprenant, il est recommandé que ces contrôles soient réalisés de manière régulière afin d'identifier une éventuelle dérive algorithmique.

★★★ Recommandation 3.2. Bilan du déploiement et de l'utilisation

En complément, il est recommandé de **mettre en place un bilan du déploiement et de l'utilisation, pour vérifier que le SIA correspond bien au besoin auquel il est censé répondre**. Ce bilan peut prendre différentes formes, par exemple par retour d'expériences avec les utilisateurs afin d'identifier des éventuels décalages populationnels, des nombres importants de faux positifs ou faux négatifs, des risques d'usages inadaptés du SIA. Ce retour d'expériences doit inclure le repérage des contournements suspectés ou avérés d'utilisation du SIA (autrement dit, une utilisation du SIA pour d'autres usages que ceux prévus). Ces bilans sont d'autant plus intéressants qu'ils sont mutualisés ou partagés, notamment aux professionnels ne possédant pas des ressources ou d'un nombre de patients suffisant pour réaliser de tels bilans.

★☆☆ Recommandation 3.3. Évaluations scientifiques

Des **évaluations scientifiques dans le domaine de la santé, avec une méthodologie adaptée**, sont également encouragées afin d'objectiver l'intérêt clinique et/ou organisationnel du SIA. Ces évaluations, plus chronophages en temps et en ressources humaines, peuvent correspondre à :

- une validation à large échelle sur l'ensemble des données historiques disponibles pour évaluer, par exemple, les taux de faux positifs et de faux négatifs ;
- la mise en œuvre d'une étude en vie réelle prospective impliquant la collecte de données permettant de documenter la performance en vie réelle ou l'intérêt, qu'il soit clinique, organisationnel ou économique.

Selon le type d'approche choisi, ce bilan peut être effectué dans un environnement informatique distinct de celui de la production. Pour les structures de soins n'ayant pas la capacité de mettre en place ces évaluations, il est recommandé de s'appuyer sur les publications scientifiques, documentations et retours d'expérience existants au sein d'autres établissements, voire via un conventionnement avec un établissement disposant des compétences.

4. Formation et acculturation des professionnels

La formation et l'acculturation des professionnels constituent des leviers essentiels pour garantir un usage éclairé et sécurisé des SIA dans les pratiques cliniques.

L'introduction de ces technologies impose de repenser les compétences initiales et continues des équipes, en visant à établir une culture partagée de l'IA entre professionnels de santé, et le cas échéant, au sein des établissements de santé. Les recommandations suivantes définissent les modalités concrètes, les publics concernés, les contenus pédagogiques et les exigences de traçabilité à mettre en œuvre, afin de permettre aux professionnels de maîtriser pleinement les enjeux et les responsabilités associés à l'utilisation des SIA.

Cadre légal et réglementaire - Rappel

Afin de garantir une utilisation responsable et éclairée des SIA, quel que soit leur niveau de risque, les fournisseurs et les déployeurs sont tenus, en vertu de l'article 4 du RIA, de s'assurer que leur personnel ainsi que toute personne agissant en leur nom disposent d'un niveau suffisant de connaissances en matière d'IA. **Selon la Commission européenne, il s'agit d'un pilier essentiel de la gouvernance de l'IA**[19].

Elle vise à s'assurer que toutes les personnes au sein de l'organisation qui interagissent avec ces systèmes disposent des compétences, connaissances et compréhension adéquates du ou des SIA utilisés. Il convient de souligner que, selon la Commission européenne, aucune obligation formelle de mesurer les connaissances des travailleurs n'est imposée dans le cadre de cet article 4.

Le Bureau de l'IA de la Commission européenne, organe responsable de la mise en œuvre du RIA, n'imposera pas d'exigences strictes en matière de formation. Toutefois, celle-ci devrait a minima permettre :

- d'assurer une compréhension générale de l'IA au sein de l'organisation ;
- de clarifier le rôle de l'organisation, qu'elle soit fournisseur ou utilisatrice de SIA ;
- de prendre en compte les risques associés aux SIA fournis ou déployés ;
- de concevoir des actions de maîtrise de l'IA adaptées, en tenant compte du niveau de connaissance des employés et du contexte d'utilisation des SIA au sein de l'organisation.

À ce titre, une structure de soins ou un établissement déployant un SIA doit s'assurer que l'ensemble de son personnel possède un niveau de connaissance minimal sur l'IA.

Il s'agit d'un élément essentiel afin que le déployeur et les personnes placées sous son autorité soient notamment en mesure de donner suite au droit des personnes à obtenir des explications sur les décisions individuelles prises les concernant grâce à certains SIA.

[19] https://digital-strategy.ec.europa.eu/fr/faqs/ai-literacy-questions-answers

Enfin, les déployeurs de SIA à haut risque sont tenus, conformément à l'article 26 du RIA, de veiller à ce que le personnel en charge de ces systèmes soit suffisamment formé pour en assurer la gestion et la surveillance humaine. **La Commission souligne que le recours à la seule notice d'utilisation ne saurait suffire ; le déployeur devra mettre en place des mesures complémentaires de formation.**

Dès lors que l'utilisation d'un SIA implique le traitement de données personnelles, le responsable de traitement (le déployeur du SIA) est tenu de mettre en place des mesures techniques et organisationnelles appropriées pour protéger les données. Parmi ces mesures, la sensibilisation et la formation de son personnel aux enjeux en matière de sécurité et de vie privée sont centrales.

Enfin, pour rappel, le CSP impose aux professionnels de santé une obligation de formation continue dans le cadre du développement professionnel continu.

En synthèse, quelles sont les obligations du déployeur ?

➔ mettre en place ou participer à des modules de formation sur l'IA en santé et à la protection des données personnelles.

Formation et acculturation générale sur l'IA au sein de la structure

Recommandation 4.1. Premier niveau de formaiton générale à l'IA

★★★

Face à la multiplication des SIA, il est recommandé, en parallèle de la mise en place de formations initiale et continue au numérique pour les professionnels en activité, de mettre en place un **premier niveau de formation générale** à l'IA accessible à tous et pour tout nouvel arrivant. L'objectif est d'atteindre un premier niveau de sensibilisation. Cette formation devrait comprendre à la fois :

- un module généraliste dédié à l'IA afin de diffuser une culture générale et commune de l'IA en santé au sein de l'ensemble des professionnels. Un besoin particulier semble émerger en lien avec l'utilisation d'IA générative et sur les risques liés à l'utilisation de données de patients.
- un module dédié à la protection des données à caractère personnel et au RGPD, les risques liés à leur utilisation et les bonnes pratiques à mettre en œuvre pour limiter ces risques ;
- un module sur la responsabilité médicale, notamment rappelant qu'à l'heure actuelle, la responsabilité du professionnel reste ainsi entière, même lorsque l'acte est accompli avec l'assistance d'un SIA.

Cette acculturation générale peut prendre différentes formes : conférences internes, ateliers multi-professionnels, retours d'expériences réguliers, MOOC ou sessions plénières ouvertes à l'ensemble des personnels. Des formations dédiées, organisées par des organismes reconnus se mettent en place et devraient être privilégiées. Une vigilance doit néanmoins être apportée au choix de la formation, face à la multiplication d'une offre de formation de qualité particulièrement hétérogène.

L'implication systématique des équipes dirigeantes et encadrantes dans les actions de sensibilisation est essentielle pour garantir leur soutien aux démarches de formation opérationnelle.

En parallèle de ces formations généralistes, la rédaction d'une charte dédiée à l'IA peut présenter un intérêt pour formaliser l'engagement des professionnels sensibilisés.

Recommandation 4.2. Formations approfondies à l'IA de profils clés

★★★ Il est recommandé de réaliser **des formations approfondies à l'IA auprès des profils clés** (ex. : le délégué à la protection des données ou le responsable du système d'information, le RSSI, le biomédical ou le référent du SIA).

Formation spécifique des utilisateurs du SIA

Recommandation 4.3. Formation obligatoire au préalable de l'utilisation du SIA

★★★ **L'établissement ou la structure de soins déployant un SIA a pour responsabilité juridique d'organiser la formation des utilisateurs (obligation de moyens).** L'accompagnement de l'éditeur est cependant nécessaire (cf. Acquisition des SIA et contractualisation). Ainsi, la mise en place d'une **formation obligatoire au préalable à l'utilisation d'un SIA**, notamment en lien avec la notice d'utilisation du fournisseur et avec ses préconisations, est indispensable pour assurer un usage sécurisé et éclairé. Cette formation pourrait être associée, si l'ergonomie du SIA le permet, à une prise en main progressive de l'utilisation du SIA afin d'assurer la bonne autonomie de l'utilisateur.

Recommandation 4.4. Habilitation au SIA

★☆☆ Pour des SIA ayant un impact important sur la prise en charge des patients, il est recommandé de mettre en place **une habilitation à l'utilisation du SIA.** Une telle habilitation pourrait notamment être **conditionnée à un seuil minimal de réussite** à des cas pratiques ou tests post-formation. **La mise en place de ces habilitations est au libre choix de l'établissement selon les cas d'usages et les risques associés identifiés.**

Recommandation 4.5. Identifier le public cible à former

★☆☆ Avant toute formation, il est recommandé en premier lieu **d'identifier l'impact du SIA sur l'organisation des soins et d'identifier quels profils et métiers auront à interagir,** plus ou moins directement avec le SIA : utilisateurs finaux (médecins, paramédicaux, internes et étudiants), équipes supports (informaticiens, ingénieurs biomédicaux, qualiticiens, juristes, DPO, acheteurs) dont certains disposent d'un profil d'administrateur du SIA. Cette identification doit permettre d'arriver à un cahier des charges de formation, plus ou moins formalisé, dédié au SIA et adapté aux besoins de chacun. **La formation à réaliser et le niveau d'information à partager doivent être adaptés à ces besoins, en ciblant bien évidemment en premier lieu les utilisateurs.**

Recommandation 4.6. Référents internes en charge de l'organisation des formations

★★★ En particulier au sein des services métiers, il est recommandé **d'identifier et former des référents internes** chargés d'assurer les formations dans chaque service, en complément des formations initiales fournies par les éditeurs industriels et permettre **la mise en place d'un compagnonnage.**

Recommandation 4.7. Contenu pédagogique des formations

★★★ En complément de la notice d'utilisation du SIA accessible au professionnel, il est recommandé que les **formations proposées abordent notamment les éléments suivants** :

- les grands principes de fonctionnement du SIA : type d'algorithme, données d'apprentissage et données nécessaires à son fonctionnement (ou non), limites techniques ;
- la destination d'usage et finalité, énoncée clairement, et le périmètre d'utilisation autorisé de chaque SIA ;
- les performances attendues (sensibilité, spécificité, valeurs prédictives) et leurs implications pratiques ;
- une sensibilisation aux limites du SIA, biais potentiels (biais algorithmiques et cognitifs) et aux risques associés tels que le biais d'automatisation et le risque d'une diminution d'esprit critique dans le temps ou effet de halo ;
- l'organisation concrète de la prise en charge intégrant le SIA (modalités d'utilisation, intégration au SI, validation humaine des résultats), associée à des exemples de mauvaises utilisations du SIA, raisonnablement prévisibles ;
- les obligations réglementaires associées à l'usage de l'IA dont l'information des personnes. À ce titre, il est recommandé de former les professionnels à la communication avec les patients sur le SIA utilisé, en particulier sur les limites, incertitudes, et **la possibilité de s'en écarter pour assurer le principe de primauté du jugement clinique** ;
- les responsabilités de chacun des utilisateurs, en rappelant que la responsabilité finale demeure humaine malgré l'usage d'un SIA ;
- le cas échéant, les procédures à suivre en cas de désaccord avec le SIA, en réaffirmant la primauté du jugement clinique ;
- les procédures de signalement des incidents liés aux SIA, tout en valorisant ces signalements comme un levier d'amélioration continue.

Recommandation 4.8. Mise en pratique et cas d'usage

★★★ **Une mise en pratique sur des cas d'usages réels ou simulés** est également recommandée au cours de la formation, notamment par des exercices avec des erreurs volontaires du SIA à détecter par les professionnels ou des cas atypiques ou à l'origine de dilemmes (ex. : discordance IA/clinicien, non recours à l'IA car patients hors situation d'usage prévue par le fournisseur/fabricant, etc.). Cette mise en pratique doit être **inclue dans l'évaluation des connaissances acquises à la suite de la formation, qui est indispensable avant l'utilisation du SIA en autonomie par le professionnel.**

Recommandation 4.9. Régularité de la formaiton

★☆☆ Il est recommandé que cette formation continue soit réalisée **à une fréquence** régulière et adaptée au contexte du déploiement (prise en compte du turn-over important et du personnel en formation).

Recommandation 4.10. Traçabilité systématique de la formation

★☆☆ Il est recommandé à la fois d'assurer une **traçabilité systématique** des formations réalisées (registre nominatif, dates, contenu) et de **délivrer un certificat interne d'habilitation spécifique** à l'usage des SIA ayant un impact important sur la prise en charge des patients.

Les réflexes à adopter systématiquement :

Le recours à la seule notice d'utilisation ne saurait suffire pour constituer une formation adaptée à l'utilisation d'un SIA utilisé en contexte de soins.

Par ailleurs, les pratiques suivantes **doivent être exclues** :

- l'absence d'accompagnement des équipes dans l'adoption d'un SIA ;
- l'absence de session obligatoire sur la protection des données personnelles et l'intelligence artificielle à tout nouvel arrivant ;
- l'absence de sensibilisation des prestataires extérieurs et intérimaire (par action directe ou par engagement contractuel) quand leur impact sur la sécurité des données peut être aussi important que celui des collaborateurs internes[20].

[20] Voir notamment Sécurité : Impliquer et former les utilisateurs | CNIL

5. Organisation des soins

L'intégration d'un SIA en contexte de soins peut avoir une incidence importante sur l'organisation des soins en modifiant les flux de travail ou en impliquant une répartition différente des activités médicales et non médicales.

Ces modifications de l'organisation des soins doivent être accompagnées en clarifiant les rôles et les responsabilités de chacun pour :

- assurer le respect des bonnes pratiques de l'utilisation du SIA ;
- assurer le maintien d'une intervention humaine lors des décisions ;
- limiter les risques (transferts de compétences[21] non prévus, etc).

Cadre légal et réglementaire - Rappel

L'utilisation d'un SIA doit respecter les règles d'exercice des professions réglementées par le CSP afin d'éviter toute requalification en exercice illégal.

L'introduction d'un SIA dans les processus et l'organisation de soins ne modifie pas les règles en matière de délégation de tâche entre professionnels, telles que définies à l'article L. 4011-1 du CSP. Plus précisément, une délégation d'activité médicale est possible uniquement à un professionnel de santé[22], dans le cadre d'un protocole de coopération local ou national[23]. Ce protocole de coopération doit préciser les critères d'éligibilité et de retrait des patients concernés, la qualification professionnelle des professionnels délégants et délégués, les formations nécessaires à sa mise en œuvre ainsi que ses dispositions d'organisations spécifiques. Le patient doit également être informé des conditions de sa prise en charge[24].

La délégation d'une activité médicale est interdite à un tiers non professionnel de santé (sociétés industrielles, prestataires non médicaux, bénévoles, etc.) et en dehors d'un protocole de coopération. Le CSP pose le principe que les actes médicaux sont réservés aux médecins et par extension, à certaines professions de santé habilitées. L'accomplissement d'actes médicaux par des personnes non habilitées, même lorsqu'elles le font sous la surveillance ou avec l'accord d'un professionnel de santé, constitue un exercice illégal de la médecine pouvant être sanctionné pénalement[25].

Les activités non médicales peuvent être confiées à des tiers, tels qu'un autre professionnel de santé, une société ou un bénévole travaillant au sein d'une association, notamment dans le cadre d'une télésurveillance médicale, et sous réserve du respect des conditions détaillées à l'article L.162-52 du CSP.

[21] Transfert de tâches habituellement réalisées par des professionnels de santé à une IA (comme le tri des patients ou la pré-analyse d'images), ce qui implique une redéfinition de leur rôle et vigilance.
[22] Article L. 4011-1 alinéa 1 du CSP
[23] Articles L. 4011-3 à L. 4011-4-8 du CSP
[24] Article L. 4011-1 du CSP
[25] Articles L.4161-1 à L.4161-5 du CSP

Recommandation 5.1. Formalisation des rôles et responsabilités des utilisateurs

★★★

Lors de l'intégration d'un SIA, il est recommandé de **formaliser les rôles et les responsabilités des professionnels impliqués dans l'usage du SIA**, en précisant :

- les différents profils métiers concernés ;
- les actions et rôles attendus pour chaque profil utilisateur : usage technique du SIA (exécution, saisie), interprétation des résultats, décision clinique, supervision, etc. ;
- les actes qu'ils sont autorisés ou non à effectuer selon leur statut (ex. : décision clinique, validation médicale) ;
- les conditions de supervision ou de délégation lorsque plusieurs services ou établissements partagent un même SIA ;
- les modalités de formations attendues par profil utilisateur ;
- in fine, documenter l'organisation des soins à cibler.

Cette formalisation peut donner lieu à une fiche dédiée par profil utilisateur de SIA (par SIA ou par type de SIA selon les cas).

Recommandation 5.2. Référent dans chaque service dédié au SIA

★★★

Dans le cas où plusieurs professionnels auront à utiliser un même SIA, il est recommandé de **désigner un référent local dédié pour chaque SIA** et chargé du suivi fonctionnel, de l'accompagnement des équipes, de la collecte des retours de terrain et de l'interface avec la gouvernance.

Recommandation 5.3. Encadrer strictement toute délégation de tâches ou activités

★★★

Concernant les coopérations interprofessionnelles liées à l'utilisation d'un SIA, il est recommandé d'**encadrer strictement toute délégation de tâches ou activités induites par le SIA,** dans le respect des compétences professionnelles, des textes réglementaires et des protocoles de coopération autorisés.

6. Au cours de l'utilisation

L'utilisation d'un SIA doit intervenir dans le respect de la notice d'utilisation et de l'usage prévu par le fournisseur/fabricant. Certains risques sont cependant d'emblée identifiés, notamment :

- le biais de surconfiance[26], d'ancrage algorithmique[27], le biais d'automatisation et d'une perte d'expertise humaine ;
- le possible décalage entre la population de patients au sein de laquelle le SIA est déployé et la population de patients dont les données ont servi à l'apprentissage du SIA, à l'origine d'une éventuelle variation de performance.

Les recommandations proposées dans cette partie abordent des volets distincts : volet assurantiel, paramétrage et bon usage.

Cadre légal et réglementaire - Rappel

L'article 26 du RIA qui impose aux déployeurs de SIA à haut risque de prendre des mesures techniques et organisationnelles appropriées afin de garantir qu'ils utilisent ces systèmes conformément à leur notice d'utilisation.

Ce même article impose au déployeur de veiller à ce que les données utilisées pour le fonctionnement d'un SIA (données d'entrées) soient pertinentes et suffisamment représentatives.

Il lui impose également de confier le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires.

Enfin, les déployeurs doivent assurer la tenue des journaux générés automatiquement par la SIA à haut risque dans la mesure où ces journaux se trouvent sous leur contrôle.

En cas d'utilisation non-conforme, il existe un risque de requalification du déployeur en tant que fournisseur (article 25 du RIA)[28].

Dès lors que l'utilisation d'un SIA implique le traitement de données personnelles, une attention particulière devra être portée par le responsable de traitement (le déployeur du SIA) et les membres de son organisation au respect du principe de minimisation (article 5 du RGPD). Ce principe impose de vérifier que **seules les données strictement nécessaires pour atteindre un objectif donné sont utilisées**.

Par ailleurs, l'introduction d'un SIA ne change pas les règles en matière de secret professionnel prévues à l'article L. 1110-4 du CSP, ni celles applicables à l'exercice des professions de santé définies aux articles L. 4111-1 à L. 4163-11 du CSP.

[26] Tendance d'un professionnel à accorder une confiance excessive aux résultats ou suggestions d'un système d'IA, au détriment de son propre esprit critique ou de la validation humaine attendue.

[27] Le biais d'ancrage algorithmique correspond à l'influence excessive de la première proposition algorithmique sur le jugement clinique.

[28] Cette requalification peut être liée aux modifications substantielles apportées par le déployeur au SIA notamment une modification de sa destination d'usage.

Recommandation 6.1. Assurance de responsabilité civile professionnelle

★★★

Il est recommandé aux professionnels utilisateurs, selon leur mode d'exercice, de vérifier auprès de leur assurance de responsabilité civile professionnelle que **l'usage des SIA est bien couvert dans le cadre de leur activité**.

Recommandation 6.2. Utilisation conforme à la notice

★★★

Avant toute utilisation ou prise en compte des résultats d'un SIA, le professionnel utilisateur doit **s'assurer qu'il l'utilise de manière conforme à la notice d'utilisation et à la destination ou finalité d'usage prévue** et notamment que :

- le patient entre dans le périmètre général d'utilisation prévu du SIA, notamment pour les systèmes conçus pour un type de population précis (ex. : âge, pathologie, contexte clinique) ;
- le patient ne présente pas de facteurs d'exclusion à l'utilisation connus (par exemple. : antécédents rares, comorbidité non couverte par l'algorithme) ;
- le SIA est correctement paramétré en fonction du profil du patient.

En cas d'utilisation non conforme, le déployeur encourt le risque d'une requalification en tant que fournisseur et, par conséquent, le risque d'assumer toutes les obligations et responsabilité correspondantes.

Recommandation 6.3. Bonnes pratiques d'utilisation

★★★

Lorsque l'utilisation d'un SIA implique la transmission de données à caractère personnel, il est recommandé que chaque professionnel utilisateur :

- **s'assure qu'il permet au SIA de fonctionner correctement**, notamment pour les SIA nécessitant des ajustements de pratiques. C'est notamment le cas des SIA d'aide à la rédaction de comptes rendus médicaux dont l'utilisation peut par exemple nécessiter d'oraliser une partie de l'examen clinique afin de s'assurer que le système capture les informations pertinentes pour les restituer au sein du compte rendu ;
- **vérifie la pertinence des données transmises** par rapport au cas d'usage. Par exemple, la transmission de données d'identification n'est, dans la majorité des cas, pas nécessaire pour le fonctionnement d'outil d'aide à la décision ;
- **mette en perspective les caractéristiques du patient avec les biais algorithmiques** connus (genre, ethnie, âge, …) ou identifiés lors de la vérification de l'adéquation du SIA au contexte local ;
- **exerce une supervision humaine et confronte l'avis du SIA** à son propre raisonnement clinique/expertise et conserve une autonomie décisionnelle en repositionnant le résultat du SIA au regard du contexte clinique global, de l'environnement du patient et de toute autre information pertinente.

7. Information des personnes et consentement

L'information des personnes (patients ou usagers du système de santé notamment) est un élément indispensable pour favoriser le bon usage des SIA, mais également pour s'assurer de l'acceptation des SIA et de garantir l'effectivité des droits**.**

Différents types d'informations doivent être différenciées :

- **l'information générale sur l'usage de SIA dans les soins** ;
- **l'information sur l'utilisation de données personnelles liée au fonctionnement des SIA** ;
- **l'information sur la/les réutilisation/s secondaire/s des données personnelles** ;
- **la transparence sur les droits des patients** (accès, opposition etc.).

Les recommandations formulées dans cette partie visent à donner des pistes pour permettre une diffusion homogène de l'information. **L'information à apporter, son niveau d'exhaustivité et ses modalités de transmission peuvent varier et seront à déterminer au cas par cas.**

La mise en œuvre de ces recommandations suppose la mise en place de certaines actions préalables :

- cartographier les SIA utilisés dans l'établissement, leurs cas d'usage et leurs besoins pour fonctionner (notamment des données personnelles traitées) ;
- identifier les flux de données, les organismes qui interviennent (rôle et responsabilité) et les réutilisations précises envisagées, le cas échéant ;
- consulter les représentants des usagers le cas échéant (notamment la Commission des usagers) afin de s'assurer de la bonne compréhension des termes employés et les besoins d'information générale identifiés ;
- déterminer les modalités de communication adéquates.

Pour plus de détails, se référer à la partie **Erreur ! Source du renvoi introuvable.**.

Cadre légal et réglementaire - Rappel

1. Consentement

Il existe différents types de consentement mobilisables en contexte de soins :

- le **consentement** prévu par le CSP **lié aux actes de diagnostic, de pronostic et de soins**. Il implique que tout acte médical/sanitaire ou traitement nécessite le recueil du consentement libre et éclairé de la personne (L. 1111-4 du CSP).
- le **consentement des personnes, au sens du RGPD**[29].

[29] Il doit résulter d'une manifestation de volonté libre, être spécifique, éclairé et univoque. Il doit également pouvoir être retiré à tout moment, sans justification, et selon des modalités aussi simples que celles mises en œuvre pour sa collecte Conformité RGPD : comment recueillir le consentement des personnes ? | CNIL

La CNIL estime que le consentement ne constitue ni la base légale, ni l'exception pour le traitement de données personnelles de santé liés à l'utilisation de SIA en contexte de soins.

Ces traitements peuvent être fondés sur :

- sur les intérêts légitimes du responsable de traitement (article 6.1.f) ou la poursuite d'une mission d'intérêt public qui lui incombe (article 6.1.e). Le choix de la base légale appropriée devra tenir compte de la qualification du responsable de traitement et du SIA concerné ;
- l'exception « médecine » au sens de l'article 9.2.h) du RGPD sous réserve que le responsable de traitement soit un établissement ou un professionnel de santé tenu au secret.
- **le consentement contextuel**, imposé pour des cas particuliers (par exemple, la participation à une recherche clinique, la captation ou l'utilisation de la voix et de l'image d'une personne).
- **le consentement éthique** pouvant être recueilli en dehors de toute obligation légale ou réglementaire, par souci de transparence et de loyauté.

À noter : Les articles 60 et 61 du RIA n'imposent de recueillir le consentement spécifique que pour les essais de SIA à haut risque réalisés en conditions réelles, qui ne sont pas abordés dans ce guide.

2. Information des personnes

Il existe plusieurs obligations d'informations générales des établissements et professionnels de santé envers le patient et notamment :

- une **obligation d'information sur l'état de santé du patient et les différentes investigations, traitements ou actions de prévention proposés** (L. 1111-2 du CSP) ;
- une **obligation d'information quant à l'utilisation de SIA qualifiés de DM pour un acte de prévention, de diagnostic ou de soin et des conséquences liées** (L. 4001-3 du CSP).

Obligations des déployeurs liées à l'utilisation d'un SIA :

Le RIA prévoit plusieurs obligations de transparence à la charge du déployeur :

- lors de l'utilisation d'un SIA à haut risque (hors DM/DMDIV) qui prend ou facilite la prise de décision concernant des personnes physiques (article 26.11) ;
- lors de l'utilisation d'un SIA à risque modéré (article 50).

Obligations des responsables de traitement de données personnelles lors de l'utilisation d'un SIA (quelle que soit sa classification)

Le RGPD impose au responsable de traitement (le déployeur d'un SIA) d'informer les personnes de ce qu'il utilise leurs données personnelles. Cette information doit notamment être compréhensible, aisément accessible et comporter les mentions prévues aux articles 13 ou 14 du RGPD (ex. : l'objectif du traitement, les catégories de données, les destinataires des données, la durée de conservation, ainsi que les droits des personnes sur leurs données).

Cette obligation vaut pour l'utilisation primaire des données (fonctionnement d'un SIA pour le soin) et leur utilisation secondaire / réutilisation (par exemple développement ou amélioration d'un modèle, évaluation du SIA).

La CNIL rappelle que :

- les utilisations secondaires/réutilisations constituent des traitements de données personnelles distincts de ceux intervenant lors de l'utilisation primaire (contexte de soins). Ces traitements devront être conformes au RGPD et à la loi « informatique et libertés » et leur mise en oeuvre pourra nécessiter la réalisation de formalités préalables auprès de la CNIL par leur responsable[30] ;
- toute structure de soins est tenue d'informer les personnes qu'elles prennent en charge du traitement de leurs données personnelles, conformément à l'article 71 de la loi « informatique et libertés ».

3. Les droits des personnes

Les droits prévus par le RIA

Le RIA prévoit le droit pour toutes personnes concernées par l'utilisation d'un SIA :

- **d'introduire une réclamation auprès de l'autorité de surveillance du marché** (article 85) ;
- **d'obtenir une explication concernant une décision individuelle prise avec l'utilisation de certains SIA** (article 86).

Les droits prévus par le RGPD

Les personnes disposent des droits suivant sur leurs données :

- un droit d'accès (article 15 du RGPD) ;
- un droit de modification (article 16 du RGPD) ;
- un droit de suppression (article 17 du RGPD) ;
- un droit d'opposition au traitement de ses données (article 21 du RGPD),
- un droit à la limitation du traitement (article 18 RGPD) ;
- un droit d'introduire une réclamation auprès de la CNIL, prévu aux articles 13 à 15 du RGPD.

Le responsable de traitement (déployeur du SIA) sera tenu de donner suite aux demandes d'exercice de droit qu'il reçoit. Il pourra s'appuyer sur ses sous-traitants (par exemple le fournisseur du SIA), qui sont tenus de mettre en œuvre les mesures appropriées à cet effet.

[30] Formalités préalables | CNIL

En synthèse, quelles sont les obligations du déployeur ?

- lors de l'utilisation d'un SIA à haut risque visé par l'annexe III[31] du RIA, le déployeur doit en informer les personnes concernées ;
- lorsque la personne interagit directement avec le SIA (exemple chatbot), celle-ci doit en être avertie et être sensibilisée afin de ne pas révéler plus d'informations que ce qui est nécessaire ;
- lorsque l'utilisation du SIA implique un traitement de ses données personnelles, une information conforme au RGPD doit être délivrée à la personne concernée et le déployeur doit donner suite à leurs demandes d'exercice de leurs droits ;
- lorsque ses données personnelles utilisées dans le cadre du soins seront réutilisées par exemple à des fins de développement, de recherche clinique ou d'évaluation du déploiement du SIA, une information conforme au RGPD doit être délivrée à la personne concernée et le responsable de traitement doit donner suite à leurs demandes d'exercice de leurs droits ;
- lors de l'utilisation d'un DM intégrant un SIA, le professionnel de santé décidant d'y recourir doit en informer les personnes[32].

Recommandation 7.1. Absence de consentement spécifique

★★★

En premier lieu, il est recommandé de **ne pas exiger de consentement spécifique pour l'utilisation d'un SIA dans le cadre du soin courant.** En effet, le recueil d'un consentement est un processus complexe qui ne semble pas adapté à la majorité des cas d'utilisation d'un SIA, notamment en raison du déséquilibre de la relation patient-professionnel de santé. Dans la majorité des situations, une information loyale et accessible à tous, accompagnée d'un droit d'opposition, est suffisante.

Cependant, il est rappelé que :

- **certains actes médicaux sont soumis au consentement de la personne au titre du CSP ;**
- **la collecte et l'utilisation d'enregistrements photo, vidéo ou vocaux permettant l'identification de la personne sont soumises au consentement de la personne au titre du code civil**.

Par ailleurs, le déployeur peut mettre en place un consentement éthique dans certains cas susceptibles d'engendrer des risques particuliers pour les personnes. Ce consentement peut être recueilli à l'écrit (ex. case à cocher par le professionnel) ou à l'oral et ne nécessite pas de formalisme particulier, sauf réglementation contraire. Pour les cas où un consentement n'est pas requis par la réglementation, les modalités d'information de la personne devront être documentées et tracées au niveau de la structure et/ou au sein du dossier médical, en fonction du niveau de recommandation retenu (cf ci-dessous).

[31] Notamment des systèmes d'IA destinés à être utilisés par les autorités publiques ou en leur nom pour évaluer l'éligibilité des personnes physiques aux prestations et services d'aide sociale essentiels, y compris les services de soins de santé, ainsi que pour octroyer, réduire, révoquer ou récupérer ces prestations et services ou systèmes d'IA destinés à évaluer et hiérarchiser les appels d'urgence émanant de personnes physiques ou à être utilisés pour envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence, y compris par la police, les pompiers et l'assistance médicale, ainsi que pour les systèmes de tri des patients admis dans les services de santé d'urgence

[32] Si les textes d'application de l'article L. 4001-3 du CSP sont encore en cours d'élaboration, les acteurs sont vivement invités à les anticiper

Information des personnes

L'information des personnes constitue une obligation légale dans les cas rappelés ci-dessus, notamment en cas de traitement de données personnelles.

Aussi, l'absence d'information peut exposer le professionnel et/ou l'établissement notamment à un risque juridique. En effet, un patient privé d'information ne peut ni exercer ses droits, y compris en cas de recours contre le fournisseur/fabricant du système, ni pleinement consentir aux actes de soins proposé.

Au-delà de ces obligations, la transparence vis-à-vis des personnes est une condition essentielle pour leur permettre de comprendre ces technologies, leurs cas d'usage et leurs limites. Cette transparence garantit une pratique professionnelle en cohérence avec le cadre de confiance dans lequel s'inscrit la relation patient/professionnel. Enfin une attention particulière devrait être portée à l'information des personnes en cas de réutilisation des données collectées dans le cadre du soin notamment à des fins d'amélioration ou de développement des modèles et SIA. Ces utilisations secondaires constituant une pratique existante et, dans certains cas, nécessaires afin d'améliorer leurs performances, il est essentiel que leurs responsables informent les personnes dès la collecte de leurs données personnelles dans le cadre du soin.

Focus - Quel bon niveau d'information ?

L'information transmise au patient concernant l'IA peut revêtir un caractère anxiogène important, à la fois sur les résultats produits par l'IA mais également sur l'utilisation des SIA. La formation des professionnels à comprendre eux-mêmes le fonctionnement et les limites des SIA est une condition indispensable pour pouvoir en parler pertinemment aux patients et permettre de démystifier l'usage de ces technologies.

Afin d'identifier le bon niveau d'information à apporter, il est recommandé :

- de ne pas surcharger l'information de termes techniques, qui est susceptible de générer confusion ou méfiance : privilégier une pédagogie transparente, compréhensible et centrée sur les bénéfices attendus pour le patient (ex. sécurité, rapidité).
- d'assurer une traçabilité formelle de l'information donnée au patient, tant pour des raisons juridiques que pour garantir la continuité de l'information ;
- de la distinguer des autres informations requises par la réglementation (information sur les frais, etc.) ;
- d'impliquer les représentants des usagers et des professionnels dans la conception des messages d'information pour adapter le vocabulaire aux perceptions des patients (ex. éviter les termes anxiogènes) et la manière pour la rendre facilement accessible à toute la patientèle/aux personnes.

Dans tous les cas, une information multi-modale constitue une démarche efficace pour toucher un maximum de personnes et satisfaire les différents niveaux de littératie en santé / numérique (vidéos, flyers, FALC, etc.), sur un site web, directement au sein de l'établissement, etc.

Au total, une gradation de l'information à apporter à la personne en 3 niveaux est proposée, en fonction du risque posé par le SIA pour le patient et de la possibilité pour le patient d'exercer des droits en réponse :

- Niveau 1 : une information générale à l'échelle de la structure ;
- Niveau 2 : pour les patients concernés par une utilisation spécifique, l'ajout d'une phrase type dans le compte-rendu qui leur sera remis ;
- Niveau 3 : pour des SIA présentant des risques importants pour le patient, une information exhaustive en amont de l'utilisation ou de la décision médicale.

★★★ Recommandation 7.2. Information générale à l'ensemble des patients

Il est recommandé d'apporter un **premier niveau d'information générale à l'ensemble des patients sur l'utilisation possible de SIA dans leur parcours de soins**.

Cette information générale peut par exemple prendre plusieurs formes :

- une **mention type dans le livret d'accueil, une affiche en salle d'attente, ou un site web, un compte-rendu avec des exemples d'utilisation et de finalité**. Par exemple : « Dans le cadre de votre prise en charge, des systèmes d'intelligence artificielle peuvent être utilisés pour améliorer votre prise en charge. Pour plus d'informations, consultez le site internet de l'établissement ou adressez-vous à l'accueil » ;
- la **rédaction d'une charte au niveau de la structure, mettant en avant les principes de l'établissement liés à la sélection de SIA et leur utilisation**. Cette charte pourrait préciser les engagements de qualité pris par la structure (ex. : la supervision humaine obligatoire, la qualité des systèmes utilisés, les cas d'usage pour lesquels un consentement du patient est nécessaire) ou le respect des présentes recommandations ;

Une **information exhaustive sur l'ensemble des SIA utilisés au sein d'une structure peut également être envisagée, en se basant notamment sur la cartographie des SIA utilisés dans l'établissement** (cf. **Erreur ! Source du renvoi introuvable.**). Cette liste des SIA peut inclure les noms des technologies utilisées ou mentionner les différents cas d'usage de ces systèmes (ex. : en radiologie pour l'aide à l'interprétation, lors des consultations pour l'aide à la génération de compte-rendu), les bénéfices attendus, les populations ciblées et l'état de déploiement du SIA (utilisation en routine ou non), les réutilisations envisagées des données.

> La mise à disposition publique d'une telle liste s'inscrit dans la démarche de "portail de transparence" pour les entrepôts de données de santé recommandée par la CNIL. Il est à noter qu'un tel portail peut à la fois présenter un atout d'attractivité pour la structure comme exposer l'établissement/le professionnel au risque de refus d'utilisation de SIA, en amont de son utilisation, alors que certains sont aujourd'hui incontournables pour la réalisation d'actes. Pour pallier ce risque, la formation des professionnels à l'information du patient (intérêt du SIA, balance bénéfice/risque, perte de chance, etc.) est indispensable afin qu'ils puissent en parler de manière éclairée au patient.

Recommandation 7.2. Information spécifique aux patients directement concernés

★★★ Il est également recommandé de compléter cette information générale par **une information spécifique à un patient et contextualisée lorsqu'il est directement concerné par l'usage d'un SIA en contexte de soins** et notamment pour les SIA d'aide au dépistage, diagnostic ou à la décision médicale, et pour les SIA basés sur de l'IA générative (ex. : aide à la rédaction de comptes-rendus). Cette information spécifique devrait être apportée aux patients, a minima via le dossier médical du patient (notamment les traces fonctionnelles) ou dans le compte-rendu d'examen.

L'ajout systématique d'une phrase personnalisable au sein des comptes-rendus médicaux constitue une bonne pratique d'information. Par exemple, peuvent être transmises les mentions suivantes :

- « Ce [type de document : compte-rendu, mail, synthèse médicale, etc.] a été établi(e) avec l'assistance du système d'intelligence artificielle [Nom, Version], validé par le Dr [Nom, fonction]. »
- « Le système d'intelligence artificielle [Nom, Version] peut être utilisé comme [Finalité du SIA : aide au diagnostic, aide à la décision médicale, etc.] dans votre prise en charge, sous la supervision du Dr [Nom, fonction]. »

Cette traçabilité de l'usage d'un SIA dans le parcours de soins constitue une garantie de transparence pour les patients. Cette information est également importante à partager dans le cas d'échanges avec d'autres professionnels, notamment pour les demandes d'expertises complémentaires ou demandes d'avis de confrères.

Lorsque cela est pertinent, des documents pédagogiques, spécifiques à un SIA, peuvent également être mis à disposition en salle d'attente ou directement transmis aux patients concernés (fascicule, fiche explicative ou notice à remettre au patient à la suite de l'information transmise par le professionnel).

À noter que cette information spécifique, sauf cas contraire, n'est pas nécessaire pour les SIA « techniques », utilisés par exemple pour améliorer la résolution d'une imagerie ou l'acquisition des coupes.

Recommandation 7.4. Information exhaustive préalable à l'utilisation

★☆☆ Dans certains cas, une **information exhaustive, préalable à l'utilisation d'un SIA peut également être apportée au patient**, notamment lorsqu'elle peut permettre l'exercice de droits pour la personne et/ou si l'utilisation du SIA présente un risque spécifique pour la personne, par exemple dans le cas où une prise en charge est majoritairement basée sur la prédiction d'un SIA et en l'absence d'autres données cliniques objectivables par un humain.

8. Décision automatisée et contrôle humain

Mise au point sur la décision automatisée et le contrôle humain

Les notions de décision automatisée et de contrôle humain sont liées mais doivent être bien distinguées.

La **décision automatisée** désigne une décision prise sans intervention humaine significative, produisant des effets juridiques ou des effets concernant une personne de manière aussi importante (ex. : priorisation d'une prise en charge, orientation du parcours, d'un traitement, mise en œuvre d'un traitemen) Elle est interdite par défaut (voir rappel du cadre légal et réglementaire).

Le **contrôle humain**, lui, est une mesure de supervision humaine active prévue par le RIA (article 14) pour tout SIA à haut risque : il s'agit de l'encadrement d'un professionnel à même de comprendre, vérifier, corriger ou contredire le résultat de l'IA.

La notion de décision automatisée, issue du RGPD garantit que les droits des personnes sont respectés, là où le contrôle humain du RIA garantit la qualité et la sécurité de l'usage.

Le contrôle humain ou la supervision humaine constitue un socle éthique, juridique et organisationnel fondamental pour le bon usage des SIA en santé, permettant de s'assurer que toute décision médicale est prise sous la responsabilité du professionnel de santé.

Plusieurs questions se posent cependant et notamment :

- quel acteur doit réaliser cette supervision : un professionnel intervenant directement dans le processus de soins ou un professionnel externe ?
- quelle qualification (spécialité médicale par exemple) doit avoir le professionnel réalisant cette supervision ?
- dans quelle temporalité cette supervision doit-elle être effectuée ?
- quelle forme peut-elle prendre et quelle proportion des cas doit-elle être revue : l'intégralité des cas, une sélection des cas, etc. ?

Cadre légal et réglementaire - Rappel

Le RIA impose aux fournisseurs de SIA à haut risque d'intégrer un contrôle humain effectif lors de leur utilisation afin de prévenir ou limiter les risques pour la santé, la sécurité et les droits fondamentaux (article 14).

Ce contrôle doit permettre aux personnes en charge de superviser ces systèmes de comprendre leurs capacités et limites, de détecter des anomalies, d'éviter les biais d'automatisation, d'interpréter correctement les résultats, de pouvoir s'écarter des décisions proposées par le système et d'intervenir ou interrompre son fonctionnement en toute sécurité.

Ces modalités doivent être documentées dans l'analyse d'impact du système sur les droits fondamentaux (AIDF), le cas échéant.

Le RIA prévoit le droit des personnes concernées par une décision fondée sur un système à haut risque d'obtenir des explications claires sur le rôle joué par l'IA et les éléments ayant conduit à cette décision (article 86). Toutefois, contrairement au RGPD, le RIA ne régit pas les décisions entièrement automatisées impliquant des données à caractère personnel.

Le RGPD interdit les décisions entièrement automatisées produisant des effets juridiques ou un impact significatif sans une intervention humaine significative (article 22), sauf si celle-ci peut être fondée sur le consentement explicite de la personne ou sur un texte européen ou national.

Cette intervention doit dépasser une simple validation pour éviter une influence excessive de l'algorithme, comme l'a précisé la Cour de justice de l'Union européenne (CJUE) notamment dans le cadre du scoring bancaire[33].

Le RGPD garantit un droit à l'information sur l'existence d'une décision automatisée, un droit à l'explicabilité de la logique sous-jacente ainsi qu'un droit à être informé des conséquences de cette décision. La CJUE a précisé que ces informations doivent être pertinentes, transparentes, compréhensibles et accessibles [34] . Les garanties associées aux décisions partiellement automatisées (nature de l'intervention humaine, niveau de risque) doivent être documentées dans l'analyse d'impact du système (AIPD), le cas échéant.

Par ailleurs, deux dispositions du CSP doivent être rappelées :

- l'article L. 1111-4 qui prévoit que « le patient prend, avec le professionnel de santé et compte tenu des informations et des préconisations qu'il lui fournit, les décisions concernant sa santé » ;
- l'article R. 4127-5 du CSP qui précise que « le médecin ne peut aliéner son indépendance professionnelle sous quelque forme que ce soit ».

À date et en égard aux dispositions du CSP, les conditions posées par l'article 22 du RGPD ne sont pas remplies, ce qui interdit par principe toute prise de décision entièrement automatisée. Toutes les décisions portant sur la prise en charge sanitaire des personnes grâce à l'utilisation de SIA devront faire l'objet d'une supervision humaine par le professionnel ayant pris en charge la personne.

En effet, aucun texte national ou européen ne reconnaît à l'utilisation d'un SIA la poursuite d'un motif d'intérêt public important ou n'autorise expressément la prise de décision automatisée dans un contexte de soins. De plus, le recueil d'un consentement est, de manière générale, peu approprié pour les traitements de données personnelles dans ce contexte.

[33] Curia, 1ère chambre, arrêt du 7 décembre 2023, dans l'affaire C-634/21
[34] Curia, 1ère chambre, arrêt du 27 février 2025, dans l'affaire C-203/22

Les modalités de mise en œuvre du contrôle humain doivent être proportionnelles à l'impact dans les soins. À ce jour, il n'y a pas de standard sur les modalités de mise en place du contrôle humain, qui doit être adapté au cas par cas à l'organisation des soins dans lequel le SIA est déployé.

★★★ Recommandation 8.1. Supervision humaine conforme aux exigences réglementaires

Il est recommandé d'**assurer une supervision humaine dans toute décision individuelle assistée par un SIA, conformément aux exigences réglementaires, et d'en assurer la traçabilité**. Une supervision humaine, par un professionnel formé et disposant de l'ensemble des informations et moyens nécessaires pour effectuer correctement sa tâche, **reste essentielle**, quelle que soit la validation scientifique du SIA.

★★★ Recommandation 8.2. Adaptation du niveau de supervision humaine

Il est recommandé **d'adapter le niveau de supervision au niveau de risque du cas d'usage et au positionnement du SIA dans l'organisation des soins** avec :

- une **supervision intégrale** (revue humaine systématique de 100 % des résultats IA), pour les décisions ayant un impact important sur la prise en charge du patient (ex. : un SIA entraînant un acte invasif chez un patient). Pour ces actes à fort impact sur la prise en charge, il est recommandé de mettre en place une organisation adaptée afin d'appliquer aux SIA non-DM les mêmes exigences de validation et de vigilance qu'aux DM, pour limiter toute dégradation de qualité et de sécurité des soins ;
- une **supervision allégée**, ciblée sur des cas sensibles ou à risque identifié, pour les cas d'usage non-cliniques.

Focus sur les SIA de tri ou de dépistage – Éléments prospectifs

Les bonnes performances de certains SIA permettent d'envisager de nouvelles organisations de soins impliquant une absence de revue de l'ensemble des résultats du SIA par un professionnel de santé, notamment dans un objectif de dépistage ou de priorisation (ex. : absence de revue par un professionnel de santé des cas identifiés comme "ne présentant pas la pathologie" par le SIA).

Cependant, la réglementation ne permet pas à l'heure actuelle d'avoir de décision entièrement automatisée produisant des effets juridiques ou un impact significatif sur les personnes, sans intervention humaine. Ainsi, des organisations de soins sans revue de l'ensemble des cas par un professionnel de santé apparaissent contraires à la réglementation et exposent le professionnel ou l'établissement à un risque juridique, d'autant plus si le SIA est utilisé en remplacement d'une pratique déjà bien établie.

Pour autant, les SIA présentent l'opportunité de développer de nouvelles stratégies, par exemple pour permettre la mise en place de dépistages à large échelle.

Ces questions nécessitent qu'un débat démocratique et éthique ait lieu afin de déterminer ce que la société souhaite autoriser et les garanties à prévoir.

D'ores et déjà, plusieurs **conditions cumulatives devront être réunies** pour permettre ces organisations innovantes, et notamment, à l'échelle de la structure :

- la mise en place d'une organisation des soins adaptée à l'utilisation du SIA ;
- le choix d'un SIA adapté et calibré, notamment en matière de sensibilité et spécificité, avec la fixation d'un seuil de faux négatifs et faux positifs adapté ;
- la mise en place d'un contrôle qualité proportionnée permettant de suivre dans le temps les taux de faux négatifs et les conséquences de faux positifs sur les personnes ;

À l'échelle nationale, la mise en place de ces organisations appelle à :

- la mise en place d'une stratégie nationale organisée, notamment pour le dépistage, impliquant l'utilisation d'un SIA ne creusant pas les inégalités de soins ;
- une implication essentielle des conseils nationaux professionnels, des représentants des spécialités médicales concernées, et des représentants de patients, qui devront être sollicitées pour avis ;
- une réflexion sur la pertinence d'une indemnisation au titre d'accidents médicaux non fautifs ouvrant un droit à une indemnisation par l'ONIAM des dommages résultant de résultats erronés liés à l'utilisation d'un SIA.

Des travaux spécifiques devront être conduits pour l'ensemble de ces différents éléments.

★★★ Recommandation 8.3. Définition des modalités de contrôle humain dans les protocoles

Il est recommandé de **définir clairement dans des protocoles internes les modalités de contrôle humain à mettre en œuvre**, notamment pour les décisions à fort impact sur les patients et la prise en charge (ex. : aucune décision de non-traitement ou de diagnostic n'est laissée à la seule appréciation d'un SIA). Ces protocoles cliniques doivent se baser sur les conditions d'utilisation définies par le fournisseur du SIA et notamment préciser les seuils d'alerte et les responsabilités des intervenants. Les sociétés savantes et CNP pourraient jouer un rôle majeur dans l'élaboration de ce type de protocoles.

★★★ Recommandation 8.4. Garantir explicitement la liberté de décision du praticien

Afin de préserver l'expertise et l'indépendance professionnelle mais aussi exclure la prise de décision automatisée, il est recommandé de **garantir explicitement la liberté de décision du praticien face aux propositions de l'IA, conformément au Code de déontologie médicale.**

À ce titre, **il semble important :**

- **d'éviter tout phénomène de « dilution de responsabilité » lié à la présence du SIA**, en rappelant clairement que la responsabilité décisionnelle finale demeure humaine ;
- **d'encourager les professionnels à toujours exercer leur jugement clinique propre et à documenter et tracer leurs décisions**, également en cas d'écart vis-à-vis des recommandations du SIA ;
- **de mettre en place, lorsque cela est nécessaire, une procédure en cas de désaccord explicite avec le SIA** pour promouvoir la réflexivité clinique et pouvant impliquer de documenter dans le dossier patient toute décision divergente du résultat du SIA, et les raisons médicales ou humaines justifiant cette divergence. En complément du signalement auprès des autorités nationales compétentes, le cas échéant, et du fournisseur, un recensement des cas/RETEX au sein de la structure peut être effectué, notamment pour identifier d'éventuels biais du SIA.

Recommandation 8.5. Analyse régulière des incidents liés à l'utilisation du SIA

★★★ Afin d'adapter la supervision au besoin et d'assurer la meilleure qualité et sécurité des soins, il est recommandé de **procéder à l'analyse régulière des incidents liés à l'utilisation des SIA** afin d'ajuster finement les modalités de supervision humaine en fonction des résultats observés (ex. : renforcer la supervision sur certains types d'erreurs récurrentes). Pour les SIA à haut risque, si l'utilisation d'un système conformément à la notice peut conduire à ce qu'il présente un risque, il convient d'en informer sans retard injustifié le fournisseur ainsi que l'autorité de surveillance du marché concernée. Il en est de même, immédiatement, en cas d'incident grave.

Les réflexes à adopter systématiquement

L'intégration dans le dossier médical de la personne des résultats générés par un SIA doivent être revus par le professionnel de santé prenant en charge la personne.

En particulier dans le cas de SIA d'aide à la rédaction de comptes-rendus, ce compte-rendu **ne devrait pas** faire l'objet d'une validation par un tiers non présent lors de la consultation ou de la réalisation de l'acte (ex. : par une secrétaire médicale). En effet, une personne n'ayant pas été présente lors de la consultation ne sera pas en mesure de détecter la présence d'hallucinations au sein du compte-rendu généré par un SIA.

9. Traçabilité des usages

La traçabilité rigoureuse des usages permet de documenter le bon usage des SIA à l'échelle d'un établissement tout en contribuant à la sécurité des données et des systèmes d'information.

La traçabilité, telle qu'utilisée dans ces recommandations, renvoie à plusieurs éléments dont :

- la conservation des résultats générés par des SIA et, le cas échéant, des données utilisées pour son fonctionnement ;
- l'identification de l'intervention d'un SIA dans le parcours de soins d'une personne et les choix cliniques associés ;
- les mesures de journalisation[35], dont l'objectif est d'assurer une traçabilité des accès et des actions des différentes personnes accédant aux systèmes d'informations et, plus précisément, aux traitements de données personnelles mis en œuvre. Il s'agit d'une mesure de sécurité importante, encouragée systématiquement par la CNIL. Les données de journalisation devraient faire l'objet de mesures d'analyse automatique afin de permettre la détection rapide des éventuelles utilisations indues du traitement.

Les enjeux de traçabilité du fournisseur (par exemple, la surveillance après mise sur marché) ne sera pas abordée. Ces recommandations n'ont pas vocation à remplacer les autres exigences ou recommandations existantes, propres aux systèmes d'informations, mais à offrir des points d'attention complémentaires.

Cadre légal et réglementaire - Rappel

Le RIA impose au fournisseur de SIA certaines obligations de traçabilité à des fins de :

- transparence vis-à-vis des déployeurs et des personnes ;
- suivi de la qualité et des performances du système ;
- suivi d'une utilisation conforme du système par le déployeur.

Pour les SIA à haut risque, ces obligations portent sur :

- la mise en place d'enregistrement automatique des événements, c'est-à-dire des journaux, tout au long de la durée de vie du SIA (article 12) ;
- la conservation de ces journaux pendant une période adaptée à la destination du SIA à haut risque, d'au moins 6 mois (article 19).

Les déployeurs de SIA à haut risque sont tenus à une obligation similaire à celle prévue par l'article 19 du RIA dès lors que les journaux sont « sous leur contrôle ».

Pour les SIA à risque modéré, le fournisseur de SIA « *qui génèrent des contenus de synthèse de type audio, image, vidéo ou texte, veillent à ce que les sorties des systèmes d'IA soient marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA* ». **Si cette obligation n'est pas à la charge directe du déployeur, elle doit faire l'objet d'une attention particulière lors de l'utilisation du SIA.**

[35] CNIL, Recommandations de la CNIL sur la journalisation https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-relative-aux-mesures-de-journalisation

Par ailleurs, le RGPD impose une obligation générale de sécurité des traitements mis en œuvre (articles 5.1.f et 32 du RGPD). Cette exigence s'applique tant aux responsables de traitement (les professionnels et les établissements déployant un SIA en contexte de soins) qu'à leurs sous-traitants notamment les fournisseurs de ces systèmes.

Pour plus de précisions sur les mesures de sécurité des données à caractère personnel, il convient de se reporter à la dernière version du guide de la sécurité des données personnelles de la CNIL[36]. Il est également possible de se reporter à la recommandation de la CNIL sur le dossier patient informatisé[37] dont la version définitive sera prochainement publiée.

Conservation des données générées par un SIA

Lorsque ces données sont intégrées au dossier patient, elles sont soumises aux durées de conservation prévues par le code de la santé publique s'agissant du dossier médical[38].

En complément de ces éléments, il est possible de se reporter au projet de recommandations de la CNIL sur le dossier patient informatisé[37].

Lorsque les données issues de l'utilisation d'un SIA ne sont pas intégrées au dossier patient, aucun texte n'impose de durées maximales ou minimales. Le principe général de conservation pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées prévue par l'article 5. 1 e) du RGPD doit être respecté et apprécié au cas par cas.

Recommandation 9.1. Conserver la notice d'utilsiation du SIA

★★★

En premier lieu, il est recommandé au **déployeur de conserver la copie de la notice d'utilisation du SIA,** qui constitue un support essentiel pour assurer son utilisation conforme et sécurisée.

Recommandation 9.2. Intégrer la traçabilité comme outil de prévention des risques

★★★

Il est recommandé en premier lieu **d'intégrer la traçabilité comme outil de prévention des risques** et comme support à la redevabilité des professionnels en cas de litige ou de contrôle réglementaire. Ceci implique une journalisation conforme à la recommandation de la CNIL ainsi que la revue régulière des traces (audits). Par ailleurs, il est recommandé :

- **de clarifier et formaliser la responsabilité de chaque acteur dans la traçabilité** (éditeur, professionnels de santé, services qualité et informatique) ;
- **d'intégrer systématiquement la traçabilité (« IA utilisée : oui/non ») dans les procédures internes** (check-list qualité, validation des dossiers) ;
- **d'intégrer la décision du professionnel de prendre en compte (ou non) les résultats générés par le SIA ainsi que le choix clinique associé** ;

[36] https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles

[37] https://www.cnil.fr/sites/cnil/files/2025-03/projet_de_recommandation_dossier_patient_informatise.pdf

[38] Conformément à l'article R. 1112-7 du CSP, ces données doivent être conservées pendant une durée maximale de 20 ans à compter de la dernière venue du patient dans l'établissement pour une consultation ou hospitalisation. Lorsque la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date. En cas de décès du patient, le dossier est conservé pendant 10 ans à compter de la date du décès.

- **d'assurer la génération automatique par le SIA de journaux techniques (logs) détaillant chaque analyse : date, heure, identifiant du cas, résultats, utilisateur** en précisant si le SIA agit sur une demande expresse d'un professionnel (qui devra être indiqué le cas échéant) ;
- **de garantir contractuellement l'accès de l'établissement aux logs techniques**, même lorsque le SIA est hébergé chez le fournisseur (système cloud) ;
- **d'anticiper la possibilité de futures exigences nationales en matière de remontées d'informations sur les incidents IA** (notamment, en cas de création d'une base nationale de signalement).

★★★ Recommandation 9.3. Conserver systématiquement les résultats du SIA

Il est recommandé de **conserver systématiquement, au sein d'un volet dédié à l'utilisation du SIA au sein du dossier patient, les résultats générés par un SIA (rapports, annotations, images).** Ils y seront conservés au même titre et pour la même durée que les autres données du dossier patient. De plus ces résultats devront faire l'objet d'un marquage spécifique permettant d'identifier leur source.

10. Vigilance, maintenance, suivi des performances, mises à jour et gestion de la qualité

Les phases de maintenance, de mise à jour et les étapes de gestion de la qualité visent à maintenir, dans la durée, la performance optimale du SIA, à prévenir et à corriger les dysfonctionnements éventuels, ainsi qu'à assurer la continuité de service et des soins en toute circonstance.

Cadre légal et réglementaire – Rappel

Vigilance

Les règlements (UE) 2017/745 et (UE) 2017/746 et leur transposition en droit français avec l'ordonnance n°2022-582 du 20 avril 2022 imposent un plus grand niveau de traçabilité et de transparence notamment dans le cadre du traitement des cas de vigilance. **À ce titre, les SIA ayant le statut de DM doivent faire l'objet de déclaration de matériovigilance et réactovigilance, au même titre que les autres DM.**

L'article L. 5212-2 du CSP précise que « *tout professionnel de santé ou tout utilisateur professionnel du dispositif ayant connaissance d'un incident grave le déclare à l'agence* » dans les meilleurs délais. « *Il peut déclarer, en outre, tous les autres incidents dont il a connaissance, suspectés d'être dus à un dispositif auprès du fabricant, afin que celui-ci puisse exercer ses activités de surveillance après commercialisation* ».

En ce qui concerne les autres incidents, il n'y a pas d'obligation de signalement.

Cependant, les utilisateurs sont incités à les transmettre au fournisseur/fabricant afin qu'il puisse exercer ses activités de surveillance après commercialisation. L'article 73 du RIA impose également au fournisseur de déclarer pour les SIA à haut risque tout incident grave aux autorités de surveillance du marché, dans un délai tenant compte de l'ampleur de l'incident grave.

À l'heure actuelle, le circuit de vigilance pour les SIA utilisés en contexte de soins mais n'ayant pas le statut de DM/DMDIV ou n'étant pas classés à haut risque reste à clarifier.

Mesures correctives, gestion de la qualité et mesures de sécurité des données à caractère personnel

Lorsqu'un fournisseur met sur le marché ou en service un SIA à haut risque et constate, ou a des raisons de penser, que celui-ci n'est pas conforme au RIA, il est tenu, conformément à l'article 20 de ce règlement, de prendre immédiatement les mesures correctives nécessaires. Ces mesures peuvent inclure la mise en conformité du système, son retrait, sa désactivation ou son rappel. Le fournisseur doit également informer, le cas échéant, les déployeurs concernés.

Par ailleurs, l'article 20 du RIA comprend également une obligation supplémentaire en faveur de la gestion de la qualité. En effet, lorsqu'un fournisseur prend connaissance qu'un SIA à haut risque présente un risque pour la santé, la sécurité ou les droits fondamentaux des personnes, il lui incombe d'en identifier immédiatement les causes. Cette démarche peut, le cas échéant, être menée en collaboration avec le déployeur à l'origine du signalement, afin d'assurer une réponse rapide et coordonnée face aux risques.

Lorsque le fonctionnement d'un SIA implique le traitement de données personnelles, le responsable de traitement est tenu d'apprécier sa conformité au RGPD et à la loi « informatique et libertés » dès la conception, c'est-à-dire avant qu'il soit alimenté par des données à caractère personnel, et de manière régulière. Cette revue régulière permet :

- de tenir compte des évolutions techniques, de l'évolution des menaces informatiques, du contexte, etc ;
- d'adopter en temps utiles les mesures correctives adéquates pour garantir la protection des données utilisées.

Parmi les obligations à la charge du responsable de traitement, celui-ci est tenu de veiller à la confidentialité, l'intégrité et la disponibilité des données personnelles qu'il traite. L'atteinte à l'un de ces principes constitue une violation de données personnelles qui est soumise dans certains cas :

- à une **obligation de notification dans les meilleurs délais auprès de la CNIL** ;
- à **l'information des personnes concernées**.

Les déployeurs sont invités à consulter le site web de la CNIL pour plus de précisions sur :

- la conduite à tenir en cas de violations de données personnelles[39] ;
- les mesures de sécurité à mettre en œuvre pour la protection des données personnelles.

★★★ Recommandation 10.1. Désigner la personne en charge des déclarations de vigilance

Il est recommandé de **désigner précisément au sein de la structure qui est en charge des déclarations de vigilance** (ex. : gestionnaire des risques, comité qualité, pharmacie, service biomédical, DSI), afin de respecter les principes et obligations en matière de vigilance existante pour les SIA ayant un statut de DM/DMDIV, indépendamment de l'imputabilité, tel que décrit dans le CSP**. Cette déclaration à l'ANSM est obligatoire pour les incidents graves.**

★☆☆ Recommandation 10.2. Circuit de signalement des incidents

En parallèle, il est recommandé de :

- mettre en place un circuit spécifique de signalement des incidents **liés aux SIA non-DM** au fournisseur pour faciliter leur identification, correction et remontée nationale si nécessaire ;
- créer une procédure interne spécifique (type « algorithmovigilance ») pour les incidents liés aux **SIA non DM/DMDIV mais présentant un risque clinique important**.

[39] Violations de données personnelles : les règles à suivre | CNIL

- adapter les formulaires internes d'événements indésirables pour inclure explicitement les **incidents impliquant des SIA** (« Case IA »).
- sensibiliser les professionnels de santé à l'identification et au signalement systématique des **erreurs ou dysfonctionnements liés à un SIA** ;
- prévoir la **désactivation rapide ou l'arrêt immédiat du SIA** en cas d'incident grave détecté, avec des procédures établies de retour en mode dégradé. À ce titre, la simulation de procédures dégradées en cas d'interruption du service du SIA peut être mise en place.

Les sujets en lien avec l'IA doivent être abordés au sein des CME, des comités qualité et gestions des risques et des commissions des usagers. À ce titre, les outils existants comme les revues de morbi-mortalité peuvent être mobilisés pour analyser les événements indésirables.

★★★ Recommandation 10.3. Formaliser une procédure de maintenance et de gestion de la qualité

La maintenance doit être considérée comme une obligation partagée entre le fournisseur et le professionnel ou l'établissement de santé déployant le SIA. Au niveau d'un établissement, cette maintenance peut impliquer la direction des systèmes d'information, les équipes cliniques et les cellules qualité/sécurité, chacun devant être clairement identifié dans ses responsabilités et les actions qui lui reviennent. Il est recommandé de **formaliser une procédure interne en lien avec la maintenance et gestion de la qualité liées au SIA**, comprenant :

- le plan précis de gestion des mises à jour (qui, quand, comment) ;
- le plan de suivi des performances (indicateurs, fréquences d'évaluation) ;
- le processus de signalement des incidents (formulaires, canaux dédiés) ;
- le plan de continuité d'activité en cas d'indisponibilité de l'IA.

★★★ Recommandation 10.4. Audits réguliers de qualité

Il est recommandé de **prévoir des audits réguliers de qualité**, notamment des cas non détectés par le SIA (faux négatifs) afin d'éviter toute omission critique due à une surconfiance en l'outil, et **de mettre en place un suivi régulier d'indicateurs de performance et d'utilisation du SIA** (ex. : taux de faux positifs corrigés par l'humain, taux d'utilisation effective).

★☆☆ Recommandation 10.5. Contrôle de performance du SIA

Par ailleurs, il est recommandé d'effectuer lorsque nécessaire des **contrôles de performance** du SIA, particulièrement en cas de changements dans l'environnement clinique ou dans la population de patients traités (« dérive du modèle »). Une information auprès du fournisseur en cas de baisse des performances du SIA peut également être réalisée.

★★★ Recommandation 10.6. Mise à jour du SIA

Les mises à jour du SIA peuvent à la fois concerner le modèle algorithmique, l'interface, l'infrastructure, l'intégration à l'écosystème du système d'information (interopérabilité notamment), etc. Ces mises à jour doivent être réalisées par les déployeurs et **devraient faire l'objet d'un paragraphe dédié lors de la contractualisation**. Dans ces cas, un défaut de mise à jour du SIA pourrait notamment relever d'une défaillance contractuelle, dégageant la responsabilité du fournisseur en cas de dommage ou incident.

Au même titre que les autres solutions numériques et systèmes d'informations, il est recommandé de :

- **contractualiser la planification des mises à jour hors production** (créneaux de nuit/week-end) pour minimiser l'impact sur l'activité clinique ;
- désigner localement **un responsable interne** pour les mises à jour (ex. : ingénieur biomédical, DSI) en coordination étroite avec le référent du SIA pour anticiper les impacts métier ;
- **exiger une information anticipée** de la part du fournisseur sur toute mise à jour, accompagnée de notes de version précisant les modifications ;
- **disposer si nécessaire d'un environnement de test** permettant de valider chaque mise à jour avant son déploiement ;
- **mettre à jour les supports de formation** lorsque nécessaire ;
- **procéder, si applicable, à un contrôle de performances après une mise à jour importante** du modèle algorithmique afin de détecter d'éventuelles régressions.

Il est recommandé de **maintenir une traçabilité complète des mises à jour techniques et algorithmiques du SIA** (ex. : date, version, finalité de la mise à jour, résultats attendus) accessible à la fois aux professionnels utilisateurs et à l'administration de l'établissement.

Recommandation 10.7. Anticiper l'indisponibilité du SIA

★★★

Le niveau de service type SLA prévu lors de la contractualisation doit notamment **clarifier les délais d'intervention et de résolution d'incident**s. Afin d'anticiper l'indisponibilité du SIA, il est recommandé en premier lieu de **classer les SIA selon leur niveau de criticité clinique pour anticiper les besoins en continuité d'activité**. Il est également de recommandé de :

- prendre en compte ces SIA dans les **plans de reprise d'activités (PRA) et plans de continuité d'activité (PCA) ;**
- prévoir un **« mode dégradé » de fonctionnement en cas d'indisponibilité du SIA avec des scénarios de bascule au plus proche du bon sens,** notamment pour les DM/DMDIV ayant un impact important sur la prise en charge des patients ;
- **sensibiliser les équipes à ces scénarios et aux solutions de secours** (ex. : utilisation parallèle de deux SIA concurrents) en fonction de la criticité du système **;**
- **prévoir des sauvegardes régulières,** lorsque cela est pertinent, conservées selon des mesures de sécurité appropriées et conformes au cadre juridique applicable.

11. Fin du cycle de vie et désinstallation

Que le SIA soit déployé directement au sein du site ou non, la désinstallation ou le décommissionnement est un élément à anticiper dès la contractualisation, qui peut préciser de nombreux éléments sur la manière dont la désinstallation va se dérouler.

En effet, plus la traçabilité des données a été détaillée en amont lors de la contractualisation, plus la désinstallation sera simple. À cet effet, le déployeur doit avoir prévu une **clause de réversibilité des données** les données de la structure qui ont été utilisées doivent être relivrées à l'établissement sous une forme ou sous une autre ou supprimées le cas échéant si les données utiles pour la prise en charge sont déjà dans le dossier médical du patient. Une traçabilité de la suppression des données par le fournisseur peut être demandée pour garantir une non-réutilisation ultérieure.

★★★ Recommandation 11.1. Impliquer l'ensemble des acteurs lors de la désinstallation

Par ailleurs, il est recommandé **d'impliquer l'ensemble des personnes compétences lors de la désinstallation** (ex. : DSI, RSSI, DPO, archiviste). Par ailleurs, pour les SIA critiques, un délai pour la désinstallation peut être discuté lors de la contractualisation (par exemple, un délai de 2 ans de période transitoire dans le cas de désinstallation d'un dossier patient informatisé).

12. Spécificités des SIA générative

Les SIA générative sont de plus en plus utilisés en contexte de soins et plus largement, au sein d'établissements de santé pour des tâches cliniques et non cliniques.

> **Pour aller plus loin**
>
> Ces systèmes d'IA générative incluent notamment :
> - **les agents conversationnels utilisant de grands modèles de langage** (LLM - pour Large Language Models). Ces systèmes de génération de texte permettent de produire, reformuler, résumer ou structurer des informations à partir de données textuelles ;
> - **les systèmes d'IA générative multi-modaux**, ccapables d'analyser des informations provenant de plusieurs modalités de données (ex. : texte, image, audio, vidéo). Ces données peuvent être spécifiques au domaine de la santé : données omiques, histologiques, etc.
>
> La **génération augmentée par récupération** (RAG pour -Retrieval Augmented Generation) peut également être utilisée pour enrichir les capacités des modèles de langage en leur permettant d'accéder à une base de connaissances spécifique (ex. : un corpus documentaire particulier, provenant d'une étude ou d'un projet de recherche).
>
> Par ailleurs, des systèmes agentiques (ou agents IA) se développent. Ces systèmes fonctionnent avec un niveau d'autonomie supérieur et visent à atteindre un objectif précis avec une supervision limitée. Ils peuvent exécuter des actions multi-étapes pour atteindre l'objectif (ex. : la planification de soins ou la gestion des rendez-vous médicaux).

Utilisation en contexte de soins

Dans le contexte de soins, les SIA générative sont utilisés principalement pour :

- le suivi de patient : transcription automatique des consultations, la rédaction assistée (comptes-rendus cliniques, courriers, etc.), synthèse ou la structuration d'informations (par exemple, antécédents médicaux). Il s'agit du cas d'usage le plus fréquent ;
- l'aide à la recherche : interrogation de référentiels, de recommandations sourcées ;
- l'aide au diagnostic ou à la décision médicale ;
- la surveillance à distance : dispositifs de suivi de patients en perte d'autonomie à distance.

D'autres SIA générative sont utilisés pour échanger avec les patients sous la forme de chatbots ou voicebots, par exemple pour recueillir de l'information lors de "pré-consultations" ou pour l'orientation des patients dans leur parcours de soins.

Pour autant, la plupart de ces SIA ne relèvent pas à l'heure actuelle de la définition d'un dispositif médical ou dispositif médical de diagnostic in vitro au sens des règlements UE

2017/745 (RDM) ou UE 2017/746 (RDIV). Des évolutions du cadre réglementaire sont cependant possibles, comme cela a été le cas au Royaume-uni[40].

Une multiplication des usages non maîtrisés par les structures

Dans le cas particulier des agents conversationnels accessibles en ligne, la possibilité pour tout utilisateur d'interagir par commandes ou « prompt » avec un SIA a entraîné une multiplication exponentielle de leurs utilisations. Leur facilité d'accès (via un navigateur internet ou téléphone personnel, sans nécessité de création de comptes), favorise des usages non maîtrisés à l'échelle d'une structure. On parle alors de« shadow IT », en l'absence de maîtrise institutionnelle de ces outils et de leurs risques.

> Certains CHU remontent ainsi des connexions particulièrement importantes de ces outils (par exemple, le CHU de Nancy a décompté 440 000 connexions à des IA génératives personnelles par des agents de l'hôpital en août 2025)[41]. Un ordre de grandeur similaire a été mesuré au CHU de Montpellier.

Cette utilisation exponentielle, essentiellement non maîtrisée par les structures, exposent l'ensemble des acteurs à plusieurs risques :

- un **manque de fiabilité clinique** en raison notamment du risque d'hallucinations ou de biais dans les données d'apprentissage et par l'utilisation de LLMs non évalués spécifiquement sur les tâches médicales pour lesquelles ils sont utilisés ;
- un **risque d'atteinte au secret médical**, lié à l'intégration de données à caractère personnel sensibles dans les requêtes effectuées aux agents conversationnels en ligne (par exemple, l'histoire de la maladie du patient, qui peut devenir une donnée identifiante notamment en cas de maladies rares) ;
- un **risque informatique** ou de **cybersécurité** spécifique imposant une vigilance accrue de la part du déployeur, avec par exemple le risque d'utilisation malveillante par un utilisateur (dont contournement de garde-fou pour récupérer des données, injection de requête ou en anglais de prompt injection, etc.). Ce risque est particulièrement présent lorsque le modèle déployé est entraîné sur des données de santé ;
- un **risque de requalification** du déployeur en tant que fournisseur en cas de modification de la finalité d'usage du SIA.

Recommandations associées aux SIA génératifs

[40] NHS, Guidance on the use of AI-enabled ambient scribing products in health and care settings, Avril 2025

[41] APM News, Les hôpitaux "déjà dépassés" par l'utilisation des IA génératives hors des cadres (Arnaud Vanneste, CHU de Nancy)

Les bonnes pratiques de ce guide sont également applicables, pour la plupart, à ces SIA générative. **Cependant, leur utilisation doit être limitée à un usage adapté et raisonné.**

★★★ Recommandation 12.1. Maîtriser le susages des SIA génératifs

À ce titre, il est recommandé, pour les structures et direction (notamment des systèmes d'informations), **de maîtriser leur usage** avec notamment :

- la mise en pace d''une **sensibilisation du personnel** aux usages à risques ;
- la promotion d'une **charte d'usage de l'IA générative avec :**
  - **les pratiques interdites**
  - **un catalogue d'usages approuvés,** offrant un niveau de risque minimal. Lorsqu'ils sont disponibles, l'utilisation des SIA validés et mis à disposition par la structure doit être privilégié
  - **le cas échéant, la mise en place d'un proxy sortant avec filtrage** en cas d'utilisation de sites identifiés comme dangereux.

Les acteurs sont invités à consulter le contenu publié par :

- ➔ l'ANSSI pour des recommandations de sécurité dédiées à l'IA générative publiées par l'ANSSI sont disponibles[42] ;
- ➔ par la CNIL s'agissant de l'utilisation d'un SIA générative[43].

[42] ANSSI, Recommandations de sécurité pour un système d'IA générative https://cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative

[43] CNIL, Système d'IA générative https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-lutilisation-dun-systeme-dia-generative

Table des annexes

Annexe 1. Mise au point sur le règlement européen sur l'IA et la classification des SIA en santé

Le RIA établit une classification des SIA selon leur niveau de risque, attribuant à chaque catégorie des exigences spécifiques :

- **risque inacceptable** : les SIA portant atteinte à la sécurité ou aux droits fondamentaux (ex. : la notation sociale, l'exploitation de la vulnérabilité des personnes, le recours à des techniques subliminale) sont interdits depuis le 2 février 2025 ;
- **haut risque** : les SIA pouvant porter atteinte à la santé, la sécurité des personnes ou à leurs droits fondamentaux sont soumis à des exigences renforcées et un marquage CE. Le RIA impose un certain nombre d'obligations pour les fournisseurs et déployeurs de SIA à haut risque. En particulier, les articles 26 et 86 du RIA énoncent notamment les obligations devant être respectées par les déployeurs, à savoir en contexte de soins les établissements de santé, les structures sociales ou médico-sociales ou les professionnels de santé. À noter que certains dispositifs médicaux (DM ou DMDIV) intégrant de l'IA seront classés comme « à haut risque » : c'est notamment le cas de ceux soumis à une évaluation de la conformité par un organisme notifié (DM de classes IIa, IIb, et III, DM de classe I stérile, de mesurage ou instrument chirurgical réutilisable/ DMDIV de classes A stérile, B, C ou D) et dont le SIA est un composant de sécurité ou le SIA lui-même est un dispositif médical). Les SIA destinés à évaluer et hiérarchiser les appels d'urgence seront également classés comme à haut risque ;
- **risque limité** : les SIA interagissant avec des personnes physiques, de type chabots. Pour ces SIA, le RIA impose des obligations de transparence afin notamment que les utilisateurs finaux soient conscients qu'ils interagissent avec un SIA. C'est notamment le cas des SIA utilisés comme aide à la rédaction de comptes-rendus médicaux à partir d'une consultation et considérés à l'heure actuelle comme SIA à risque limité ;
- **risque minimal**. Le RIA ne prévoit pas d'obligation spécifique pour ces systèmes. La grande majorité des SIA actuellement utilisés dans l'UE entrent dans cette catégorie.

En parallèle, une catégorie ad hoc a été créée pour les SIA à usage général, ayant la capacité d'être utilisés et adaptés à un large éventail d'applications pour lesquelles ils n'ont pas été conçu intentionnellement et spécifiquement (ex. : génération de texte, d'image). Des obligations spécifiques s'appliqueront également à ces systèmes à usage général.

Publié au Journal officiel le 12 juillet 2024, la majorité des obligations du RIA seront applicables à compter du 2 août 2026, en particulier l'application des règles relatives aux SIA à haut risque de l'annexe III.

Les règles relatives aux SIA à haut risque de l'annexe I (dont les DM et DM-DIV) entreront en application à partir du 2 août 2027.

Annexe 2. Stratégie de la HAS et de la CNIL concernant l'IA

Stratégie de la HAS

La majorité des SIA utilisés en contexte de soins, sous forme de technologies numériques ayant le statut de dispositif médical ou non, sont aujourd'hui en dehors du champ d'évaluation de la HAS, qui vise à éclairer les décisions de remboursement. De ce fait, les utilisateurs, qu'ils soient patients ou professionnels, peuvent utiliser des SIA sans être pleinement éclairés sur leurs performances et leurs limites ou, a contrario, être réticents à leur utilisation pour ces mêmes raisons. Depuis 2022, la HAS développe une dynamique nationale en construisant un cadre de confiance autour de l'utilisation des SIA en santé, articulé autour de trois objectifs majeurs :

- guider les professionnels et établissements de santé dans leurs choix de technologies numériques pertinentes. Un guide d'aide au choix a été publié en 2023 et une production est en cours afin d'orienter le rationnel économique lié à l'achat de technologies numériques ;
- développer un cadre d'évaluation adapté, notamment à travers la construction de nouvelles démarches d'évaluation et des travaux d'évaluations pilotes ;
- accompagner activement le développement des usages de l'IA en contexte de soins. Cette production s'inscrit dans cette dynamique.

Ces trois axes sont inscrits dans le projet stratégique de la HAS 2025-2030 et ont été intégrés depuis 2024 au 6e cycle de certification des établissements de santé pour renforcer la stratégie de maîtrise des risques numériques et liés à l'intelligence artificielle.

Stratégie de la CNIL

Le développement de l'IA s'accompagne d'enjeux en matière de protection des données et des libertés individuelles. En effet, de très nombreux SIA se repose sur des traitements de données personnelles, que cela soit au stade de leur développement ou de leur déploiement. Fort de ce constat, l'IA est l'un des 4 axes du plan stratégique 2025-2028 de la CNIL. Concrètement, la CNIL met en œuvre un plan d'action ambitieux articulé autour de 4 volets :

- appréhender le fonctionnement des SIA et leurs impacts pour les personnes, en réalisant une vielle active du sujet et en partageant la connaissance auprès des différents publics (voir notamment le dossier « IA » du LINC) ;
- permettre et encadrer le développement d'IA respectueuses de la vie privée en clarifiant le cadre applicable aux SIA, en produisant des ressources visant à apporter de la sécurité juridique aux acteurs (fiches pratiques, questions/réponses, etc. disponibles sur le hub « Intelligence artificielle » du site web de la CNIL) ;
- fédérer et accompagner les acteurs innovants de l'écosystème IA en France et en Europe, en instruisant des demandes de conseils et en mettant en œuvre des dispositifs innovant tels que le Bac à Sable ou l'accompagnement renforcé ;
- auditer et contrôler les SIA et protéger les personnes, en initiant la réflexion sur les modalités de contrôles de ces dispositifs complexes, au titre du RGPD et du RIA.

Dans le secteur de la santé, la CNIL a mis en œuvre en 2024 une consultation publique en ce qui concerne ses référentiels. Les professionnels ont fait état de grandes attentes concernant les sujets IA. Pour y répondre, la CNIL axe désormais ses travaux sur l'inter-régulation afin d'élaborer des recommandations transversales et pluridisciplinaires comme c'est le cas précis dans ce guide commun HAS / CNIL. La CNIL prévoit également la publication prochaine d'une fiche récapitulant les règles applicables au développement de SIA dans le domaine de la santé, avec des exemples concrets issus des demandes d'autorisation, du bac à sable ou de l'accompagnement renforcé.

Annexe 3. Méthodologie du projet

La démarche suivie pour l'élaboration des présentes recommandations a été structurée autour de plusieurs étapes complémentaires :

1. **Analyse du cadre législatif et réglementaire applicable.**

Le cadre législatif et réglementaire associé à l'usage des SIA en santé est en constante évolution, à la fois au niveau européen et au niveau national. Les analyses réalisées dans cette production s'appuient sur les textes disponibles à la date de rédaction, ainsi que sur les interprétations actuellement stabilisées par les autorités compétentes. Elles représentent ainsi une photographie juridique qui pourra évoluer dans un futur proche. En particulier, des clarifications substantielles sont attendues de la part de la Commission européenne, concernant notamment :

- l'encadrement des modèles d'IA à usage général (GPAI) et leurs obligations spécifiques ;
- les modalités de mises en œuvre des obligations pour les déployeurs et fournisseurs.

En conséquence, certaines des recommandations proposées ici, bien qu'ancrées dans le droit en vigueur, pourront nécessiter des ajustements ultérieurs.

2. **Constitution et mobilisation d'un groupe de travail pluridisciplinaire.**

Un groupe de travail multi-institutionnel a été mis en place par la HAS, réunissant des professionnels de santé de diverses disciplines et profils, des experts du numérique en santé, des ingénieurs biomédicaux, des juristes spécialisés, des représentants d'usagers. La priorisation des recommandations a été effectuée par avis d'expert. La composition précise est détaillée ci-dessous.

3. **Recueil des retours d'expérience et consultation des parties prenantes.**

De nombreuses parties prenantes ont été consultées lors du cadrage des travaux. En complément et afin d'enrichir les travaux du groupe de travail, un questionnaire structuré a été diffusé préalablement auprès de CNP, d'établissements de santé, de professionnels libéraux, d'industriels et d'experts du secteur. Les réponses recueillies ont fait l'objet d'une analyse qualitative, mettant en évidence les pratiques existantes, les points de convergence et de divergence, ainsi que les attentes exprimées par les acteurs de terrain. Ces éléments ont été intégrés à chaque étape de la réflexion collective.

4. **Revue ciblée de la littérature.**

Une revue systématique ciblée a été menée en parallèle, centrée sur les démarches qualité et les bonnes pratiques liées à l'usage des SIA en contexte de soins, au niveau national et international. Cette analyse documentaire a permis d'alimenter les débats du groupe de travail et de confronter les propositions formulées aux données probantes disponibles.

5. **Consultation publique.**

Une version intermédiaire des recommandations est soumise à consultation publique pendant, afin de permettre à l'ensemble des acteurs concernés -établissements, professionnels, industriels, usagers – de contribuer aux travaux. Les différents retours de cette consultation seront analysés et intégrés, après validation avec le groupe de travail, dans la version finale du document.

Participants

Les organismes professionnels et associations de patients et d'usagers suivants ont été sollicités pour proposer des experts conviés à titre individuel dans les groupes de travail/lecture :

Conseil national de l'ordre des médecins

France Asso Santé

Groupe de travail

M. Bendjebbar Étienne, Responsable innovation, CHU de Nantes

M. Boulogne Philippe, Directeur des systèmes d'information, Hopital Foch et Expert Visiteur Numérique HAS

Dr Canarelli Jean, Médecin biologiste, Ajaccio et Délégué général aux données de santé et au numérique du CNOM

M. Dauphin Arthur, Représentant des usagers, Paris

Mme Dufourt Caroline, Déléguée à la protection des données, Hopital Américain de Paris

Dr Farah Line, Délégation du numérique en santé, ministère de la Santé

M. Février Yann, Chargé de mission SI, GHT Est-Hérault Sud-Aveyron et Expert Visiteur Numérique HAS

Pr Isnard Bagnis Corinne, Néphrologue, AP-HP

Dr Gérardin Christel, Interniste, APHP

M. Kirche Stéphane, Directeur des technologies de la santé, de l'innovation et de l'ingénierie clinique, CH de Chalon

Dr Maillard Nicolas, Pharmacien, CH de Vannes

Pr Morquin David, Infectiologue, CHU de Montpellier

Mme Sumbal Davina, Responsable qualité, Hôpital Saint Joseph

Pr Vuiblet Vincent, Pathologiste, CHU de Reims

Mme Williatte Lina, Professeur des Universités Catholiques et Avocat, Lille

Remerciements

La HAS et la CNIL tiennent à remercier l'ensemble des participants cités ci-dessus ainsi que l'ANSM et la DGCCRF pour leur relecture précieuse lors de l'élaboration du document.

Retrouvez tous nos travaux sur
www.has-sante.fr

HAS
HAUTE AUTORITÉ DE SANTÉ
Développer la qualité dans le champ sanitaire, social et médico-social